SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja
Prezes Rady Ministrów
RM-0610-69-23

Druk nr 3457

Warszawa, 3 lipca 2023 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem

Mateusz Morawiecki

/podpisano kwalifikowanym podpisem elektronicznym/

Projekt

U S T A W A

z dnia

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[1), 2)]

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913) wprowadza się następujące zmiany:

1) oznaczenie i tytuł rozdziału 1 otrzymują brzmienie:

„DZIAŁ I. POSTANOWIENIA OGÓLNE”;

2) w art. 1:

a) w ust. 1:

– po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanego dalej „rozporządzeniem 2019/881”;”,

– w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4–6 w brzmieniu:

---

1) Niniejsza ustawa w zakresie swojej regulacji:
   1) służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15);
   2) wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE. L 321 z 17.12.2018, str. 36, Dz. Urz. UE L 334 z 27.12.2019, str. 164 oraz Dz. Urz. UE L 419 z 11.12.2020, str. 36).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym oraz ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych.

„4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa sieci lub usług komunikacji elektronicznej i zgłaszania incydentów telekomunikacyjnych;

5) zasady i tryb wyznaczania operatora strategicznej sieci bezpieczeństwa oraz jego zadania;

6) zasady przyznania zasobów częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz;”,

b) w ust. 2:

– uchyla się pkt 1,

– pkt 2 otrzymuje brzmienie:

„2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73 oraz z Dz. Urz. UE L 333 z 27.12.2022, str. 80), z wyjątkiem art. 67a;”;

3) art. 2 otrzymuje brzmienie:

„Art. 2. Użyte w ustawie określenia oznaczają:

1) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30 oraz Dz. Urz. UE L 169 z 25.06.2019, str. 1), zwanym dalej „rozporządzeniem 765/2008”;

2) bezpieczeństwo sieci lub usług komunikacji elektronicznej – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:

a) tych sieci lub usług,

b) przetwarzanych informacji objętych tajemnicą komunikacji elektronicznej,

c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;

3) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

4) certyfikat – europejski certyfikat cyberbezpieczeństwa albo krajowy certyfikat cyberbezpieczeństwa;

5) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

6) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

7) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

8) CSIRT INT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Szefa Agencji Wywiadu na rzecz Agencji Wywiadu oraz jednostek organizacyjnych podległych ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowanych;

9) CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;

10) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na rzecz przedsiębiorców komunikacji elektronicznej;

11) cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami;

12) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz na inne podmioty;

13) deklaracja zgodności – oświadczenie dostawcy produktu ICT, usługi ICT lub procesu ICT, że jest on zgodny z europejskim programem certyfikacji

cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881 lub krajowym programem certyfikacji cyberbezpieczeństwa;

14) dostarczanie sieci telekomunikacyjnej – dostarczanie sieci telekomunikacyjnej, o którym mowa w art. 2 pkt 5 ustawy z dnia… – Prawo komunikacji elektronicznej (Dz. U. poz. …);
15) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w art. 2 pkt 3–6 rozporządzenia 765/2008;
16) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;
17) incydent krytyczny – incydent lub incydent telekomunikacyjny skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
18) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
19) incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;
20) incydent telekomunikacyjny – każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci lub usług komunikacji elektronicznej;
21) incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15;
22) ISAC – centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;

23) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia 765/2008;
24) komunikat elektroniczny – komunikat elektroniczny, o którym mowa w art. 2 pkt 19 ustawy z dnia …– Prawo komunikacji elektronicznej;
25) krajowy certyfikat cyberbezpieczeństwa – certyfikat cyberbezpieczeństwa wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa;
26) krajowa deklaracja zgodności – deklaracja zgodności wydana w ramach krajowego programu certyfikacji cyberbezpieczeństwa;
27) krajowy program certyfikacji cyberbezpieczeństwa – kompleksowy zbiór przepisów, wymagań technicznych, norm i procedur określonych przez Radę Ministrów i mających zastosowanie do certyfikacji lub oceny zgodności produktów ICT, usług ICT lub procesów ICT objętych zakresem danego programu;
28) krajowy poziom uzasadnienia zaufania – potwierdzenie, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymagania wskazanego poziomu bezpieczeństwa określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
29) obsługa incydentu lub incydentu telekomunikacyjnego – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu lub incydentu telekomunikacyjnego;
30) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;
31) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;
32) poważny incydent telekomunikacyjny – incydent telekomunikacyjny o znaczącym wpływie na bezpieczeństwo sieci lub usług komunikacji elektronicznej;
33) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;
34) produkt ICT – element lub grupę elementów systemu informacyjnego;
35) przedsiębiorca komunikacji elektronicznej – przedsiębiorcę komunikacji elektronicznej, o którym mowa w art. 2 pkt 39 ustawy z dnia … Prawo komunikacji elektronicznej;

36) przedsiębiorca telekomunikacyjny – przedsiębiorcę telekomunikacyjnego, o którym mowa w art. 2 pkt 40 ustawy z dnia …– Prawo komunikacji elektronicznej;
37) ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
38) SOC wewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa utworzony w ramach struktury organizacyjnej operatora usługi kluczowej;
39) SOC zewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa operatora usługi kluczowej, świadczący usługi na rzecz tego operatora działający poza jego strukturą organizacyjną;
40) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
41) system informacyjny – system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. poz. 57 i 1123), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
42) sytuacja szczególnego zagrożenia – sytuacja, o której mowa w art. 2 pkt 65 ustawy z dnia …– Prawo komunikacji elektronicznej;
43) telekomunikacyjne urządzenia końcowe – telekomunikacyjne urządzenia końcowe, o których mowa w art. 2 pkt 71 ustawy z dnia …– Prawo komunikacji elektronicznej;
44) usługa cyfrowa – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), wymienioną w załączniku nr 2 do ustawy;
45) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;
46) usługa kluczowa – usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;
47) usługa komunikacji elektronicznej – usługę, o której mowa w art. 2 pkt 76 ustawy z dnia … – Prawo komunikacji elektronicznej;
48) zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;

49) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.”;

4) po art. 2 dodaje się oznaczenie działu II oraz rozdział 1 i tytuły w brzmieniu:

„DZIAŁ II.

Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa

Rozdział 1

Krajowy system cyberbezpieczeństwa”;

5) w art. 3 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu:

„2. Ustawa ma zastosowanie we wszystkich stanach gotowości obronnej państwa.”;

6) po art. 3 dodaje się art. 3a w brzmieniu:

„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu:

1) wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usługi kluczowej, usługi cyfrowej lub realizację zadań publicznych;
2) czasowego ograniczenia ruchu sieciowego z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu.”;

7) użyte w art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 12 w ust. 3 i 4, w art. 14 ust. 3, w art. 15 w ust. 2 w pkt 3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 48 w pkt 1, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy”;

8) w art. 4:

a) po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) przedsiębiorców komunikacji elektronicznej;”,

b) po pkt 6 dodaje się pkt 6a–6c w brzmieniu:

„6a) CSIRT INT;

6b) CSIRT Telco;

6c) ISAC, wpisany do wykazu, o którym mowa w art. 25a ust. 4;”,

c) w pkt 7 wyrazy „w art. 9 pkt 1–6, 8, 9, 11 i 12” zastępuje się wyrazami „w art. 9 pkt 1–6 i 8–10”,

d) po pkt 7 dodaje się pkt 7a w brzmieniu:

„7a) Urząd Komisji Nadzoru Finansowego;”,

e) pkt 8 otrzymuje brzmienie:

„8) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2023 r. poz. 742 i 1088);”,

f) po pkt 14 dodaje się pkt 14a i 14b w brzmieniu:

„14a) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2022 r. poz. 2625 i 2687 oraz z 2023 r. poz. 295, 412 i 877);

14b) Polski Fundusz Rozwoju oraz inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2023 r. poz. 1103);”,

g) pkt 16 otrzymuje brzmienie:

„16) SOC zewnętrzne;”,

h) po pkt 17 dodaje się pkt 17a w brzmieniu:

„17a) Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE”;”;

9) w art. 7:

a) po ust. 3 dodaje się ust. 3a w brzmieniu:

„3a. W przypadku podmiotów, dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, wpisanie do wykazu operatorów usług kluczowych albo zmiana danych tych podmiotów dokonywana jest z urzędu.”,

b) w ust. 4 wyrazy „nie później niż w terminie 6 miesięcy” zastępuje się wyrazami „niezwłocznie, nie później niż w terminie 1 miesiąca”,

c) ust. 5 otrzymuje brzmienie:

„5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.”;

10) użyte w art. 8 w pkt 3, w pkt 5 w lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, w ust. 3 w pkt 1, 2, 4 i 10, w pkt 14 w lit. b i c oraz w ust. 6 w pkt 2, w art. 33 w ust. 4a, w art. 35 w ust. 4 i 5, w art. 37 w ust. 1, w art. 39 w ust. 1, w ust. 3 we wprowadzeniu do wyliczenia i w ust. 4 we wprowadzeniu do wyliczenia, w art. 46 w ust. 1 w pkt 5, w art. 51 w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i 2, w art. 73 w ust. 5 w pkt 1, w art. 83, w różnej liczbie i różnym przypadku, wyrazy „zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i odpowiednim przypadku wyrazem „cyberzagrożenie”;

11) w art. 8 w pkt 5 lit. b otrzymuje brzmienie:

„b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji,”;

12) w art. 9:

a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”,

b) ust. 2 otrzymuje brzmienie:

„2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa dane osób, o których mowa w ust. 1 pkt 1, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych – w terminie 14 dni od dnia ich zmiany. Organ właściwy do spraw cyberbezpieczeństwa przekazuje te dane do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.”;

13) w art. 10:

a) w ust. 1, w ust. 2 we wprowadzeniu do wyliczenia oraz w ust. 3 i 4 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”,

b) w ust. 2 pkt 2 otrzymuje brzmienie:

„2) ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”,

c) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazami „bezpieczeństwa systemów informacyjnych”;

14) w art. 11:

a) w ust. 1 w pkt 4 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”,

b) w ust. 2 po wyrazach „przekazywane jest w postaci elektronicznej” dodaje się wyrazy „za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1”,

c) ust. 3 otrzymuje brzmienie:

„3. Operator usługi kluczowej niezależnie od zadań określonych w ust. 1:

1) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, koordynowanej przez CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

2) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach.”,

d) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. W przypadku, gdy:

1) operator usługi kluczowej jest przedsiębiorcą komunikacji elektronicznej oraz

2) zgłasza incydent poważny, będący również poważnym incydentem telekomunikacyjnym

– zgłoszenie, zawierające elementy wskazane w art. 20e, jest przekazywane tylko do właściwego CSIRT sektorowego.

3b. Operator usługi kluczowej współdziała również z CSIRT Telco w sytuacji, o której mowa w ust. 3a.”;

15) w art. 13:

a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”,

b) uchyla się ust. 3,

c) dodaje się ust. 5 w brzmieniu:

„5. W uzasadnionym przypadku, CSIRT sektorowy przekazuje do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV informacje, o których mowa w ust. 1, niezwłocznie po stwierdzeniu zasadności przekazania danej informacji, nie później jednak niż w ciągu 8 godzin od takiego stwierdzenia.”;

16) art. 14 otrzymuje brzmienie:

„Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3b, art. 12 i art. 13, w zakresie bezpieczeństwa systemów informacyjnych są realizowane w ramach SOC wewnętrznego lub SOC zewnętrznego.

2. Operator usługi kluczowej powołuje SOC wewnętrzny lub zawiera umowę o świadczenie usług przez SOC zewnętrzny.

3. Organ tworzący lub nadzorujący operatora usługi kluczowej może utworzyć na rzecz tego operatora SOC zewnętrzny.

4. SOC wewnętrzny może realizować zadania, o których mowa w ust. 1, jako SOC zewnętrzny także na rzecz innych operatorów usług kluczowych.

5. SOC wewnętrzny lub SOC zewnętrzny prowadzi działania zapewniające cyberbezpieczeństwo na podstawie przeprowadzonego szacowania ryzyka, w szczególności wprowadza zabezpieczenia, zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów informacyjnych, a także eksploatacji i architektury systemów informacyjnych, w celu:

1) monitorowania i wykrywania incydentów;
2) reagowania na incydenty;
3) zapobiegania incydentom;
4) zarządzania jakością zabezpieczeń systemów informacyjnych, informacji i aktywów;
5) aktualizowania analizy ryzyka w przypadku zmiany struktury organizacyjnej, procesów lub technologii, które mogą wpływać na działania, o których mowa w pkt 1–3.

6. Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o sposobie realizacji obowiązku, o którym mowa w ust. 2, polegającego na powołaniu SOC wewnętrznego lub zawarciu umowy o świadczenie usług przez SOC zewnętrzny, lub o zmianie sposobu realizacji tego obowiązku.

7. W przypadku zawarcia umowy o świadczenie usług przez SOC zewnętrzny operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o:

1) zawarciu takiej umowy oraz dacie jej zawarcia,
2) danych kontaktowych podmiotu, z którym zawarta została umowa, o których mowa w ust. 12 pkt 4,
3) zakresie świadczonej usługi,

4) terminie obowiązywania umowy,

5) rozwiązaniu umowy

– w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.

8. W przypadku, gdy jest to niezbędne dla zapewnienia bezpieczeństwa systemów informacyjnych, podmiot prowadzący SOC zapewnia bezpieczny i zdalny dostęp do swoich systemów informacyjnych obsługiwanemu operatorowi usługi kluczowej przez co najmniej:

1) ustalenie zasad dostępu do systemu informacyjnego;

2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;

3) minimalizację zakresu danych przechowywanych poza bezpiecznym środowiskiem.

9. Umowa o świadczenie usług przez SOC zewnętrzny zawiera postanowienie, że świadczenie tych usług podlega prawu polskiemu.

10. Infrastruktura SOC wewnętrznego lub SOC zewnętrznego wykorzystywana do realizacji zadań, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3b, art. 12 i art. 13, znajduje się na terytorium Rzeczypospolitej Polskiej.

11. Osoba realizująca zadania, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3b, art. 12 i art. 13, w ramach SOC wewnętrznego lub SOC zewnętrznego, posiada poświadczenie bezpieczeństwa w zakresie dostępu do informacji niejawnych oznaczonych klauzulą „poufne” lub wyższą.

12. SOC zewnętrzny udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:

1) nazwę SOC zewnętrznego;

2) zakres działania, w tym:

   a) oferowany rodzaj wsparcia,

   b) zasady współpracy i wymiany informacji,

   c) politykę komunikacji;

3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów;

4) dane kontaktowe, w tym:

   a) adres ze wskazaniem strefy czasowej,

   b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC,

c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC zewnętrznym,

d) sposoby kontaktu z SOC zewnętrznym, w tym sposób zgłaszania incydentów.”;

17) po art. 14 dodaje się art. 14a w brzmieniu:

„14a. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz SOC wewnętrznych i SOC zewnętrznych, zwany dalej „wykazem SOC”.

2. Wykaz SOC zawiera:

1) nazwę (firmę) podmiotu prowadzącego SOC wewnętrzny lub SOC zewnętrzny;
2) nazwę (firmę) podmiotów, na rzecz których SOC wewnętrzny lub SOC zewnętrzny jest prowadzony;
3) siedzibę i adres SOC wewnętrznego lub SOC zewnętrznego;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) datę wpisania do wykazu SOC;
7) datę wykreślenia z wykazu SOC.

3. Wpisanie do wykazu SOC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie, nie później niż w terminie 14 dni po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1–5.

4. W przypadku podmiotów, dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, wpisanie do wykazu SOC dokonuje się z urzędu po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6.

5. Zmiana danych w wykazie SOC następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Przepis ust. 4 stosuje się odpowiednio.

6. Wnioski, o których mowa w ust. 3 i 5, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

7. Wpisanie do wykazu SOC i wykreślenie z tego wykazu oraz zmiana danych w wykazie SOC są czynnościami materialno-technicznymi.

8. Minister właściwy do spraw informatyzacji może, z urzędu, wpisać do wykazu, o którym mowa w ust. 1, inny podmiot niż SOC wewnętrzny lub SOC zewnętrzny, jeżeli podmiot ten co najmniej:

1) świadczy usługi z zakresu cyberbezpieczeństwa, w szczególności związane z:
   a) monitorowaniem, wykrywaniem incydentów, reagowaniem na incydenty i zapobieganiem incydentom,
   b) zarządzaniem jakością zabezpieczeń systemów, informacji i powierzonych aktywów,
   c) aktualizowaniem ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reagowanie na incydent;
2) posiada dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756 i 1030);
3) zawrze z ministrem właściwym do spraw informatyzacji porozumienie w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

9. Podmiot, o którym mowa w ust. 8, informuje ministra właściwego do spraw informatyzacji o wszelkich zmianach w zakresie warunków, o których mowa w ust. 8 pkt 1 i 2.

10. Minister właściwy do spraw informatyzacji wykreśla z wykazu wpisany z urzędu podmiot, który przestał spełniać warunki, o których mowa w ust. 8.

11 Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym.

12. Minister właściwy do spraw informatyzacji udostępnia dane z wykazu SOC, na wniosek, następującym podmiotom:

1) organowi właściwemu do spraw cyberbezpieczeństwa,
2) Policji,
3) Żandarmerii Wojskowej,
4) Straży Granicznej,
5) Centralnemu Biuru Antykorupcyjnemu,
6) Agencji Bezpieczeństwa Wewnętrznego,
7) Agencji Wywiadu,

8) Służbie Kontrwywiadu Wojskowego,
9) Służbie Wywiadu Wojskowego,
10) sądom,
11) prokuraturze,
12) organom Krajowej Administracji Skarbowej,
13) dyrektorowi Rządowego Centrum Bezpieczeństwa,
14) Służbie Ochrony Państwa

– w zakresie niezbędnym do realizacji ich ustawowych zadań.

13. Dane z wykazu SOC mogą być udostępniane, w zakresie o którym mowa w ust. 11 i 12, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”;

18) użyty w art. 17 w ust. 2, art. 69 w ust. 1 oraz w ust. 2 w pkt 1, 6 i 7 w różnej liczbie i przypadku wyraz „cyberbezpieczeństwo” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „bezpieczeństwo systemów informacyjnych”;
19) w art. 17 w ust. 2 w pkt 1 skreśla się wyrazy „systemów informacyjnych i”;
20) po rozdziale 4 dodaje się rozdział 4a w brzmieniu:

„Rozdział 4a

Zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów

Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia.

2. Przedsiębiorca komunikacji elektronicznej:

1) przeprowadza systematyczne szacowanie ryzyka wystąpienia sytuacji szczególnego zagrożenia co najmniej raz w roku;
2) podejmuje środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:
   a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej,

b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia,

c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,

d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej

– przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków;

3) dokumentuje czynności, o których mowa w pkt 1 i 2.

3. Przedsiębiorca komunikacji elektronicznej sporządzający plan działań w sytuacji szczególnego zagrożenia dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2.

4. Przedsiębiorca komunikacji elektronicznej:

1) wyznacza dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

2) przekazuje do Prezesa UKE dane osób, o których mowa w pkt 1, zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych – w terminie 14 dni od dnia zmiany tych danych.

5. Prezes UKE przekazuje te dane, o których mowa w ust. 4, do CSIRT Telco oraz do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

6. Przepisu ust. 4 nie stosuje się do przedsiębiorcy komunikacji elektronicznej, który jest mikroprzedsiębiorcą, małym przedsiębiorcą lub średnim przedsiębiorcą.

7. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej.

Art. 20b. 1. Prezes UKE może dokonywać oceny zastosowanych przez przedsiębiorcę komunikacji elektronicznej środków technicznych i organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2, kierując się rekomendacjami ENISA.

2. Przedsiębiorca komunikacji elektronicznej jest obowiązany do przekazania Prezesowi UKE, na jego żądanie, informacji niezbędnych do dokonania oceny.

3. Żądanie, o którym mowa w ust. 2, zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę;
3) wskazanie zakresu żądanych informacji oraz okresu, którego dotyczą;
4) wskazanie celu, jakiemu informacje mają służyć;
5) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
6) pouczenie o zagrożeniu karą, o której mowa w art. 76a ust. 1 pkt 4.

4. Prezes UKE może, w drodze decyzji, w przypadku powstania w wyniku dokonanej oceny, o której mowa w ust. 1, uzasadnionych wątpliwości co do stosowania właściwych środków technicznych i organizacyjnych, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek:

1) właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych lub
2) poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę komunikacji elektronicznej, niezależny podmiot i udostępnienia Prezesowi UKE wyników tego audytu.

5. W decyzji nakładającej obowiązek, o którym mowa w ust. 4:

1) w pkt 1 – Prezes UKE wskazuje termin właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych;
2) w pkt 2 – Prezes UKE określa termin udostępnienia wyników audytu bezpieczeństwa.

6. Do audytu bezpieczeństwa, o którym mowa w ust. 5 pkt 2, stosuje się odpowiednio art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5. Audytorzy, o których mowa w art. 15 ust. 2 pkt 2, wykonujący audyt bezpieczeństwa muszą być niezależni od przedsiębiorcy komunikacji elektronicznej, u którego prowadzony jest audyt bezpieczeństwa.

Art. 20c. Przedsiębiorca komunikacji elektronicznej:

1) zapewnia obsługę incydentu telekomunikacyjnego;
2) może przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco informacje:

a) o cyberzagrożeniach, podatnościach i incydentach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci lub usług komunikacji elektronicznej,

b) o wykorzystywanych technologiach;

3) zapewnia dostęp do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań.

Art. 20d. 1. Przedsiębiorca komunikacji elektronicznej:

1) uznaje incydent telekomunikacyjny za poważny incydent telekomunikacyjny;
2) zgłasza poważny incydent telekomunikacyjny, niezwłocznie, nie później niż w ciągu 8 godzin od momentu jego wykrycia, do CSIRT Telco;
3) współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco oraz z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej przy użyciu innych dostępnych środków komunikacji.

3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, biorąc pod uwagę rekomendacje ENISA, progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny, uwzględniając:

1) liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ;
2) czas trwania skutków incydentu telekomunikacyjnego;
3) obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego;
4) zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług;
5) wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej;
6) wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122);
7) wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych;
8) wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Art. 20e. 1. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy oraz numer we właściwym rejestrze, jeżeli został nadany;
2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu telekomunikacyjnego na sieci i usługi, w tym:
   a) sieci telekomunikacyjne, na które poważny incydent telekomunikacyjny miał wpływ,
   b) usługi komunikacji elektronicznej zgłaszającego, na które poważny incydent telekomunikacyjny miał wpływ,
   c) liczbę użytkowników usługi komunikacji elektronicznej, na których poważny incydent telekomunikacyjny miał wpływ,
   d) moment wystąpienia i wykrycia poważnego incydentu telekomunikacyjnego oraz czas jego trwania,
   e) zasięg geograficzny obszaru, którego dotyczy poważny incydent telekomunikacyjny,
   f) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi kluczowej przez operatorów usług kluczowych, jeżeli jest znany,
   g) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi cyfrowej przez dostawców usług cyfrowych, jeżeli jest znany,
   h) przyczynę zaistnienia poważnego incydentu telekomunikacyjnego i sposób jego przebiegu oraz skutki jego oddziaływania na sieci telekomunikacyjne lub świadczone usługi komunikacji elektronicznej,
   i) wpływ poważnego incydentu telekomunikacyjnego na połączenia z numerami alarmowymi,
   j) wpływ poważnego incydentu telekomunikacyjnego na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;
6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych.

2. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, może zawierać inne istotne informacje.

3. Przedsiębiorca komunikacji elektronicznej przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu telekomunikacyjnego.

4. Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20d ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu telekomunikacyjnego przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco.

5. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco może zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

6. W zgłoszeniu przedsiębiorca komunikacji elektronicznej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 20f. 1. Przedsiębiorca komunikacji elektronicznej udostępnia na swojej stronie internetowej informacje o:

1) potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej;
2) rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
3) przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

2. W przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego przedsiębiorca komunikacji elektronicznej, informuje swoich użytkowników, na których takie zagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach. Przedsiębiorca komunikacji elektronicznej informuje tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej.

3. Przedsiębiorca komunikacji elektronicznej informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.

Art. 20g. W przypadku stwierdzenia przesyłania komunikatów elektronicznych zagrażających bezpieczeństwu sieci lub usług komunikacji elektronicznej, przedsiębiorca komunikacji elektronicznej, może zastosować środki polegające na:

1) zablokowaniu przesłania takiego komunikatu,
2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej

– w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.

Art. 20h. 1. Prezes UKE, kierując się rekomendacjami ENISA dotyczącymi raportowania incydentów telekomunikacyjnych:

1) informuje o wystąpieniu poważnego incydentu telekomunikacyjnego organy regulacyjne innych państw członkowskich oraz ENISA, jeżeli uzna charakter tego incydentu za istotny;
2) przekazuje Komisji Europejskiej oraz ENISA sprawozdanie za rok poprzedni zawierające informacje o poważnych incydentach telekomunikacyjnych.

2. W przypadkach uzasadnionych interesem publicznym Prezes UKE może udostępniać na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej informację o wystąpieniu poważnego incydentu telekomunikacyjnego.

3. Prezes UKE informuje niezwłocznie, w terminie nie dłuższym niż 3 dni, przedsiębiorcę komunikacji elektronicznej, u którego wystąpił poważny incydent telekomunikacyjny, o opublikowaniu informacji, o której mowa w ust. 2, wraz ze wskazaniem adresu elektronicznego, pod którym udostępniona jest ta informacja.

4. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 3, jest obowiązany udostępniać na swojej stronie internetowej informację o wystąpieniu poważnego incydentu telekomunikacyjnego oraz umieścić adres elektroniczny, o którym mowa w ust. 3, niezwłocznie, nie później niż w terminie 3 dni od dnia otrzymania informacji, o której mowa w ust. 3.

5. Prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej, o którym mowa w ust. 3, obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób

jej publikacji, jeżeli sposoby opublikowania informacji, o których mowa w ust. 2 i 3, w niewystarczającym stopniu służą ochronie interesu publicznego.”;

21) w art. 21:

a) w ust. 1 wyrazy „osoby odpowiedzialnej” zastępuje się wyrazami „dwóch osób odpowiedzialnych”,

b) w ust. 2 i 3 wyrazy „jedną osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”;

22) w art. 22:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne są objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zgłaszają incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT INT.”,

b) w ust. 2 po wyrazach „w ust. 1 pkt 2” dodaje się wyrazy „oraz ust. 1a”,

c) dodaje się ust. 3–5 w brzmieniu:

„3. Niezależnie od zadań, określonych w ust. 1, Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne są objęte jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, przekazuje jednocześnie CSIRT INT w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, zgłoszenie, o którym mowa w ust. 1 pkt 2.

4. Jednostki, o których mowa w ust. 3:

1) współdziałają z CSIRT INT podczas obsługi incydentu w podmiocie publicznym, przekazując niezbędne dane, w tym dane osobowe;

2) zapewniają CSIRT INT dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań;

3) przekazują do CSIRT INT dane osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

5. CSIRT INT niezwłocznie przekazuje informacje, o których mowa w ust. 4, do CSIRT GOV.”;

23) w art. 23 w ust. 3 i 4 oraz w art. 24 w zdaniu pierwszym wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”;

24) po rozdziale 5 dodaje się rozdział 5a w brzmieniu:

„Rozdział 5a

ISAC w krajowym systemie cyberbezpieczeństwa

Art. 25a. 1. ISAC oraz minister właściwy do spraw informatyzacji mogą zawrzeć porozumienie w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, jeżeli ISAC w szczególności:

1) wspiera podmioty krajowego systemu cyberbezpieczeństwa w:
   a) rozpoznawaniu cyberzagrożeń i obsługi incydentów,
   b) podnoszeniu świadomości cyfrowej;
2) gromadzi i analizuje informacje o podatnościach, cyberzagrożeniach i incydentach oraz zapewnia podmiotom krajowego systemy cyberbezpieczeństwa dostęp do tych informacji i wyników analiz.

2. Do porozumienia, o którym mowa w ust. 1, art. 46 ust. 3 stosuje się odpowiednio.

3. Podmioty tworzące ISAC wyznaczają przedstawiciela w celu zawarcia porozumienia, o którym mowa w ust. 1, oraz wykonania obowiązków, o których mowa w ust. 8 i 9.

4. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC, które zawarły porozumienie, o którym mowa w ust. 1, zwany dalej „wykazem ISAC”.

5. Wykaz ISAC zawiera:

1) nazwę ISAC i nazwy podmiotów go tworzących;
2) imię i nazwisko osoby reprezentującej ISAC lub jego przedstawiciela wraz z numerem telefonu oraz adresem poczty elektronicznej;

3) siedzibę i adres ISAC, jeżeli posiada;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) adres poczty elektronicznej ISAC;
7) adres strony internetowej ISAC, jeżeli posiada;
8) adres do doręczeń elektronicznych ISAC, jeżeli posiada;
9) datę zawarcia porozumienia;
10) datę wpisania do wykazu ISAC;
11) datę wykreślenia z wykazu ISAC.

6. Wpisanie do wykazu ISAC następuje niezwłocznie, najpóźniej w ciągu 7 dni od zawarcia porozumienia, o którym mowa w ust. 1.

7. Wykreślenie ISAC z wykazu ISAC następuje w przypadku:
1) rozwiązania porozumienia, o którym mowa w ust. 1;
2) rozwiązania ISAC.

8. Zmiana danych w wykazie ISAC następuje na wniosek jednego z podmiotów tworzących ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu. Wniosek sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

9. Podmioty tworzące ISAC są obowiązane poinformować o rozwiązaniu ISAC.

10. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno-technicznymi.

11. Wykaz ISAC jest udostępniany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. W udostępnianym wykazie nie umieszcza się informacji wskazanych w ust. 5 pkt 2.

12. ISAC wpisany do wykazu ISAC współpracuje z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów.

13. Minister właściwy do spraw informatyzacji, na wniosek organu właściwego do spraw cyberbezpieczeństwa albo z urzędu, może przeprowadzić kontrolę:
1) realizacji obowiązków, o których mowa w ust. 12, ISAC wpisanego do wykazu ISAC;

2) przestrzegania przez ISAC wpisany do wykazu ISAC, zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa określonych w porozumieniu, o którym mowa w ust. 1.

14. Do kontroli, o której mowa w ust. 13, przepis art. 54 ust. 2 stosuje się odpowiednio.

15. W razie stwierdzenia, że ISAC wpisany do wykazu ISAC nie realizuje obowiązków, o których mowa w ust. 12, lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa określone w porozumieniu, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji, w zależności od rodzaju i stopnia stwierdzonych nieprawidłowości, może:

1) wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości w określonym terminie lub

2) wypowiedzieć porozumienie, o którym mowa w ust. 1.”;

25) w art. 26:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. W czasie stanu wojennego i w czasie wojny CSIRT MON, w imieniu Ministra Obrony Narodowej, koordynuje działania CSIRT NASK i CSIRT GOV.”,

b) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach, na wniosek podmiotów krajowego systemu cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w jednolitym wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów i incydentów telekomunikacyjnych.”,

c) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu:

„2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów i incydentów telekomunikacyjnych, o których mowa w ust. 2:

1) CSIRT NASK za zgodą ministra właściwego do spraw informatyzacji;

2) CSIRT GOV za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego, lub

3) CSIRT MON za zgodą Ministra Obrony Narodowej.

2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków porozumiewania się na odległość.”,

d) w ust. 3:

– w pkt 1 wyrazy „i incydentów” zastępuje się wyrazami „incydentów i incydentów telekomunikacyjnych”,

– w pkt 2 po wyrazie „incydentami” dodaje się wyrazy: „i incydentami telekomunikacyjnymi”,

– w pkt 3 wyrazy „incydentów i ryzyk” zastępuje się wyrazami „incydentów, incydentów telekomunikacyjnych i ryzyk”,

– pkt 5 otrzymuje brzmienie:

„5) reagowanie oraz koordynacja reagowania na zgłoszone incydenty i incydenty telekomunikacyjne;”,

– w pkt 6 wyrazy „w tym incydentów poważnych oraz incydentów istotnych” zastępuje się wyrazami „w tym incydentów poważnych, incydentów istotnych oraz incydentów telekomunikacyjnych”,

– w pkt 10 po wyrazach „i incydentów krytycznych” dodaje się wyrazy „z CSIRT INT”,

– w pkt 12 wyrazy „30 maja” zastępuje się wyrazami „31 stycznia”,

– pkt 16 otrzymuje brzmienie:

„16) udział w sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz ENISA;”,

– dodaje się pkt 17–22 w brzmieniu:

„17) gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych;

18) przygotowywanie na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych;

19) przygotowywanie na zlecenie Pełnomocnika analiz skutków incydentów i incydentów telekomunikacyjnych oraz analiz przebiegu obsługi incydentów i incydentów telekomunikacyjnych;

20) przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa;

21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, przez:
   a) wykonywanie oceny bezpieczeństwa,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach;
22) udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRT MON, CSIRT NASK lub CSIRT GOV, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.”,

e) ust. 4 otrzymuje brzmienie:

„4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu lub incydentu telekomunikacyjnego, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określą we współpracy z CSIRT sektorowymi, CSIRT Telco i CSIRT INT sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu lub incydentu telekomunikacyjnego.”,

f) w ust. 5
   – wprowadzenie do wyliczenia otrzymuje brzmienie:
   „Do zadań CSIRT MON należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”,
   – w pkt 2 wyrazy „przedsiębiorcy realizujący zadania na rzecz Sił Zbrojnych” zastępuje się wyrazami „przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych”,

g) w ust. 6:
   – w pkt 1:
      – – wprowadzenie do wyliczenia otrzymuje brzmienie:
      „koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”,
      – – lit. a otrzymuje brzmienie:
      „a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6 i 10 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”,

– – lit. c otrzymuje brzmienie:

„c) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce,”,

– po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) koordynacja obsługi incydentów telekomunikacyjnych zgłaszanych przez przedsiębiorców komunikacji elektronicznej, z wyjątkiem incydentów telekomunikacyjnych zgłaszanych przez podmioty wskazane w ust. 5 i 7,”,

h) w ust. 7:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„Do zadań CSIRT GOV należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”;

– po pkt 4 dodaje się pkt 4a–4c w brzmieniu:

„4a) Państwowe Gospodarstwo Wodne Wody Polskie;

4b) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju;

4c) Urząd Komisji Nadzoru Finansowego;”,

i) w ust. 8 wyrazy „zgłoszenie incydentu” zastępuje się wyrazami „zgłoszenie incydentu lub incydentu telekomunikacyjnego”,

j) ust. 9 otrzymuje brzmienie:

„9. Działalność bieżąca CSIRT NASK jest finansowana w formie dotacji podmiotowej ze środków, których dysponentem jest minister właściwy do spraw informatyzacji.”,

k) po ust. 9 dodaje się ust. 9a w brzmieniu:

„9a. Rozbudowa i modernizacja infrastruktury teleinformatycznej CSIRT NASK służącej realizacji jego zadań może być dofinansowana w formie dotacji celowej ze środków budżetu państwa, których dysponentem jest minister właściwy do spraw informatyzacji.”,

l) w ust. 11 we wprowadzeniu do wyliczenia wyrazy „Ministra Cyfryzacji” zastępuje się wyrazami „ministra właściwego do spraw informatyzacji”,

m) dodaje się ust. 12 w brzmieniu:

„12. Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy do spraw informatyzacji informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w ust. 10. Pełnomocnik

udostępnia komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”;

26) w art. 31:

a) po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w art. 20d ust. 1 pkt 2, a także uzgodnią sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji – w przypadku braku możliwości dokonania zgłoszenia albo przekazania tych informacji w postaci elektronicznej.”,

b) ust. 2 otrzymuje brzmienie:

„2. Komunikat zawierający informacje, o których mowa w ust. 1 i 1a, CSIRT MON, CSIRT NASK i CSIRT GOV udostępnia na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego. Komunikat podlega również udostępnieniu w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.”;

27) w art. 32 ust. 4 otrzymuje brzmienie:

„4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy lub CSIRT Telco na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotów krajowego systemu cyberbezpieczeństwa, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”;

28) w art. 33:

a) po ust. 1 dodaje się ust. 1a–1e w brzmieniu:

„1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT.

1b. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, jest uprawniony do stosowania technik mających na celu: obserwację i analizę pracy urządzenia lub oprogramowania, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja)

jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez urządzenie informatyczne lub oprogramowanie.

1c. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, o którym mowa w ust. 1, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, badanych urządzeń i oprogramowania, które ograniczyłyby możliwość przeprowadzenia badania.

1d. Badanie, o którym mowa w ust. 1:

1) nie narusza autorskich praw osobistych oraz majątkowych, oraz
2) nie wymaga zgody licencjodawcy lub dysponenta urządzenia informatycznego, oprogramowania lub usługi cyfrowej.

1e. Postanowienia umów sprzeczne z art. 33 ust. 1–1d są nieważne.”,

b) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie urządzenia informatycznego lub oprogramowania, informuje pozostałe CSIRT poziomu krajowego o fakcie podjęcia badań oraz o urządzeniu informatycznym lub oprogramowaniu, którego badanie dotyczy. Informacja ta może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”,

c) po ust. 4b dodaje się ust. 4c w brzmieniu:

„4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik udostępnia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”,

d) w ust. 5 wyrazy „od dnia otrzymania rekomendacji” zastępuje się wyrazami „od dnia udostępnienia rekomendacji na stronie podmiotowej w Biuletynie Informacji Publicznej”;

29) w art. 34 ust. 1 otrzymuje brzmienie:

„1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy, CSIRT Telco oraz SOC zewnętrzne współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”;

30) po art. 34 dodaje się art. 34a i art. 34b w brzmieniu:

„Art. 34a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco przekazują informacje o incydentach telekomunikacyjnych Prezesowi UKE w celu realizacji obowiązków, o których mowa w art. 20h ust. 1 pkt 1.

2. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco raz na pół roku przygotowują sprawozdania dotyczące liczby i rodzajów poważnych incydentów telekomunikacyjnych, które przekazują Prezesowi UKE oraz Pełnomocnikowi.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają z Prezesem UKE sposób i tryb przekazywania informacji, o których mowa w ust. 1.

Art. 34b. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują z Prezesem UKE oraz CSIRT Telco przy wykonywaniu ustawowych zadań.”;

31) w art. 35 ust. 5 otrzymuje brzmienie:

„5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać Pełnomocnikowi do udostępnienia na jego stronie podmiotowej w Biuletynie Informacji Publicznej informacje o podatnościach, incydentach krytycznych oraz o cyberzagrożeniach:

1) jeżeli przekazywanie tych informacji przyczyni się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów;
2) wyłącznie w zakresie niezbędnym do realizacji tych celów, oraz
3) jeżeli publikacja informacji nie będzie naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.”;

32) w art. 36:

a) ust. 2 otrzymuje brzmienie:

„2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Pełnomocnika, ministra właściwego do spraw informatyzacji oraz Rządowego Centrum Bezpieczeństwa.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. W posiedzeniach Zespołu może uczestniczyć Pełnomocnik.”,

c) w ust. 6 zdanie pierwsze otrzymuje brzmienie:

„Dyrektor Rządowego Centrum Bezpieczeństwa na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1,

zawiadamia niezwłocznie członków Zespołu i Pełnomocnika o terminie i miejscu posiedzenia Zespołu.”;

33) po art. 36 dodaje się art. 36a w brzmieniu:

„Art. 36a. W przypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;

34) po rozdziale 6 dodaje się rozdział 6a i 6b w brzmieniu:

„Rozdział 6a

Zadania CSIRT INT

Art. 36b. 1. Do zadań CSIRT INT należy zapewnianie wsparcia w obsłudze incydentów zgłaszanych przez:

1) jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
2) Agencję Wywiadu.

2. W zakresie określonym w ust. 1 CSIRT INT współpracuje z CSIRT GOV.

3. Do zadań CSIRT INT w ramach wspierania podmiotów określonych w ust. 1 należy:

1) przyjmowanie zgłoszeń o incydentach w podmiotach publicznych;
2) reagowanie na incydenty w podmiotach publicznych;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo w podmiotach publicznych;
4) współpraca z podmiotami publicznymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;

5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty w podmiotach publicznych oraz wymiany informacji o cyberzagrożeniach;
6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie podnoszenia świadomości cyberzagrożeń;
7) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów, o których mowa w ust. 1, w szczególności przez:
   a) wykonywanie testów bezpieczeństwa w porozumieniu z podmiotami, o których mowa w ust. 1,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

Art. 36c. CSIRT INT niezwłocznie, nie później niż w ciągu 8 godzin, przekazuje zgłoszenie, o którym mowa w art. 22 ust. 1a, do CSIRT GOV.

Rozdział 6b

Ocena bezpieczeństwa

Art. 36d. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy lub CSIRT Telco mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.

2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu.

3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych:

1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów, o których mowa w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2023 r. poz. 1136);
2) akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych.

4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest:

1) w przypadku podmiotów, o których mowa w art. 26 ust. 5 – CSIRT MON;

2) w przypadku podmiotów, o których mowa w art. 26 ust. 6 pkt 1 lit. a–k i pkt 1a – CSIRT NASK;

3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4 – CSIRT GOV.

5. CSIRT MON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa.

6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej za zgodą właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego operatora usługi kluczowej CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora.

7. CSIRT INT może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu, o którym mowa w art. 36b ust. 1, za zgodą CSIRT GOV.

8. CSIRT Telco może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego przedsiębiorcy komunikacji elektronicznej za zgodą właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego przedsiębiorcy komunikacji elektronicznej CSIRT Telco informuje Prezesa UKE.

Art. 36e. 1. Ocena bezpieczeństwa może być przeprowadzona za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w formie pisemnej lub elektronicznej pod rygorem nieważności.

2. Ocena bezpieczeństwa powinna być prowadzona z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie.

3. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa.

4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe,

o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2022 r. poz. 1138, z późn. zm.[3)]), oraz ich używać w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

5. Używając urządzeń lub programów komputerowych, o których mowa w ust. 4, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może uzyskać dostęp do informacji dla niej nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, lub może uzyskać dostęp do całości lub części systemu informacyjnego.

6. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco w wyniku przeprowadzania oceny bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe i CSIRT Telco oraz podlegają one niezwłocznemu zniszczeniu, które przeprowadza komisja i które dokumentuje się protokołem zniszczenia tych informacji.

7. Po przeprowadzeniu oceny bezpieczeństwa CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco sporządza i przekazuje podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego.

Art. 36f. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy albo CSIRT Telco informuje niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych.

Art. 36g. Rada Ministrów może określić, w drodze rozporządzenia, sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36e ust. 6, i tryb działania komisji, a także wzór protokołu, mając na uwadze rodzaj materiałów podlegających zniszczeniu.”;

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 1726, 1855, 2339 i 2600 oraz z 2023 r. poz. 289, 818 i 852.

35) w art. 37 ust. 1–3 otrzymują brzmienie:

„1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641 oraz z 2022 r. poz. 1700).

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent operatorem usługi kluczowej, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach istotnych lub wystąpić do organu właściwego do spraw cyberbezpieczeństwa dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu, albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.”;

36) w art. 39:

a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco przetwarzają dane pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami”,

b) użyte w ust. 2 oraz w ust. 5–8 i ust. 9 we wprowadzeniu do wyliczenia w różnej liczbie i w różnym przypadku wyrazy „i sektorowe zespoły cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy i CSIRT Telco”,

c) w ust. 3:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe i CSIRT Telco przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami:”,

– pkt 2 otrzymuje brzmienie:

„2) dotyczące telekomunikacyjnych urządzeń końcowych;”,

– w pkt 4 kropkę zastępuje się średnikiem i dodaje się pkt 5 w brzmieniu:

„5) gromadzone przez przedsiębiorców komunikacji elektronicznej w związku ze świadczeniem usług komunikacji elektronicznej.”,

d) w ust. 4:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes UKE przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami:”,

– w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) gromadzone przez przedsiębiorców komunikacji elektronicznej.”,

e) ust. 5 i 6 otrzymują brzmienie:

„5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8, art. 36b, art. 36c, art. 44 ust. 1–3 oraz art. 44a ust. 3–5.

6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8, art. 44 ust. 1–3 oraz art. 44a ust. 3–5, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco w terminie 5 lat od zakończenia obsługi incydentu lub incydentu telekomunikacyjnego, którego dotyczą.”,

f) w ust. 7 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT, CSIRT Telco”,

g) w ust. 8 i 9 po wyrazach „CSIRT MON, CSIRT NASK” dodaje się wyrazy „CSIRT Telco”,

h) dodaje się ust. 10 w brzmieniu:

„10. Dane, o których mowa w ust. 4, są usuwane lub anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika, organy właściwe do spraw cyberbezpieczeństwa oraz Prezesa UKE niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z niniejszej ustawy.”;

37) w art. 40:

a) w ust. 1 wyrazy „CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco”,

b) w ust. 2 i 3 wyrazy „CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco”;

38) w art. 42:

a) w ust. 1:

– pkt 4 otrzymuje brzmienie:

„4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych;”,

– w pkt 5 wyrazy „CSIRT NASK, CSIRT GOV, CSIRT MON” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT INT”,

– w pkt 7 wyrazy „CSIRT NASK, CSIRT GOV lub CSIRT MON” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”,

b) w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”;

39) po art. 43 dodaje się oznaczenie rozdziału 8a i tytuł w brzmieniu:

„Rozdział 8a

CSIRT sektorowy i CSIRT Telco”;

40) w art. 44:

a) ust. 1 otrzymuje brzmienie:

„1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 do ustawy, do którego zadań należy:

1) przyjmowanie zgłoszeń o incydentach;

2) reagowanie na incydenty;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;
4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;
6) współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach;
7) współpraca z CSIRT Telco w reagowaniu na incydenty poważne, będącymi również poważnymi incydentami telekomunikacyjnymi.”,

b) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu:

„1a. CSIRT sektorowy przekazuje zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4, niezwłocznie, nie później niż 8 godzin od jego otrzymania, do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV.

1b. CSIRT sektorowy może, w szczególności:

1) zapewniać we współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń wśród operatorów usług kluczowych danego sektora lub podsektora;
2) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które ich dotyczą;
3) wspierać, w uzgodnieniu z operatorem usługi kluczowej, wykonywanie przez niego obowiązków określonych w art. 11 ust. 1–3, art. 12 i art. 13;
4) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV;

5) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w danym sektorze lub podsektorze, w szczególności przez:
   a) wykonywanie oceny bezpieczeństwa,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.”,

c) uchyla się ust. 2,

d) ust. 4 otrzymuje brzmienie:

„4. Organ właściwy do spraw cyberbezpieczeństwa informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań.”,

e) dodaje się ust. 5–11 w brzmieniu:

„5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego jednostkom jemu podległym albo przez niego nadzorowanym albo organowi przez niego nadzorowanemu.

6. Organ właściwy do spraw cyberbezpieczeństwa może, w drodze porozumienia z innym organem właściwym do spraw cyberbezpieczeństwa, wyznaczyć spośród jednostek jemu podległych albo przez niego nadzorowanych jednostkę, która będzie wykonywała zadania CSIRT sektorowego dla kilku sektorów lub podsektorów dla których ten organ jest właściwy. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu zasady odpowiedzialności za zadania oraz sprawowania nadzoru nad CSIRT sektorowym.

7. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT MON, CSIRT NASK albo CSIRT GOV realizację zadania lub zadań CSIRT sektorowego.

8. Powierzenie, o którym mowa w ust. 7, następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa:

1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego;

3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.

9. W porozumieniu, o którym mowa w ust. 8, określa się zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań, zasady odpowiedzialności oraz zasady finansowania.

10. Komunikat o zawarciu porozumienia, o którym mowa w ust. 6 lub 8, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa i wskazuje się:

1) adres strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;
2) termin, od którego porozumienie będzie obowiązywało.

11. Organ właściwy do spraw cyberbezpieczeństwa informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w ust. 6 i 8. Pełnomocnik udostępnia komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”;

41) po art. 44 dodaje się art. 44a i art. 44b w brzmieniu:

„Art. 44a. 1. Prezes UKE zapewnia funkcjonowanie CSIRT Telco.

2. Prezes UKE może powierzyć jednostce podległej lub nadzorowanej przez ministra właściwego do spraw informatyzacji prowadzenie CSIRT Telco – za zgodą tego ministra. Powierzenie następuje na podstawie porozumienia, w którym określa się zasady sprawowania przez Prezesa UKE kontroli nad prawidłowym wykonywaniem powierzonych zadań oraz zasady finansowania. Przepis art. 44 ust. 10 i 11 stosuje się odpowiednio.

3. Do zadań CSIRT Telco należy:

1) przyjmowanie zgłoszeń o incydentach telekomunikacyjnych;
2) reagowanie na incydenty telekomunikacyjne;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci i usług komunikacji elektronicznej;
4) współpraca z przedsiębiorcami komunikacji elektronicznej w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;

5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymiany informacji o cyberzagrożeniach;
6) współpraca z CSIRT sektorowymi w reagowaniu na poważne incydenty telekomunikacyjne, będące również incydentami poważnymi;
7) współpraca z organem właściwym do spraw ochrony danych osobowych podczas reagowania na incydent telekomunikacyjny, który doprowadził do naruszenia ochrony danych osobowych.

4. CSIRT Telco może, w szczególności:

1) zapewniać dynamiczną analizę ryzyka i incydentów telekomunikacyjnych oraz wspomagać podnoszenie świadomości cyberzagrożeń;
2) koordynować w uzgodnieniu z przedsiębiorcami komunikacji elektronicznej obsługę incydentów telekomunikacyjnych, które dotyczą różnych przedsiębiorców komunikacji elektronicznej;
3) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa sieci lub usług komunikacji elektronicznej przez:
   a) wykonywanie oceny bezpieczeństwa,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

5. CSIRT Telco, przekazuje zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, niezwłocznie, nie później niż 8 godzin od jego otrzymania, do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV.

6. CSIRT Telco może zwrócić się do Prezesa UKE o wezwanie przedsiębiorcy komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego.

7. CSIRT Telco udostępnia na swojej stronie internetowej i na stronie podmiotowej Biuletynu Informacji Publicznej CSIRT Telco komunikat zawierający informacje, o których mowa w art. 31 ust. 1a.

Art. 44b. 1. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego.

2. Prezes UKE raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT Telco.”;

42) w art. 45 w ust. 1 w pkt 6 w lit. c kropkę zastępuje się średnikiem i dodaje się pkt 7 w brzmieniu:

„7) prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.”;

43) w art. 46:

a) w ust. 1 w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6–8 w brzmieniu:

„6) wymianę danych kontaktowych o CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT Telco, CSIRT INT, CSIRT sektorowym, SOC, ISAC wpisanych do wykazu ISAC;

7) wymianę danych, o których mowa w art. 9 ust. 2, art. 20a ust. 4 pkt 2, art. 22 ust. 1 pkt 5;

8) przekazywanie informacji, o których mowa w art. 20c pkt 2.”,

b) ust. 2 otrzymuje brzmienie:

„2. Pełnomocnik, CSIRT MON, CSIRT NASK i CSIRT GOV korzystają z systemu teleinformatycznego, o którym mowa w ust. 1.”,

c) po ust. 2 dodaje się ust. 2a–2d w brzmieniu:

„2a. CSIRT sektorowe, CSIRT INT, CSIRT Telco, Prezes UKE korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości.

2b. Operatorzy usług kluczowych korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie niezbędnym do realizowania obowiązków, o których mowa w rozdziale 3.

2c. Szczegółowe zasady korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, określa porozumienie zawarte pomiędzy ministrem właściwym do spraw informatyzacji, a podmiotem, o którym mowa w ust. 2–2b.

2d. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2–2b, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”;

44) po art. 47 dodaje się art. 47a w brzmieniu:

„Art. 47a. 1. Narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2022 r. poz. 498), z chwilą przekazania staje się własnością osoby, która je otrzymała.

2. Określone w ust. 1 nabycie narzędzia do uwierzytelnienia dwuskładnikowego nie rodzi zobowiązań podatkowych, z wyjątkiem ewentualnych zobowiązań z tytułu podatku od towarów i usług.”;

45) w art. 48 w pkt 1 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT”;

46) użyte w art. 49 w ust. 3 w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”;

47) w art. 51:

a) pkt 5 otrzymuje brzmienie:

„5) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów, a także koordynowanie działań CSIRT NASK i CSIRT GOV w czasie stanu wojennego oraz w czasie wojny;”,

b) pkt 7 otrzymuje brzmienie:

„7) ocenę cyberzagrożeń w każdym ze stanów gotowości obronnej państwa oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;”,

c) pkt 8 otrzymuje brzmienie:

„8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego i w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia;”;

48) po art. 52 dodaje się art. 52a w brzmieniu:

„Art. 52a. W celu zabezpieczenia realizacji przewidzianych w ustawie zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, o których mowa w art. 26 ust. 1a, art. 36a, art. 42 w związku z art. 41 pkt 6, 9 i 11, art. 44 ust. 8 pkt 3, art. 51, art. 52 i art. 67c ust. 1, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły

specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.”;

49) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych, SOC zewnętrznych i przedsiębiorców komunikacji elektronicznej”;

50) w art. 53:

a) w ust. 1:

– pkt 1 otrzymuje brzmienie:

„1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi SOC zewnętrznego wymogów, o których mowa w art. 14 ust. 3–7 oraz wykonywania obowiązków, o których mowa w art. 66b i art. 66c;”,

– w pkt 2 lit. a i b otrzymują brzmienie:

„a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania cyberzagrożeniom i zgłaszania incydentów poważnych oraz wykonywania obowiązków, o których mowa w art. 66b i art. 66c,

b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych oraz wykonywania obowiązków, o których mowa w art. 66b i art. 66c;”,

– dodaje się pkt 3 w brzmieniu:

„3) Prezes UKE w zakresie wypełniania przez przedsiębiorców komunikacji elektronicznej obowiązków określonych w art. 20a ust. 2 i 3, art. 20b ust. 2 i 4, art. 20d ust. 1 i art. 20f oraz wykonywania obowiązków, o których mowa w art. 66b i art. 66c.”,

b) w ust. 2 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:

„3) Prezes UKE prowadzi kontrole w zakresie, o którym mowa w ust. 1 w pkt 3, oraz nakłada kary pieniężne na przedsiębiorców komunikacji elektronicznej.”;

51) w art. 54 dodaje się ust. 3 w brzmieniu:

„3. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 3, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.”;

52) po art. 54 dodaje się art. 54a w brzmieniu:

„Art. 54a. Prezes UKE może, po otrzymaniu wniosku od CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco, wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego.”;

53) w art. 56 dodaje się ust. 3 w brzmieniu:

„3. Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt.”;

54) art. 59 otrzymuje brzmienie:

„Art. 59. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy do spraw cyberbezpieczeństwa, minister właściwy do spraw informatyzacji lub Prezes UKE uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje temu podmiotowi zalecenia pokontrolne dotyczące usunięcia nieprawidłowości.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy do spraw cyberbezpieczeństwa, ministra właściwego do spraw informatyzacji lub Prezesa UKE o sposobie wykonania zaleceń.”;

55) po rozdziale 11 dodaje się rozdział 11a w brzmieniu:

„Rozdział 11a

Krajowy system certyfikacji cyberbezpieczeństwa

Art. 59a. 1. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:

1) ministra właściwego do spraw informatyzacji;
2) Polskie Centrum Akredytacji;
3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;
4) dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje wyroby ocenie zgodności zgodnie z ustawą.

2. Nadzór nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa sprawuje minister właściwy do spraw informatyzacji.

Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa;
2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, stosowania przepisów rozporządzenia 2019/881 oraz postanowień krajowych lub europejskich programów certyfikacji cyberbezpieczeństwa;
3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59a ust. 1 pkt 3 i 4;
4) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;
5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;
6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania wysoki;
7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania wysoki;
8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;
9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa innych państw członkowskich lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymaganiami rozporządzenia 2019/881 lub z wymaganiami określonymi europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa;
10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa;

11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;
12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b–d oraz ust. 8 rozporządzenia 2019/881;
13) uczestniczenie w pracach ECCG;
14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;
15) nadzorowanie i egzekwowanie zawartych w europejskim programie certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymaganiami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;
16) przeprowadzanie badań certyfikowanych produktów ICT, usług ICT lub procesów ICT.

Art. 59c. Polskie Centrum Akredytacji sprawuje nadzór w zakresie udzielonej akredytacji nad akredytowanymi jednostkami prowadzącymi ocenę zgodności produktów ICT, usług ICT lub procesów ICT w obszarze cyberbezpieczeństwa, przy uwzględnieniu wymagań, o których mowa w art. 22 ust. 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) oraz wymagań określonych w:

1) załączniku do rozporządzenia 2019/881;
2) poszczególnych europejskich programach certyfikacji cyberbezpieczeństwa lub krajowych programach certyfikacji cyberbezpieczeństwa.

Art. 59d. 1. Minister właściwy do spraw informatyzacji może, na podstawie umowy, zlecić podmiotom dysponującym wiedzą i kompetencjami w zakresie technologii produktów ICT, usług ICT lub procesów ICT, przygotowanie projektów, dokumentacji, opinii, ekspertyz i analiz dla tych produktów ICT, usług ICT lub procesów ICT.

2. Rada Ministrów może określić, w drodze rozporządzenia, krajowy program certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT, zawierający:

1) wskazanie, czy w ramach programu jest dozwolone wydanie deklaracji zgodności,
2) dokumentację techniczną i sposób jej przechowywania,

3) treść i wzór graficzny krajowych certyfikatów cyberbezpieczeństwa i krajowych deklaracji zgodności okres dostępności krajowych deklaracji zgodności, dokumentacji technicznej oraz innych istotnych informacji,
4) szczegółowe wymagania z zakresu cyberbezpieczeństwa odpowiadające poszczególnym krajowym poziomom uzasadnienia zaufania,
5) szczegółowe metody stosowane w celu wykazania, że zostały spełnione wymagania odpowiadające określonemu krajowemu poziomowi uzasadnienia zaufania,
6) sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymaganiami krajowych certyfikatów cyberbezpieczeństwa lub deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymaganiami cyberbezpieczeństwa,
7) warunki wydawania, utrzymywania, przedłużania i odnawiania ważności certyfikatów

– biorąc pod uwagę rodzaje produktów ICT, usług ICT lub procesów ICT oraz stopień cyberzagrożeń, jakie dotyczą tych produktów ICT, usług ICT lub procesów ICT.

Art. 59e. Dostawca ubiegający się o uzyskanie certyfikatu lub dostawca certyfikowanych produktów ICT, usług ICT lub procesów ICT jest obowiązany dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność wszystkie informacje niezbędne do oceny czy określony produkt ICT, usługa ICT lub proces ICT spełnia wymagania określone w europejskim lub krajowym programie certyfikacji cyberbezpieczeństwa.

Art. 59f. 1. Krajowy program certyfikacji cyberbezpieczeństwa wskazuje jeden lub więcej krajowych poziomów uzasadnienia zaufania produktów ICT, usług ICT lub procesów ICT.

2. Krajowy poziom uzasadnienia zaufania określa się jako:

1) podstawowy – co potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa lub wydana została krajowa deklaracja zgodności, spełniają odpowiadające im wymagania bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków;
2) istotny – co potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające

mu wymagania bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk wystąpienia incydentów i cyberataków przeprowadzanych przez osoby dysponujące niezaawansowanym sprzętem oraz podstawowymi umiejętnościami w zakresie przełamywania zabezpieczeń systemów informacyjnych;

3) wysoki – co potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymagania bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach w zakresie przełamywania zabezpieczeń systemów informacyjnych lub dysponujące zawansowanym sprzętem.

3. Metody stosowane w ramach oceny danego produktu ICT, usługi ICT lub procesu ICT obejmują:

1) w przypadku krajowego poziomu uzasadnienia zaufania „podstawowy” – przegląd dokumentacji technicznej lub działania o równoważnym skutku;

2) w przypadku krajowego poziomu uzasadnienia zaufania „istotny” – sprawdzenie tego produktu ICT, usługi ICT lub procesu ICT w celu wykazania, że nie występują powszechnie znane podatności oraz testowanie w celu wykazania, że w produkcie ICT, usłudze ICT lub procesie ICT prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa lub działania o równoważnym skutku;

3) w przypadku krajowego poziomu uzasadnienia zaufania „wysoki” – sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, testowanie, czy w produkcie ICT, usłudze ICT lub procesie ICT prawidłowo zaimplementowane zostały niezbędne, nowoczesne funkcjonalności bezpieczeństwa oraz ocenę sprawdzającą za pomocą testów penetracyjnych ich odporność na zaawansowane atak lub działania o równoważnym skutku.

Art. 59g. Produkt ICT, usługa ICT lub proces ICT dla którego wydano certyfikat odwołujący się do krajowego poziomu uzasadnienia zaufania lub sporządzono deklarację zgodności odwołującą się do krajowego poziomu uzasadnienia zaufania spełnia wymagania określone w odpowiednim krajowym programie cyberbezpieczeństwa, pozwalające stwierdzić, że dany produkt ICT, usługa ICT lub proces ICT zapewnia ochronę przed cyberzagrożeniami i cyberatakami na odpowiednim poziomie.

Art. 59h. 1. Oceny zgodności w obszarze cyberbezpieczeństwa dokonuje jednostka oceniająca zgodność akredytowana z uwzględnieniem wymagań określonych w art. 59c posiadająca akredytację obejmującą ocenę zgodności produktu ICT, usługi ICT lub procesu ICT, w obszarze cyberbezpieczeństwa.

2. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji.

3. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.

4. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych programów certyfikacji cyberbezpieczeństwa i europejskich programów certyfikacji cyberbezpieczeństwa.

5. Informacja o udzielonej akredytacji, o której mowa w ust. 2, zawiera:

1) oznaczenie podmiotu, któremu udzielono akredytacji;
2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.

6. Akredytacji udziela się na okres nie dłuższy niż 5 lat.

7. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu akredytacji jednostce oceniającej zgodność.

8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera:

1) oznaczenie podmiotu, któremu cofnięto akredytację;
2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;
3) datę cofnięcia akredytacji.

Art. 59i. 1. W przypadku, gdy europejski program certyfikacji cyberbezpieczeństwa określa szczegółowe lub dodatkowe wymagania, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, czynności w ramach oceny zgodności dokonywanej na jego podstawie wykonuje tylko jednostka oceniająca zgodność posiadająca zezwolenie ministra właściwego do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie przez jednostkę oceniającą zgodność zadań w ramach programów certyfikacji cyberbezpieczeństwa, o których mowa w ust. 1, na wniosek jednostki oceniającej zgodność, która spełniła wymagania określone w tych programach.

3. Minister właściwy do spraw informatyzacji może z urzędu cofnąć albo zawiesić zezwolenie, o którym mowa w ust. 2, jeżeli podmiot naruszył postanowienia ustawy,

rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa. Cofnięcie albo zawieszenie zezwolenia następuje w drodze decyzji.

4. Decyzję o zawieszeniu zezwolenia wydaje się na czas określony, nie dłuższy niż 2 lat.

5. W przypadku przywrócenia zgodności z postanowieniami ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu zezwolenia.

6. Minister właściwy do spraw informatyzacji cofa zezwolenie, jeżeli upłynął okres, na który wydano decyzję, o której mowa w ust. 4, a naruszenie postanowień ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa, nie ustało.

7. Do postępowań, o których mowa w ust. 3, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 59j. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności na wniosek dostawcy.

2. Metody przeprowadzania oceny zgodności określają europejskie programy certyfikacji cyberbezpieczeństwa lub krajowe programy certyfikacji cyberbezpieczeństwa.

3. Pozytywny wynik oceny zgodności stanowi podstawę do wydania certyfikatu.

Art. 59k. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem:

1) deklaracji zgodności – badaniom przez dostawcę sprzętu lub oprogramowania, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy;
2) certyfikatu – ocenie zgodności przez jednostkę oceniającą zgodność, w zakresie właściwym do danego programu certyfikacji cyberbezpieczeństwa.

Art. 59l. 1. Dostawca składa wniosek o certyfikację produktu ICT, usługi ICT lub procesu ICT do jednostki oceniającej zgodność.

2. Wniosek o certyfikację zawiera co najmniej:

1) nazwę albo imię i nazwisko wnioskującego oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;
2) informacje potwierdzające spełnianie wymagań krajowego lub europejskiego programu certyfikacji cyberbezpieczeństwa;

3) wskazanie zakresu certyfikacji.

3. Do wniosku dołącza się dokumenty potwierdzające spełnienie wymagań określonych we właściwym programie certyfikacji.

4. Wniosek składa się na piśmie utrwalonym w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

Art. 59m. Jednostka oceniająca zgodność niezwłocznie przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, dane podmiotu, któremu cofnięto certyfikat wraz ze wskazaniem przyczyny jego cofnięcia albo dane podmiotu, któremu odmówiono wydania certyfikatu wraz ze wskazaniem przyczyn odmowy.

Art. 59n. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji niezwłocznie przesyła, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285) do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:

1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania wysoki;
2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania wysoki.

2. Minister właściwy do spraw informatyzacji:

1) zatwierdza certyfikat, o którym mowa w ust. 1;
2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą, rozporządzeniem 2019/881 lub programami, o których mowa w ust. 1.

3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się, jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.

4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg oceny zgodności.

5. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy może zasięgnąć opinii instytutu badawczego nadzorowanego przez tego ministra w zakresie

zgodności certyfikacji z krajowym lub europejskim programem certyfikacji cyberbezpieczeństwa. Instytut badawczy przekazuje opinię w terminie 1 miesiąca od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

6. Minister właściwy do spraw informatyzacji cofa certyfikat, jeżeli jest on niezgodny z ustawą, rozporządzeniem 2019/881, europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa.

7. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

Art. 59o. W przypadku stwierdzenia, że podmiot ubiegający się o uzyskanie certyfikatu nie realizuje obowiązku określonego w art. 59e, jednostka oceniająca zgodność odmawia dokonania oceny zgodności.

Art. 59p. 1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) oznaczenie produktu ICT, usługi ICT lub procesu ICT podlegającego certyfikacji;
4) numer lub oznaczenie certyfikatu;
5) zakres certyfikacji;
6) okres, na jaki został wydany certyfikat;
7) wskazanie poziomu uzasadnienia zaufania określonego w europejskim programie certyfikacji cyberbezpieczeństwa lub krajowego poziomu uzasadnienia zaufania określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
8) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

3. Okres ważności krajowych certyfikatów cyberbezpieczeństwa jest określany na podstawie charakterystyki specyfikacji technicznej dla konkretnego produktu ICT, usługi ICT lub procesu ICT.

Art. 59q. 1. W okresie, na jaki został wydany certyfikat produkt ICT, usługa ICT lub proces ICT dla którego go wydano, ma spełniać wymagania obowiązujące na dzień jego wydania.

2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że produkt ICT, usługa ICT lub proces ICT, dla którego wydano certyfikat, nie spełnia lub przestał spełniać wymagania.

3. Jednostka oceniająca zgodność informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Art. 59r. 1. Jednostka oceniająca zgodność monitoruje spełnienie wymagań przez produkt ICT, usługę ICT lub proces ICT przez cały okres na jaki został wydany certyfikat.

2. Dostawca udostępnia na wniosek jednostki oceniającej zgodność, która wydała certyfikat, wszystkie informacje niezbędne do oceny czy produkt ICT, usługa ICT lub proces ICT spełnia wymagania określone w krajowym programie certyfikacji w terminie wskazanym przez jednostkę oceniającą zgodność nie krótszym niż 30 dni.

3. W przypadku, gdy dostawca nie przedstawił żądanych informacji w terminie wskazanym w ust. 2, jednostka oceniająca zgodność może cofnąć wydany certyfikat.

4. W przypadku, gdy jednostka oceniająca zgodność stwierdziła, że produkt ICT, usługa ICT lub proces ICT przestał spełniać wymagania, jednostka oceniająca zgodność cofa certyfikat.

Art. 59s. 1. W przypadku, gdy produkt ICT, usługa ICT lub proces ICT po uzyskaniu certyfikatu przestały spełniać wymagania określone w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, jego dostawca niezwłocznie przekazuje informacje o tym jednostce oceniającej zgodność, która wydała certyfikat wraz z informacją o planowanych działaniach mających na celu przywrócenie zgodności z wymaganiami oraz terminem ich realizacji nie dłuższym niż 2 miesiące.

2. W okresie, o którym mowa w ust. 1, dostawca nie może powoływać się na posiadanie certyfikatu dla produktu ICT, usługi ICT lub procesu ICT, który przestał spełniać wymagania.

3. W przypadku, gdy w określonym terminie zgodność z wymaganiami nie została przywrócona, jednostka oceniająca zgodność cofa certyfikat.

Art. 59t. 1. Dostawca, który poddał produkt ICT, usługę ICT lub proces ICT ocenie zgodności z wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa i stwierdził ich spełnienie, może sporządzić krajową deklarację zgodności.

2. Krajowa deklaracja zgodności zawiera co najmniej:

1) nazwę podmiotu, który sporządził deklarację;
2) okres, na jaki została wydana deklaracja;
3) wskazanie krajowego programu certyfikacji cyberbezpieczeństwa w ramach którego została wydana deklaracja;
4) wskazanie wymagań zawartych w krajowym programie certyfikacji cyberbezpieczeństwa, które spełnia produkt ICT, usługa ICT lub proces ICT;
5) wskazanie metod, jakie zostały zastosowane dla stwierdzenia, że wymagania, o których mowa w pkt 4, zostały spełnione;
6) datę wydania i podpis podmiotu, który sporządził deklarację.

3. Przez sporządzenie i podpisanie deklaracji zgodności dostawca przyjmuje na siebie odpowiedzialność za zgodność wyrobu z wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa.

4. Krajowa deklaracja zgodności odwołuje się do określonych w krajowym programie certyfikacji cyberbezpieczeństwa wymagań oraz metod stosowanych w celu wykazania, że zostały spełnione wymagania odpowiadające określonemu krajowemu poziomowi uzasadnienia zaufania.

5. Przez cały okres na jaki została wydana deklaracja zgodności produkt ICT, usługa ICT lub proces ICT spełniają wymagania określone w krajowym programie certyfikacji cyberbezpieczeństwa.

6. Krajowa deklaracja zgodności wydawana jest wyłącznie dla produktów ICT, usług ICT lub procesów ICT odpowiadających wymaganiom dla krajowego poziomu uzasadnienia zaufania „podstawowy”.

Art. 59u. Po wydaniu deklaracji zgodności dostawca niezwłocznie przesyła jej kopię ministrowi właściwemu do spraw informatyzacji na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Art. 59v. Domniemywa się, że produkt ICT, usługa ICT lub proces ICT, dla którego wydano deklarację zgodności, jest zgodny z wymaganiami określonymi w obowiązujących krajowych programach certyfikacji cyberbezpieczeństwa lub europejskich programach certyfikacji cyberbezpieczeństwa.

Art. 59w. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa produktów ICT, usług ICT lub procesów ICT lub

dla których została wydana krajowa deklaracja zgodności, udostępnia publicznie informacje zawierające:

1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT;
2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;
3) informacje o danych kontaktowych wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;
4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatności związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności.

Art. 59x. Na wniosek ministra właściwego do spraw informatyzacji podmiot, o którym mowa w art. 59a ust. 1 pkt 3 i 4, przedstawia informacje dotyczące:

1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;
2) funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa;
3) liczby wydanych certyfikatów, w tym programów, w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;
4) liczby wydanych deklaracji zgodności, w tym programów, w ramach których zostały wydane.

Art. 59y. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59a ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.

2. Do kontroli, o której mowa w ust. 1, przeprowadzonej wobec podmiotów:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców;

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

Art. 59z. Do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa stosuje się przepisy art. 55–59.

Art. 59za. Minister właściwy do spraw informatyzacji w ramach przeprowadzanej kontroli może poddać produkt ICT, usługę ICT lub proces ICT, dla których został wydany certyfikat lub deklaracja zgodności, badaniom lub zlecić ich przeprowadzenie, w celu ustalenia, czy spełniają one wymagania określone w ustawie, rozporządzeniu 2019/881, krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa.

Art. 59zb. 1. Badanie, o którym mowa w art. 59za, może zostać przeprowadzone na próbkach produktu ICT.

2. Podmiot kontrolowany jest obowiązany do przekazania osobom prowadzącym czynności kontrolne wskazanej przez nie próbki produktu ICT. Z przekazania próbki sporządza się protokół.

3. Protokół zawiera nazwę produktu ICT, oznaczenie certyfikatu wydanego dla tego produktu ICT lub deklaracji zgodności wydanej dla tego produktu ICT, wielkość próbki przekazanej do badania, dane identyfikujące produkt ICT, takie jak numer seryjny przekazanego jako próbka egzemplarza produktu ICT oraz datę przekazania próbki.

4. Jeżeli przeprowadzone badania wykazały, że produkt ICT nie spełnia wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości informację o niespełnianiu przez produkt ICT wymagań określonych w programie certyfikacji.

5. W przypadku certyfikatów zatwierdzanych przez ministra właściwego do spraw informatyzacji, minister właściwy do spraw informatyzacji uchyla decyzję o zatwierdzeniu certyfikatu.

6. Koszty badań, o których mowa w art. 59za, ponosi podmiot kontrolowany.

7. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, wzór protokołu, o którym mowa w ust. 3, kierując się potrzebą zapewnienia możliwości identyfikacji próbki produktu ICT oraz jednolitości i przejrzystości protokołów.

Art. 59zc. 1. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że produkt ICT nie spełnia wymagań określonych w ustawie, rozporządzeniu 2019/881,

w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa informuje o tym podmiot, który wydał dany certyfikat.

2. Minister właściwy do spraw informatyzacji może cofnąć certyfikat w przypadku stwierdzenia, że produkt ICT, dla którego został wydany certyfikat odwołujący się do poziomu zaufania wysoki określony w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa.

Art. 59zd. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:

1) podmiot, który wydał europejską lub krajową deklarację zgodności, jeżeli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja dotyczy nie spełnia wymagań określonych w programie certyfikacji cyberbezpieczeństwa;
2) jednostkę oceniającą zgodność.

2. Minister właściwy do spraw informatyzacji rozpatruje skargi, o których mowa w ust. 1, w sposób i na zasadach określonych w programie certyfikacji cyberbezpieczeństwa, a w przypadku jeżeli program nie określa sposobu i zasad rozpatrywania skarg stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.”;

56) w art. 62 w ust. 1:
   a) w pkt 1 i 2 wyrazy „CSIRT MON, CSIRT NASK i CSIRT GOV” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT i CSIRT sektorowy”,
   b) w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 i 8 w brzmieniu:
      „7) wydawanie ostrzeżeń, o których mowa w art. 67a ustawy;
      8) zlecenie zapewnienia wsparcia, o którym mowa w art. 26 ust. 2a.”;
57) po art. 62 dodaje się art. 62a w brzmieniu:

„Art. 62a. 1. Pełnomocnik może wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

2. Rekomendacje Pełnomocnika są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. Podmiot krajowego systemu cyberbezpieczeństwa, do którego zostały skierowane rekomendacje uwzględnia je w zarządzaniu ryzykiem.”;

58) art. 64 otrzymuje brzmienie:

„Art. 64. Przy Radzie Ministrów działa Kolegium, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, CSIRT Telco, CSIRT INT, Prezesa UKE i organów właściwych do spraw cyberbezpieczeństwa.”;

59) po art. 64 dodaje się art. 64a w brzmieniu:

„Art. 64a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 66a ust. 2, sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT.

3. Zadania, o których mowa w ust. 1 i 2, są wykonywane w ramach ustawowych zadań odpowiednio CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT.”;

60) w art. 65:

a) w ust. 1:

– pkt 1a otrzymuje brzmienie:

„1a) planowanych do ustalenia przez Prezesa UKE w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 110 ust. 2 ustawy z dnia …– Prawo komunikacji elektronicznej, jeżeli ta decyzja jest wydawana po przeprowadzeniu aukcji, o której mowa w art. 104 ust. 3 pkt 2 ustawy z dnia …. – Prawo komunikacji elektronicznej;”,

– pkt 2 otrzymuje brzmienie:

„2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT

GOV, CSIRT sektorowe, CSIRT Telco, CSIRT INT, i organy właściwe do spraw cyberbezpieczeństwa powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania cyberzagrożeniom;”,

– pkt 4 otrzymuje brzmienie:

„4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, CSIRT Telco, CSIRT INT i organów właściwych do spraw cyberbezpieczeństwa;”,

– w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 i 9 w brzmieniu:

„8) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka;

9) wyznaczenia operatora strategicznej sieci bezpieczeństwa.”,

b) w ust. 2 przed wyrazami „Rady Ministrów” dodaje się wyraz „Prezesa”,

c) dodaje się ust. 3 w brzmieniu:

„3. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”;

61) w art. 66:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) członkowie Kolegium:

a) minister właściwy do spraw wewnętrznych,

b) minister właściwy do spraw informatyzacji,

c) minister właściwy do spraw energii,

d) Minister Obrony Narodowej,

e) minister właściwy do spraw zagranicznych,

f) Szef Kancelarii Prezesa Rady Ministrów,

g) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,

h) minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności

służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego.”,

b) ust. 4 otrzymuje brzmienie:

„4. W posiedzeniach Kolegium uczestniczą również:

1) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;
2) Dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;
3) Prokurator Generalny albo jego zastępca;
4) Przewodniczący Komisji Nadzoru Finansowego;
5) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;
6) Szef Agencji Wywiadu albo jego zastępca;
7) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;
8) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;
9) Szef Służby Wywiadu Wojskowego albo jego zastępca;
10) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego albo jego zastępca.”,

c) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3–8 w brzmieniu:

„3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;
4) może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;
5) może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;
6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1;
7) powołuje zespół opiniujący, o którym mowa w art. 66a ust. 12 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład;
8) rozstrzyga spór, o którym mowa w art. 66a ust. 12 pkt 2, wskazując właściwego członka zespołu opiniującego.”,

d) w ust. 7 po wyrazach „CSIRT NASK,” dodaje się wyrazy „CSIRT INT”,

e) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:

„7a. Sekretarz Kolegium może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 6. Zastępcę sekretarza Kolegium odwołuje sekretarz Kolegium.

7b. W przypadku nieobecności Sekretarza Kolegium jego obowiązki wykonuje zastępca sekretarza Kolegium, w tym zastępuje go na posiedzeniu Kolegium.”;

62) po art. 66 dodaje się art. 66a–66e w brzmieniu:

„Art. 66a. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium postępowanie w sprawie uznania dostawcy produktów ICT, usług ICT lub procesów ICT, zwanego dalej „dostawcą sprzętu lub oprogramowania”, które są wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 1 i 2 oraz 3–20,

2) przedsiębiorców komunikacji elektronicznej obowiązanych posiadać aktualne i uzgodnione oraz wprowadzone do stosowania plany działań w sytuacji szczególnego zagrożenia,

3) właścicieli lub posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

– za dostawcę wysokiego ryzyka.

2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się, jeżeli ustawa nie stanowi inaczej, przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.

3. Stroną postępowania w sprawie uznania za dostawcę wysokiego ryzyka jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.

4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek na prawach strony, przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności

przeciętnego wynagrodzenia w gospodarce narodowej wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504, 1504 i 2461). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.

5. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania.

6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie udostępnia się także w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, niezwłocznie po doręczeniu tego zawiadomienia.

7. Jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania.

8. Przed rozstrzygnięciem sprawy minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

9. Opinia, o której mowa w ust. 8, zawiera analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;

2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:
   a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,
   b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności w przypadku, gdy nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,
   c) struktury własnościowej dostawcy sprzętu lub oprogramowania,
   d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;
3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.05.2019, str. 1, z późn. zm.[4)]);
4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
5) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt 1–3, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

10. Sporządzając opinię, o której mowa w ust. 8 zdanie pierwsze, Kolegium uwzględnia:

---

4) Zmiany tekstu wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 230 z 17.07.2020, str. 37, Dz. Urz. UE L 246 z 30.07.2020, str. 4, Dz. Urz. UE L 351I z 22.10.2020, str. 1, Dz. Urz. UE L 393 z 23.11.2020, str. 1 oraz Dz. Urz. UE L 114 z 12.04.2022, str. 60.

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
2) analizy, o których mowa w art. 64a ust. 1 i 2.

11. Procedura sporządzenia opinii, o której mowa w ust. 8, zdanie pierwsze przebiega w następujący sposób:

1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzą przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;
2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, które następnie przekazuje zespołowi opiniującemu. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego;
3) jeżeli nie zostały wykonane analizy, o których mowa w art. 64a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie;
4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
5) uzgodnienie opinii następuje na posiedzeniu Kolegium;
6) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

12. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.

13. Decyzja, o której mowa w ust. 12, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.

14. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 12, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

15. Decyzja, o której mowa w ust. 12, podlega natychmiastowemu wykonaniu.

16. Od decyzji, o której mowa w ust. 12, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 12, podmioty, o których mowa w art. 66a ust. 1 pkt 1–3:

1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;
2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12.

2. Przedsiębiorcy komunikacji elektronicznej obowiązani posiadać aktualne i uzgodnione plany działań oraz wprowadzone do stosowania w sytuacji szczególnego zagrożenia, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeżeli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń.

4. Podmioty, o których mowa w art. 66a ust. 1 pkt 1– 3, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, 1812, 1933 i 2185 oraz z 2023 r. poz. 412 i 825), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 12.

5. W przypadku gdy podmioty, o których mowa w art. 66a ust. 1 pkt 1–3, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej

niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 12, a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 5 lat.

Art. 66c. 1. Podmioty, o których mowa w art. 66a ust. 1 pkt 1–3, są obowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 66a ust. 12.

2. Uprawnionymi organami do uzyskania informacji, o których mowa w ust. 1, są wobec:

1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa;
2) SOC zewnętrznych – minister właściwy do spraw informatyzacji;
3) przedsiębiorców komunikacji elektronicznej – Prezes UKE;
4) podmiotów publicznych – właściwe organy nadzoru lub minister właściwy do spraw informatyzacji;
5) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym – ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialni za systemy, o których mowa w art. 3 pkt 2 tej ustawy.

3. Wniosek zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę wydania decyzji, o której mowa w art. 66a ust. 13;
3) wskazanie zakresu żądanych informacji;
4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
5) uzasadnienie;
6) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 2d.

4. Minister właściwy do spraw informatyzacji może zwrócić się do uprawnionych organów, o których mowa w ust. 2 pkt 1 lub ust. 2 pkt 3–5, aby uzyskały informacje, o których mowa w ust. 1.

5. Na wniosek ministra właściwego do spraw informatyzacji uprawniony organ, o którym mowa w ust. 2 pkt 1 lub ust. 2 pkt 3–5, przekazuje uzyskane informacje, o których mowa w ust. 1, temu ministrowi.

Art. 66d. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 66a ust. 12, na posiedzeniu niejawnym w składzie trzech sędziów.

2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.

Art. 66e. Minister właściwy do spraw informatyzacji prowadzi i udostępnia przy użyciu systemu teleinformatycznego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 66a ust. 12.”;

63) w art. 67 w ust. 1 po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) Szefa Agencji Wywiadu – w odniesieniu do działalności CSIRT INT;”;

64) po rozdziale 12 dodaje się rozdział 12a w brzmieniu:

„Rozdział 12a

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

Art. 67a. 1. W przypadku uzyskania informacji wskazującej na możliwość wystąpienia incydentu krytycznego Pełnomocnik może wydać ostrzeżenie w celu poinformowania o cyberzagrożeniu:

1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
3) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2022 poz. 2360 i 2640);
4) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.

2. Do ostrzeżenia nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Pełnomocnik, przed wydaniem ostrzeżenia, przeprowadza we współpracy z Zespołem analizę obejmującą:

1) istotność cyberzagrożenia;
2) prawdopodobieństwo wystąpienia incydentu krytycznego;
3) rodzaje ryzyk;
4) skuteczność zalecenia określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu krytycznego lub alternatywnych metod zapewnienia cyberbezpieczeństwa.

4. Ostrzeżenie zawiera:

1) określenie rodzaju lub rodzajów podmiotów wskazanych w ust. 1, będących jego adresatami;
2) zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego;
3) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 3;
4) datę wydania ostrzeżenia.

5. Pełnomocnik odwołuje ostrzeżenie po:

1) uzyskaniu informacji o ustaniu zagrożenia wystąpienia incydentu krytycznego;
2) przeprowadzaniu przeglądu i ustaleniu, że nie jest zasadne jego utrzymanie.

6. Pełnomocnik przeprowadza przegląd ostrzeżeń nie rzadziej niż raz na rok od jego wydania. W ramach przeglądu ostrzeżeń Pełnomocnik może przeprowadzić analizę, o której mowa w ust. 3.

7. Pełnomocnik udostępnia w Biuletynie Informacji Publicznej na swoje stronie podmiotowej, a także na stronie internetowej urzędu obsługującego Pełnomocnika:

1) informację o wydanym ostrzeżeniu, a także o odwołaniu ostrzeżenia;
2) listę wydanych i odwołanych ostrzeżeń.

8. Informacja o wydaniu ostrzeżenia może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

9. Zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego może polegać na:

1) przeprowadzeniu szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzeniu środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
2) dokonaniu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością;
3) wdrożeniu określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;
4) dokonaniu określonej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;
5) prowadzeniu wzmożonego monitorowania zachowania systemu;
6) odstąpieniu od korzystania z określonego sprzętu lub oprogramowania;
7) wprowadzeniu reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.

Art. 67b. 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 66b oraz art. 66c.

2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o decyzjach wydanych na podstawie art. 66a ust. 12.

Art. 67c. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26 ustawy.

2. Decyzja, o której mowa w ust. 1, określa w szczególności:
1) zakres powierzonych zadań;
2) czas realizacji powierzonych zadań lub sposób ich odwołania;
3) w razie potrzeby – szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV;
4) zasady informowania Kolegium o stanie realizacji powierzonych zadań.

3. Realizacja zadań, o których mowa w ust. 1, jest dokonywana przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych, z uwzględnieniem art. 52a.

4. Decyzję, o której mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Informacja o ogłoszeniu decyzji jest udostępniana na stronach internetowych CSIRT GOV, CSIRT MON, CSIRT NASK lub

w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.”;

65) w art. 73:

a) w ust. 1:

– w pkt 4 wyraz „osoby” zastępuje się wyrazem „osób”,

– w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 i 15 w brzmieniu:

„14) z własnej winy nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11;

15) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 3.”,

b) po ust. 1 dodaje się ust. 1a–1e w brzmieniu:

„1a. Jednostka oceniająca zgodność, która nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne, podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”.

1b. Jednostka oceniająca zgodność:

1) która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających, w chwili jego wydania, wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,

2) działa bez wymaganej akredytacji

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

1c. Dostawcy produktów ICT, usług ICT lub procesów ICT albo jednostka oceniająca zgodność, które:

1) uniemożliwiają właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y,

2) utrudniają właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

1d. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadjącą osobowości prawnej, która wprowadza w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

1e. Dostawca, który nie wykonuje obowiązku określonego w art. 59u podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.”,

c) po ust. 2 dodaje się ust. 2a–2c w brzmieniu:

„2a. Karze pieniężnej podlega podmiot określony w art. 66a ust. 1 pkt 1–3, który nie dostosował się do obowiązków określonych w art. 66b.

2b. Na podmiot publiczny, który nie wyznaczył osób, o których mowa w art. 21, może być nałożona kara pieniężna, jeżeli brak wyznaczenia tych osób uniemożliwia lub utrudnia wymianę informacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa a tym podmiotem.

2c. Na podmiot, który nie wypełnia obowiązków informacyjnych, o których mowa w art. 66c, może zostać nałożona kara pieniężna, jeżeli przemawia za tym charakter lub zakres naruszenia.”,

d) w ust. 3:

– pkt 9 otrzymuje brzmienie:

„9) ust. 1 pkt 10, 14 i 15, wynosi do 100 000 zł;”,

– dodaje się pkt 14–16 w brzmieniu:

„14) ust. 2a, wynosi:

a) w przypadku podmiotów określonych w art. 66a ust. 1 pkt 1–3, z wyjątkiem podmiotów, o których mowa w art. 4 pkt 3–6b, 7–15 i 17–20, do 3% jego całkowitego rocznego światowego obrotu podmiotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów, o których mowa w art. 4 pkt 3–6b, 7–15 i 17–20, do 100 000 zł;

15) ust. 2b, wynosi do 10 000 zł;

16) ust. 2c, wynosi do 50 000 zł.”,

e) dodaje się ust. 6 i 7 w brzmieniu:

„6. Niezależnie od kary pieniężnej, o której mowa w ust. 2b, minister właściwy do spraw informatyzacji może nałożyć, w drodze decyzji, na kierującego podmiotem publicznym, o którym mowa w art. 4 pkt 7–15, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek. Za minimalne wynagrodzenie uznaje się minimalne wynagrodzenie obowiązujące 1 stycznia w roku kalendarzowym, w którym wszczęto postępowanie w sprawie nałożenia kary.

7. Niezależnie od kary pieniężnej, o której mowa w ust. 2c, można nałożyć na kierującego podmiotem, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego tego podmiotu lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.”;

66) w art. 74:

a) ust. 1 otrzymuje brzmienie:

„1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.”,

b) po ust. 1 dodaje się ust. 1a–1d w brzmieniu:

„1a. Karę pieniężną, o której mowa w art. 73 ust. 1a–1e, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

1b. Karę pieniężną, o której mowa w art. 73 ust. 2a nakłada, w drodze decyzji:

1) w przypadku przedsiębiorców komunikacji elektronicznej – Prezes UKE;

2) w przypadku operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej – organ właściwy do spraw cyberbezpieczeństwa;

3) w przypadku podmiotów określonych w art. 66a ust. 1 pkt 1–3, innych niż przedsiębiorcy komunikacji elektronicznej, operatorzy usług kluczowych, dostawcy usług cyfrowych – minister właściwy do spraw informatyzacji.

1c. Karę pieniężną, o której mowa w art. 73 ust. 2b, nakłada w drodze decyzji minister właściwy do spraw informatyzacji.

1d. Karę pieniężną, o której mowa w art. 73 ust. 2c i 7, może nałożyć w drodze decyzji organ uprawniony do żądania informacji zgodnie z właściwością określoną w art. 66c ust. 2.”;

67) po art. 74 dodaje się art. 74a w brzmieniu:

„Art. 74a 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ust. 2a, podmiot, wobec którego wszczęto to postępowanie, jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej.

2. W przypadku gdy podmiot, wobec którego wszczęto postępowanie w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ust. 2a:

1) nie dostarczył danych niezbędnych do określenia podstawy wymiaru kary pieniężnej lub
2) dostarczone przez ten podmiot dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej

– organ uprawniony do nałożenia kary ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu.”;

68) po art. 75 dodaje się art. 75a w brzmieniu:

„Art. 75a. 1. Organ właściwy do spraw cyberbezpieczeństwa nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT sektorowego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44 ust. 1a.

2. Szef Agencji Wywiadu nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT INT, jeżeli nie został wykonany obowiązek, o którym mowa w art. 36c.

3. Prezes UKE nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT Telco, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44a ust. 5.

4. Kara pieniężna, o której mowa w ust. 1–3, nakładana jest w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek. Za minimalne wynagrodzenie uznaje się minimalne wynagrodzenie za pracę obowiązujące w dniu 1 stycznia roku, w którym nie został wykonany obowiązek.”;

69) po art. 76 dodaje się art. 76a i art. 76b w brzmieniu:

„Art. 76a. 1. Karze pieniężnej podlega przedsiębiorca komunikacji elektronicznej, który:

1) nie wypełnia obowiązku systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia, o którym mowa w art. 20a ust. 2 pkt 1;
2) nie podejmuje środków, o których mowa w art. 20a ust. 2 pkt 2;
3) nie dokumentuje czynności, o których mowa w art. 20a ust. 2 pkt 1 i 2;
4) nie przekazuje informacji, o których mowa w art. 20b ust. 2, w terminie wskazanym w żądaniu Prezesa UKE;
5) nie wykonuje obowiązku, o którym mowa w art. 20b ust. 4, w terminie wskazanym w decyzji Prezesa UKE;
6) nie obsługuje incydentu telekomunikacyjnego, o którym mowa w art. 20c pkt 1;
7) nie zgłasza poważnego incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;
8) nie współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco lub z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV i tym samym nie wykonuje obowiązku, o którym mowa w art. 20d ust. 1 pkt 3;
9) nie usuwa w wyznaczonym przez Prezesa UKE terminie podatności, która doprowadziła lub mogła doprowadzić do incydentu telekomunikacyjnego lub krytycznego, o której mowa w art. 54a;
10) nie wykonuje zaleceń pokontrolnych Prezesa UKE, o których mowa w art. 59.

2. Prezes UKE, jeżeli przemawia za tym charakter lub zakres naruszenia, może nałożyć karę pieniężną na przedsiębiorcę komunikacji elektronicznej, który:

1) nie wyznacza dwóch osób, o których mowa w art. 20a ust. 4 pkt 1;
2) nie zapewnia dostępu do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań;
3) nie wykonuje obowiązku, o którym mowa w art. 20f ust. 1 i 2;
4) nie wykonuje obowiązku, o którym mowa w art. 20h ust. 5.

3. Kara, o której mowa w ust. 1 i 2, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

4. Karę, o której mowa w ust. 1:

1) pkt 6 – nakłada się za każdy stwierdzony przypadek zaniechania obsługi incydentu telekomunikacyjnego;
2) pkt 7 – nakłada się za każdy stwierdzony przypadek niezgłoszenia poważnego incydentu telekomunikacyjnego.

5. Niezależnie od kar pieniężnych, o których mowa w ust. 1 i 2, Prezes UKE może nałożyć na osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy komunikacji elektronicznej lub związku takich przedsiębiorców karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.

Art. 76b. 1. Kary pieniężne, o których mowa w art. 76a ust. 1 i 2, nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.

2. W przypadku, gdy podmiot w roku kalendarzowym poprzedzającym rok nałożenia kary pieniężnej nie osiągnął przychodu lub osiągnął przychód w wysokości nieprzekraczającej 500 000 zł, Prezes UKE nakładając karę pieniężną uwzględnia średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej.

3. W przypadku, gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, lub gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł.

4. W przypadku, gdy przed wydaniem decyzji o nałożeniu kary pieniężnej podmiot nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary pieniężnej, Prezes UKE nakładając karę pieniężną, uwzględnia:

1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok;
2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających ten rok. Przepis ust. 3 stosuje się odpowiednio.

5. W przypadku, gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, o którym mowa w ust. 1, Prezes UKE uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary. Przepisy ust. 2–4 stosuje się odpowiednio.

6. Ustalając wysokość kary pieniężnej Prezes UKE uwzględnia charakter i zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

7. Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 1 miesiąca od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 złotych.”;

70) po art. 76b dodaje się oznaczenie i tytuł działu oraz oznaczenie i tytuł rozdziału w brzmieniu:

„DZIAŁ III. STRATEGICZNA SIEĆ BEZPIECZEŃSTWA

Rozdział 1

Operator strategicznej sieci bezpieczeństwa

Art. 76c. 1. W celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, tworzy się, utrzymuje, rozwija i modernizuje infrastrukturę strategicznej sieci bezpieczeństwa, będącej siecią telekomunikacyjną w rozumieniu art. 2 pkt 58 ustawy z dnia … – Prawo komunikacji elektronicznej.

2. Strategiczna sieć bezpieczeństwa jest uruchamiana oraz zarządzana przez operatora strategicznej sieci bezpieczeństwa.

3. Strategiczna sieć bezpieczeństwa zapewnia poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych niezbędny do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w tym spełnia wymagania techniczne umożliwiające szyfrowaną komunikację między użytkownikami końcowymi tej sieci.

4. Prezes Rady Ministrów może określić, w drodze rozporządzenia, minimalne wymagania techniczne jakie musi spełniać strategiczna sieć bezpieczeństwa oraz minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo-technicznej.

Art. 76d. 1. Prezes Rady Ministrów wyznacza operatora strategicznej sieci bezpieczeństwa spośród podmiotów spełniających łącznie następujące warunki:

1) będących jednoosobową spółką Skarbu Państwa,
2) będących przedsiębiorcą telekomunikacyjnym,
3) posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 76c ust. 1 lub które zobowiązały się do jej pozyskania,
4) posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
5) posiadających świadectwo bezpieczeństwa przemysłowego pierwszego stopnia, o którym mowa w art. 55 ust. 1 pkt 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych,
6) dających rękojmię należytego wykonywania zadań operatora strategicznej sieci bezpieczeństwa

– pod warunkiem wyrażenia zgody na pełnienie funkcji operatora strategicznej sieci bezpieczeństwa.

2. Prezes Rady Ministrów przed wyznaczeniem operatora strategicznej sieci bezpieczeństwa zasięga opinii Kolegium.

3. Operator strategicznej sieci bezpieczeństwa jest obowiązany do prowadzenia wyodrębnionej ewidencji księgowej środków otrzymanych na realizację zadań, o których mowa w art. 76c ust. 1, oraz wydatków dokonywanych z tych środków.

Art. 76e. 1. Operator strategicznej sieci bezpieczeństwa w celu realizacji zadań, o których mowa w art. 76c ust. 1, świadczy usługi telekomunikacyjne oraz może świadczyć usługi związane z zapewnieniem udogodnień towarzyszących oraz usługi z zakresu cyberbezpieczeństwa, a także prowadzić działalność badawczo-rozwojową.

2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 62 ust. 2 pkt 2 i 3 ustawy z dnia … – Prawo komunikacji elektronicznej. Wykorzystanie częstotliwości użytkowanych jako rządowe przez operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3.

3. Wykorzystanie częstotliwości, o których mowa w art. 76s ust. 1, przez operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 138 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.

Art. 76f. 1. Operator strategicznej sieci bezpieczeństwa świadczy usługi, na potrzeby realizacji zadań określonych w art. 76c ust. 1, na rzecz:

1) Kancelarii Prezydenta Rzeczypospolitej Polskiej,
2) Kancelarii Sejmu,
3) Kancelarii Senatu,
4) Kancelarii Prezesa Rady Ministrów,
5) Biura Bezpieczeństwa Narodowego,
6) urzędów obsługujących organy administracji rządowej, organy jednostek samorządu terytorialnego oraz podmiotów podległych tym organom albo przez nie nadzorowanych, wykonującym zadania z zakresu:
   a) ochrony bezpieczeństwa i porządku publicznego,
   b) bezpieczeństwa i obronności państwa,
   c) bezpieczeństwa ekonomicznego,
   d) ochrony granicy państwa,
   e) ochrony ludności i obrony cywilnej,
   f) zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa,
   g) dostaw energii,
   h) ochrony interesów Rzeczypospolitej Polskiej,
   i) ochrony zdrowia,
   j) weterynaryjnej ochrony zdrowia publicznego,
   k) nadzoru sanitarnego,
   l) ochrony środowiska,
   m) sprawiedliwości,
   n) systemu powiadamiania ratunkowego,
7) sądów,
8) prokuratury,
9) Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej,
10) podmiotów wykonujących na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa

– na wniosek tych podmiotów.

2. Podmioty, o których mowa w ust. 1, korzystają z usług telekomunikacyjnych w ruchomej publicznej sieci telekomunikacyjnej świadczonych przez operatora strategicznej sieci bezpieczeństwa, przy pomocy strategicznej sieci bezpieczeństwa, w zakresie niezbędnym do zapewnienia w tych podmiotach realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

3. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i Siły Zbrojne Rzeczypospolitej Polskiej oraz jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej nie mają obowiązku korzystania z sieci, o której mowa w art. 76c ust. 1.

4. Prezes Rady Ministrów może zobowiązać operatora strategicznej sieci bezpieczeństwa do świadczenia usług, o których mowa w art. 76e ust. 1:

1) właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym – na wniosek organu, we właściwości którego znajduje się określony system infrastruktury krytycznej, lub
2) przedsiębiorcom realizującym zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny – na wniosek Ministra Obrony Narodowej.

5. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Państwowa Straż Pożarna, Służba Ochrony Państwa oraz Policja mogą zlecić operatorowi strategicznej sieci bezpieczeństwa świadczenie usługi wsparcia technicznego, przy realizacji ich zadań ustawowych, z uwzględnieniem prac badawczo-rozwojowych dotyczących nowoczesnych systemów łączności. Usługi wsparcia technicznego mogą polegać w szczególności na utrzymaniu, rozbudowie i modyfikacji sieci teleinformatycznych w zakresie sieci rozległych oraz zestawienia i utrzymania łączy dostępowych do takich sieci.

6. Świadczenie przez operatora strategicznej sieci bezpieczeństwa usług, o których mowa w ust. 1–5 oraz w art. 76e ust. 1, wymaga zawarcia umowy pomiędzy operatorem strategicznej sieci bezpieczeństwa, a właściwym podmiotem, o którym mowa w ust. 1, 2 i 4.

7. Umowa, o której mowa w ust. 6, określa w szczególności obowiązek zapewnienia przez operatora strategicznej sieci bezpieczeństwa usług telekomunikacyjnych o określonej jakości, dostępności, pojemności i wydajności, w tym w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, a w przypadku wydania rozporządzenia, o którym mowa w art. 76c ust. 4, także obowiązek zapewnienia określonego w rozporządzeniu poziomu bezpieczeństwa sieci i usług. Umowa określa również zasady odpłatności za świadczone usługi.

8. W przypadku uporczywego niewywiązywania się przez operatora strategicznej sieci bezpieczeństwa z obowiązków wynikających z umowy, o której mowa w ust. 6, podmiot na rzecz którego operator strategicznej sieci bezpieczeństwa świadczy usługi może rozwiązać taką umowę, informując Prezesa Rady Ministrów o przyczynach rozwiązania umowy.

9. W przypadku, o którym mowa w ust. 8, podmiot może zlecić świadczenie usług objętych umową, o której mowa w ust. 6, operatorowi telekomunikacyjnemu innemu niż operator strategicznej sieci bezpieczeństwa, dającemu rękojmię zapewnienia bezpieczeństwa świadczonych usług na poziomie nie niższym niż określony w rozwiązanej umowie z operatorem strategicznej sieci bezpieczeństwa lub w przepisach wydanych na podstawie art. 76c ust. 4.

Art. 76g. 1. W związku z ochroną istotnych interesów bezpieczeństwa państwa przy zawieraniu umów, o których mowa w art. 76f ust. 6, dotyczących realizacji zadań, o których mowa w art. 76c ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.

2. Cena za usługi świadczone przez operatora strategicznej sieci bezpieczeństwa uwzględnia koszt usługi powiększony o rozsądną marżę przy uwzględnieniu, że w koszt usługi nie wlicza się usług lub sprzętu sfinansowanych z dotacji, o której mowa w art. 76u ust. 1.

Art. 76h. 1. Prezes UKE może dokonywać analizy cen usług telekomunikacyjnych stosowanych przez operatora strategicznej sieci bezpieczeństwa, o których mowa w art. 76g ust. 2.

2. Podmioty, o których mowa w art. 76f ust. 1, mogą złożyć wniosek o dokonanie analizy, o której mowa w ust. 1.

3. Prezes UKE dokonuje analizy, o której mowa w ust. 1, w terminie:

1) 7 dni od złożenia wniosku, o którym mowa w ust. 2, jeżeli usługa telekomunikacyjna jest lub ma być świadczona w związku z ochroną życia lub zdrowia lub w sytuacji obowiązywania stanów nadzwyczajnych lub zapobieżenia skutkom katastrof naturalnych lub awarii technicznych noszących znamiona klęski żywiołowej, lub
2) 1 miesiąca od złożenia wniosku, o którym mowa w ust. 2 – w pozostałych przypadkach.

4. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę, których dotyczą, podmiot zobowiązany do zawarcia umowy z operatorem strategicznej sieci bezpieczeństwa może rozpocząć procedurę zawarcia umowy o świadczenie usług telekomunikacyjnych z innym dostawcą usług. Prezes UKE informuje operatora strategicznej sieci bezpieczeństwa o wynikach analizy, o której mowa w ust. 1.

5. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę, których dotyczą, operator strategicznej sieci bezpieczeństwa w terminie 7 dni, od dnia otrzymania informacji, o której mowa w ust. 4, jest obowiązany przedstawić nową ofertę podmiotowi zobowiązanemu do zawarcia umowy z operatorem strategicznej sieci bezpieczeństwa. Prezes UKE, na wniosek operatora strategicznej sieci bezpieczeństwa lub podmiotu zobowiązanego do zawarcia umowy z operatorem strategicznej sieci bezpieczeństwa, dokonuje analizy cen usług telekomunikacyjnych przedstawionych w nowej ofercie w terminie 21 dni, od otrzymania wniosku. O wyniku analizy jest informowany operator strategicznej sieci bezpieczeństwa oraz podmiot, do którego ta oferta została skierowana.

6. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 5 zdanie drugie, przekraczają koszty oraz rozsądną marżę, Prezes UKE wydaje decyzję zastępującą albo zmieniającą umowę, uwzględniając przedłożoną ofertę oraz określa cenę świadczonych usług na poziomie odpowiadającym kosztom oraz rozsądnej marży.

Art. 76i. 1. Operator strategicznej sieci bezpieczeństwa przekazuje Prezesowi UKE informacje o zawartej umowie na świadczenie usług za pośrednictwem strategicznej sieci bezpieczeństwa, w szczególności cenę oraz zakres świadczonych usług, w terminie 14 dni od dnia zawarcia umowy.

2. Operator strategicznej sieci bezpieczeństwa jest obowiązany do przekazywania na żądanie Prezesa UKE informacji niezbędnych do wykonywania przez Prezesa UKE jego uprawnień i obowiązków, w terminie 21 dni od otrzymania żądania.

Art. 76j. 1. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2023 r. poz. 733), zapewnia operatorowi strategicznej sieci bezpieczeństwa dostęp do infrastruktury technicznej, w tym współkorzystanie z niej, w celu realizacji zadań, o których mowa w art. 76c ust. 1.

2. Dostęp do infrastruktury technicznej jest odpłatny, chyba że strony umowy postanowią inaczej.

3. Opłaty z tytułu dostępu do infrastruktury technicznej określa się w wysokości, która umożliwia zwrot części kosztów, które ponosi operator sieci w związku z utrzymaniem tej infrastruktury oraz z zapewnieniem dostępu.

4. Warunki dostępu, o którym mowa w ust. 1, w tym techniczne, eksploatacyjne i finansowe warunki współpracy, określa umowa zawarta w formie pisemnej lub elektronicznej pomiędzy operatorem strategicznej sieci bezpieczeństwa a operatorem sieci. Przepisy art. 19 ust. 1–2a, 4 i 5, art. 20, art. 24 i art. 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio.

5. W przypadku odmowy udzielenia dostępu do infrastruktury technicznej przez operatora sieci lub niezawarcia umowy o dostępie do infrastruktury technicznej w terminie 2 miesięcy od dnia złożenia wniosku o taki dostęp, operator strategicznej sieci bezpieczeństwa może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do infrastruktury technicznej.

6. Do wniosku do Prezesa UKE o wydanie decyzji w sprawie dostępu do infrastruktury technicznej dołącza się:

1) wniosek w sprawie zawarcia umowy o dostępie do infrastruktury technicznej;
2) potwierdzenie doręczenia drugiej stronie lub potwierdzenie nadania przesyłką poleconą wniosku, o którym mowa w pkt 1;
3) dokumenty z negocjacji prowadzonych z drugą stroną, o ile druga strona podjęła negocjacje;
4) projekt umowy o dostępie do infrastruktury technicznej, z zaznaczeniem tych części umowy, co do których strony nie doszły do porozumienia.

7. Strony są obowiązane przedłożyć Prezesowi UKE, na jego żądanie, w terminie 14 dni, swoje stanowiska wobec rozbieżności oraz dokumenty niezbędne do rozpatrzenia wniosku.

8. Prezes UKE wydaje decyzję w sprawie dostępu do infrastruktury technicznej w celu realizacji przez operatora strategicznej sieci bezpieczeństwa zadań, o których mowa w art. 76c ust. 1, w terminie 2 miesięcy od dnia złożenia wniosku o jej wydanie przez operatora strategicznej sieci bezpieczeństwa, biorąc pod uwagę w szczególności konieczność zapewnienia niedyskryminacyjnych i proporcjonalnych warunków dostępu.

9. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, w terminie 14 dni od dnia otrzymania zawiadomienia o wszczęciu postępowania o wydanie decyzji w sprawie dostępu do infrastruktury technicznej, przedstawia Prezesowi UKE uzasadnienie wysokości opłat z tytułu dostępu do infrastruktury technicznej, w którym uwzględnia kryteria, o których mowa w ust. 3.

10. Decyzja w sprawie dostępu do infrastruktury technicznej w zakresie nią objętym zastępuje umowę o tym dostępie.

11. W przypadku zawarcia przez zainteresowane strony umowy o dostępie do infrastruktury technicznej, decyzja o dostępie do infrastruktury technicznej wygasa z mocy prawa w części objętej umową.

12. Decyzja w sprawie dostępu do infrastruktury technicznej może zostać zmieniona przez Prezesa UKE na wniosek każdej ze stron, której ona dotyczy, lub z urzędu, w przypadkach uzasadnionych potrzebą zapewnienia ochrony interesów odbiorców usług świadczonych przez podmioty wykonujące zadania z zakresu użyteczności publicznej lub użytkowników końcowych lub zapewnienia ochrony skutecznej konkurencji.

13. W postępowaniu w sprawie zmiany decyzji w sprawie dostępu do infrastruktury technicznej przepisy ust. 3 oraz ust. 8–10 stosuje się odpowiednio.

Art. 76k. 1. Na potrzeby realizacji zadań, o których mowa w art. 76c ust. 1:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa,
2) jednostka samorządu terytorialnego, oraz
3) właściciel lub zarządca nieruchomości

– zapewnia operatorowi strategicznej sieci bezpieczeństwa dostęp do nieruchomości, w tym do budynku, polegający na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości.

2. Warunki dostępu, o którym mowa w ust. 1, określa odpowiednio umowa zawarta pomiędzy operatorem strategicznej sieci bezpieczeństwa, a podmiotami, o których mowa w ust. 1. Przepisy art. 19 ust. 1–2a, 4 i 5, art. 20 i art. 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio.

3. Umowa, o której mowa w ust. 2, jest zawierana w formie pisemnej lub elektronicznej.

4. Dostęp, o którym mowa w ust. 1, jeżeli podmiotem zapewniającym dostęp jest:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa jest nieodpłatny;
2) jednostka samorządu terytorialnego, właściciel lub zarządca nieruchomości, jest nieodpłatny, przy czym operator strategicznej sieci bezpieczeństwa ponosi:
   a) proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością,
   b) proporcjonalną część kosztów, które wystąpiły po stronie udostępniającego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu,
   c) koszty przywrócenia nieruchomości do stanu poprzedniego.

5. W przypadku odmowy udzielenia dostępu do nieruchomości przez podmioty, o których mowa w ust. 1, lub niezawarcia umowy o dostępie do nieruchomości w terminie miesiąca od dnia złożenia wniosku o taki dostęp, każda ze stron może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do nieruchomości.

6. Przepisy art. 76j ust. 6–8 oraz ust. 10–13 stosuje się odpowiednio.

Art. 76l. Od decyzji Prezesa UKE dotyczącej dostępu telekomunikacyjnego, o którym mowa w art. 76j ust. 5 oraz art. 76k ust. 5, przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

Art. 76m. 1. Operatorowi strategicznej sieci bezpieczeństwa przysługuje prawo pierwokupu sieci telekomunikacyjnych będących własnością:

1) Skarbu Państwa lub innych państwowych osób prawnych, w szczególności podmiotów, o którym mowa w art. 2 pkt 87 lit. a, b, d, e, g i h ustawy z dnia …– Prawo komunikacji elektronicznej;
2) jednostek samorządu terytorialnego.

2. Podmioty, o których mowa w ust. 1, informują operatora strategicznej sieci bezpieczeństwa o zamiarze zbycia sieci telekomunikacyjnych, określając termin na skorzystanie z prawa pierwokupu nie krótszy niż 2 tygodnie.

3. W przypadku braku odpowiedzi od operatora strategicznej sieci bezpieczeństwa w wyznaczonym terminie przyjmuje się, że operator strategicznej sieci bezpieczeństwa zrezygnował ze skorzystania z prawa pierwokupu.

Art. 76n. 1. Prezes UKE może, w przypadku wystąpienia sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 65 lit. a ustawy z dnia …– Prawo komunikacji elektronicznej, oraz pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758–768 MHz, w drodze decyzji, na uzasadniony wniosek operatora strategicznej sieci bezpieczeństwa, na czas określony nałożyć na podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz obowiązek udostępnienia operatorowi strategicznej sieci bezpieczeństwa zasobów częstotliwości z tego zakresu.

2. Operator strategicznej sieci bezpieczeństwa wskazuje we wniosku, o którym mowa w ust. 1, czas, obszar, zasób częstotliwości z zakresu 713–733 MHz lub 768–788 MHz o udostępnienie, których wnosi.

3. Uzasadnienie wniosku, o którym mowa w ust. 1, zawiera:

1) opis sytuacji szczególnego zagrożenia, o której mowa w ust. 1;
2) wskazanie przyczyn pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758–768 MHz;
3) wskazanie obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1.

4. Decyzję, o której mowa w ust. 1, Prezes UKE wydaje na czas określony, nie dłuższy niż czas trwania sytuacji, o których mowa w ust. 1, przy czym nie dłuższy niż 72 godziny. W przypadku ustania okoliczności, o których mowa w ust. 1, operator strategicznej sieci bezpieczeństwa niezwłocznie zwalnia udostępnione zasoby częstotliwości. Decyzji nadaje się rygor natychmiastowej wykonalności.

5. Obszar udostępnienia zasobów częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz nie może przekraczać obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1.

6. Podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz jest obowiązany udostępnić operatorowi strategicznej sieci bezpieczeństwa

zasoby częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz niezwłocznie, nie później niż w ciągu jednej godziny, z wyjątkiem częstotliwości, które zostały udostępnione Siłom Zbrojnym Rzeczypospolitej Polskiej.

7. W sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 65 lit. a ustawy z dnia …– Prawo komunikacji elektronicznej, operator strategicznej sieci bezpieczeństwa jest obowiązany udostępnić Siłom Zbrojnym Rzeczypospolitej Polskiej udostępnione mu przez podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz zasoby częstotliwości z tego zakresu niezwłocznie, nie później niż w ciągu jednej godziny, na czas na jaki zostały mu udostępnione.

8. W przypadku udostępnienia częstotliwości operatorowi strategicznej sieci bezpieczeństwa, podmiot dysponujący rezerwacją częstotliwości nie uiszcza opłaty za prawo dysponowania częstotliwością, za okres udostępnienia częstotliwości.

9. Do roszczenia o odszkodowanie z tytułu strat poniesionych przez podmiot dysponujący rezerwacją częstotliwości wskutek wydania decyzji, o której mowa w ust. 1, stosuje się odpowiednio przepisy ustawy z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela (Dz. U. poz. 1955).

Art. 76o. Podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz określa kanał komunikacji elektronicznej, umożliwiający niezwłoczną wymianę komunikatów z operatorem strategicznej sieci bezpieczeństwa i przekazuje informację o tym kanale do operatora strategicznej sieci bezpieczeństwa w terminie 14 dni od otrzymania decyzji w sprawie rezerwacji częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz.

Art. 76p. W zakresie nieuregulowanym w ustawie do operatora strategicznej sieci bezpieczeństwa przepisy ustawy z dnia …. – Prawo komunikacji elektronicznej stosuje się odpowiednio.

Art. 76q. 1. W przypadku, w którym podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa przestaje spełniać którąkolwiek z przesłanek, o których mowa w art. 76d ust. 1, Prezes Rady Ministrów może:

1) odwołać operatora strategicznej sieci bezpieczeństwa, wskazując termin tego odwołania, oraz
2) wyznaczyć nowego operatora strategicznej sieci bezpieczeństwa za jego zgodą, wskazując termin objęcia tej funkcji.

2. Prezes Rady Ministrów, po zasięgnięciu opinii dotychczasowego operatora strategicznej sieci bezpieczeństwa, wyznacza termin odwołania dotychczasowego operatora oraz wyznaczenia nowego.

3. Prezes Rady Ministrów, w drodze zarządzenia, określa sposób przekazania majątku trwałego nabytego z wykorzystaniem środków publicznych, w celu wykonywania zadań, o których mowa w art. 76c ust. 1, na rzecz nowego operatora strategicznej sieci bezpieczeństwa.

Art. 76r. W przypadku, o którym mowa w art. 76q ust. 1:

1) podmiot wyznaczony na nowego operatora strategicznej sieci bezpieczeństwa jest następcą prawnym i wstępuje w ogół praw i obowiązków dotychczasowego operatora strategicznej sieci bezpieczeństwa w zakresie realizacji zadań, o których mowa w art. 76c ust. 1;
2) umowy, o których mowa w art. 76f ust. 6, wygasają z mocy prawa w terminie 3 miesięcy od wyznaczenia nowego operatora strategicznej sieci bezpieczeństwa.

Rozdział 2

Przyznanie częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz

Art. 76s. 1. Prezes UKE, w drodze decyzji, przydziela operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe w zakresie 703–713 MHz oraz 758–768 MHz.

2. Do decyzji, o której mowa w ust. 1, przepisy art. 68 oraz art. 69 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.

3. W decyzji, o której mowa w ust. 1, Prezes UKE określa wymogi pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o częstotliwości, o których mowa w ust. 1.

Art. 76t. 1. W przypadku zmiany operatora nowy operator strategicznej sieci bezpieczeństwa obejmuje prawa i obowiązki wynikające z przydziału częstotliwości, o którym mowa w art. 76s ust. 1.

2. Prezes UKE potwierdza, w terminie 14 dni od wyznaczenia nowego operatora strategicznej sieci bezpieczeństwa, o którym mowa w ust. 1, w drodze zaświadczenia, przejęcie przez nowego operatora strategicznej sieci bezpieczeństwa, praw i obowiązków wynikających z przydziału częstotliwości, o którym mowa w art. 76s ust. 1.

3. Zaświadczenie, o którym mowa w ust. 2, wydaje się na wniosek nowego operatora strategicznej sieci bezpieczeństwa.

Rozdział 3

Finansowanie strategicznej sieci bezpieczeństwa

Art. 76u. 1. Operator strategicznej sieci bezpieczeństwa otrzymuje dotację celową z części budżetu państwa, której dysponentem jest minister właściwy do spraw aktywów państwowych, na realizację zadań związanych z utworzeniem, utrzymaniem, rozwojem i modernizacją infrastruktury strategicznej sieci bezpieczeństwa.

2. Podstawę obliczenia należnej operatorowi strategicznej sieci bezpieczeństwa dotacji, o której mowa w ust. 1, stanowi ustalony przez ministra właściwego do spraw aktywów państwowych koszt realizacji poszczególnych zadań.

3. Szczegółowe warunki wypłaty środków, o których mowa w ust. 1, kwoty należne z tytułu realizacji zadań, o których mowa w ust. 1, oraz sposób i zasady rozliczeń określa umowa zawarta między ministrem właściwym do spraw aktywów państwowych a operatorem strategicznej sieci bezpieczeństwa.

4. Umowa określa również zasady zwrotu niewykorzystanych środków publicznych przeznaczonych na wykonywanie zadań, o których mowa w art. 76c ust. 1, w przypadku, o którym mowa w art. 76q ust. 1 pkt 1.

5. Minister właściwy do spraw aktywów państwowych określi łączną kwotę dotacji, o której mowa w ust. 1, na podstawie danych dotyczących kosztu realizacji zadań, o których mowa w ust. 1, oraz liczby zrealizowanych zadań, przedstawionych przez operatora strategicznej sieci bezpieczeństwa.

6. Ze środków dotacji nie może być dofinansowana działalność gospodarcza operatora strategicznej sieci bezpieczeństwa.”;

71) oznaczenie i tytuł rozdziału 15 otrzymują brzmienie:

„DZIAŁ IV

Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe”;

72) w art. 93 uchyla się ust. 8 i 23;

73) w załączniku nr 1 do ustawy:

a) w wierszu „Ochrona zdrowia” w kolumnie trzeciej „Rodzaj podmiotów:

– wiersz drugi otrzymuje brzmienie: „Jednostka podległa ministrowi właściwemu do spraw zdrowia lub przez niego nadzorowana”,

– skreśla się wiersz czwarty i piąty w brzmieniu: „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu

ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301 oraz z 2023 r. poz. 605 i 650) oraz „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”,

– po wierszu dwunastym dodaje się wiersz trzynasty w brzmieniu: „Jednostka będąca administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2022 r. poz. 1720, 1733, 2705 i 2770)”,

b) w wierszu „Infrastruktura cyfrowa” w kolumnie trzeciej „Rodzaj podmiotów” po wierszu trzecim dodaje się wiersz czwarty w brzmieniu „Operator strategicznej sieci bezpieczeństwa”;

74) dodaje się załącznik nr 3 w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. W ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2023 r. poz. 973) w art. 13 w ust. 1 w pkt 30 kropkę zastępuje się średnikiem i dodaje się pkt 31 w brzmieniu:

„31) podmiocie wyznaczonym na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …).”.

Art. 3. W ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, 1812, 1933 i 2185 oraz z 2023 r. poz. 412 i 825) w art. 226 w ust. 1 w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:

„19) obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i….) lub usługę ICT lub proces ICT, określone w tej decyzji.”.

Art. 4. Do postępowań o udzielenie zamówienia publicznego wszczętych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy ustawy zmienianej w art. 1 i art. 3 w brzmieniu nadanym niniejszą ustawą.

Art. 5. 1. Postanowienia umów, o których mowa w art. 33 ust. 1c ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, obowiązujących w dniu wejścia w życie

ustawy, sprzeczne z art. 33 ust. 1–1d ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, są nieważne.

2. Porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, zawarte przed datą wejścia w życie niniejszej ustawy, zachowują ważność.

Art. 6. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 7. 1. Operator usługi kluczowej wykonuje po raz pierwszy obowiązek, o którym mowa w art. 9 ust. 2 ustawy zmienianej w art. 1, w terminie 14 dni od dnia wejścia w życie niniejszej ustawy.

2. Do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

3. Operator usługi kluczowej realizuje obowiązki, o których mowa w art. 11 ust. 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

Art. 8. Z dniem wejścia w życie ustawy:

1) wewnętrzna struktura odpowiedzialna za cyberbezpieczeństwo powołana w ramach operatora usługi kluczowej przed wejściem w życie niniejszej ustawy staje się SOC wewnętrznym;
2) podmiot świadczący usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę staje się SOC zewnętrznym.

Art. 9. Przedsiębiorca komunikacji elektronicznej:

1) do dnia publikacji komunikatu, o którym mowa w art. 18 ust. 2, zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą do CSIRT MON, CSIRT NASK albo CSIRT GOV zgodnie z właściwością określoną w art. 26 tej ustawy;
2) zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, do CSIRT Telco od dnia publikacji komunikatu, o którym mowa w art. 18 ust. 2.

Art. 10. CSIRT MON, CSIRT NASK lub CSIRT GOV dostosowują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym do przepisów art. 26 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 11. Podmioty, o których mowa w art. 4 pkt 7–15 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, wyznaczają osoby, o których mowa w art. 21 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 12. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa oraz Przewodniczący Kolegium do Spraw Cyberbezpieczeństwa mogą, nie wcześniej niż po upływie trzech miesięcy od dnia wejścia w życie niniejszej ustawy, zlecić przeprowadzenie badania, o którym mowa w art. 33 ust. 1a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 13. Do dnia publikacji komunikatu, o którym mowa w art. 18 ust. 2, w uzgodnieniach, o których mowa w art. 31 ust. 1a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, nie bierze udziału CSIRT Telco.

Art. 14. 1. Szef Agencji Wywiadu informuje jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122), o osiągnięciu przez CSIRT INT zdolności operacyjnej.

2. Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów,

instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym do czasu otrzymania informacji o osiągnięciu zdolności operacyjnej przez CSIRT INT, zgłaszają incydenty w podmiocie publicznym do CSIRT GOV.

Art. 15. 1. Organ właściwy do spraw cyberbezpieczeństwa ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Organ właściwy do spraw cyberbezpieczeństwa publikuje komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

3. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również udostępniana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa,
2) CSIRT MON, CSIRT NASK, CSIRT GOV

– a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 16. W sprawozdaniu organu właściwego do spraw cyberbezpieczeństwa, o którym mowa w art. 44b ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, które jest sporządzane za rok, w którym został utworzony CSIRT sektorowy, zawiera się informacje dotyczące utworzenia CSIRT sektorowego oraz jego funkcjonowania.

Art. 17. Z dniem wejścia ustawy sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym staje się CSIRT sektorowym.

Art. 18. 1. Prezes Urzędu Komunikacji Elektronicznej powołuje CSIRT Telco w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Prezes Urzędu Komunikacji Elektronicznej publikuje komunikat o osiągnięciu przez CSIRT Telco zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

3. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT Telco jest również udostępniana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa,
2) CSIRT MON, CSIRT NASK, CSIRT GOV,

3) Prezesa UKE, w tym na stronie podmiotowej Prezesa UKE w Biuletynie Informacji Publicznej

– a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 19. W sprawozdaniu Prezesa Urzędu Komunikacji Elektronicznej, o którym mowa w art. 44b ust. 2 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, które jest sporządzane za rok, w którym został utworzony CSIRT Telco, zawiera się informacje dotyczące utworzenia CSIRT Telco oraz jego funkcjonowania.

Art. 20. 1. Prezes Rady Ministrów wyznacza operatora strategicznej sieci bezpieczeństwa w terminie do 1 miesiąca od dnia wejścia w życie ustawy.

2. Do czasu osiągnięcia przez operatora strategicznej sieci bezpieczeństwa pełnej zdolności operacyjnej do świadczenia usług, o których mowa w art. 76f ust. 2 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, podmioty, o których mowa w art. 76f ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, mogą zawierać umowy na świadczenie usług, o których mowa w art. 76f ust. 2 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, także z innymi operatorami telekomunikacyjnymi.

3. Prezes Rady Ministrów podaje do publicznej wiadomości informacje o osiągnięciu pełnej zdolności operacyjnej do świadczenia usług przez operatora strategicznej sieci bezpieczeństwa.

Art. 21. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,093 mln zł;
2) w 2025 r. – 4,208 mln zł;
3) w 2026 r. – 4,208 mln zł;
4) w 2027 r. – 4,208 mln zł;
5) w 2028 r. – 4,208 mln zł;
6) w 2029 r. – 4,208 mln zł;
7) w 2030 r. – 4,208 mln zł;
8) w 2031 r. – 4,208 mln zł;
9) w 2032 r. – 4,208 mln zł;
10) w 2033 r. – 4,208 mln zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 5,599 mln zł;
2) w 2025 r. – 3,672 mln zł;
3) w 2026 r. – 3,672 mln zł;
4) w 2027 r. – 3,672 mln zł;
5) w 2028 r. – 3,672 mln zł;
6) w 2029 r. – 3,672 mln zł;
7) w 2030 r. – 3,672 mln zł;
8) w 2031 r. – 3,672 mln zł;
9) w 2032 r. – 3,672 mln zł;
10) w 2033 r. – 3,672 mln zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 69,838 mln zł;
2) w 2025 r. – 66,551 mln zł;
3) w 2026 r. – 63,178 mln zł;
4) w 2027 r. – 62,473 mln zł;
5) w 2028 r. – 66,599 mln zł;
6) w 2029 r. – 70,561 mln zł;
7) w 2030 r. – 80,688 mln zł;
8) w 2031 r. – 80,916 mln zł;
9) w 2032 r. – 73,141 mln zł;
10) w 2033 r. – 73,164 mln zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,093 mln zł;
2) w 2025 r. – 4,208 mln zł;
3) w 2026 r. – 4,208 mln zł;
4) w 2027 r. – 4,208 mln zł;
5) w 2028 r. – 4,208 mln zł;
6) w 2029 r. – 4,208 mln zł;
7) w 2030 r. – 4,208 mln zł;

8) w 2031 r. – 4,208 mln zł;

9) w 2032 r. – 4,208 mln zł;

10) w 2033 r. – 4,208 mln zł.

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,586 mln zł;

2) w 2025 r. – 4,746 mln zł;

3) w 2026 r. – 4,746 mln zł;

4) w 2027 r. – 4,746 mln zł;

5) w 2028 r. – 4,746 mln zł;

6) w 2029 r. – 4,746 mln zł;

7) w 2030 r. – 4,746 mln zł;

8) w 2031 r. – 4,746 mln zł;

9) w 2032 r. – 4,746 mln zł;

10) w 2033 r. – 4,746 mln zł.

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,586 mln zł;

2) w 2025 r. – 4,746 mln zł;

3) w 2026 r. – 4,746 mln zł;

4) w 2027 r. – 4,746 mln zł;

5) w 2028 r. – 4,746 mln zł;

6) w 2029 r. – 4,746 mln zł;

7) w 2030 r. – 4,746 mln zł;

8) w 2031 r. – 4,746 mln zł;

9) w 2032 r. – 4,746 mln zł;

10) w 2033 r. – 4,746 mln zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 55 – aktywa państwowe, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 189,000 mln zł;

2) w 2025 r. – 748,000 mln zł;

3) w 2026 r. – 1 459,000 mln zł;

4) w 2027 r. – 544,000 mln zł;

5) w 2028 r. – 552,000 mln zł;
6) w 2029 r. – 569,000 mln zł;
7) w 2030 r. – 622,000 mln zł;
8) w 2031 r. – 650,000 mln zł;
9) w 2032 r. – 662,000 mln zł;
10) w 2033 r. – 720,000 mln zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 3,000 mln zł;
2) w 2025 r. – 3,000 mln zł;
3) w 2026 r. – 3,000 mln zł;
4) w 2027 r. – 3,000 mln zł;
5) w 2028 r. – 3,000 mln zł;
6) w 2029 r. – 3,000 mln zł;
7) w 2030 r. – 3,000 mln zł;
8) w 2031 r. – 3,000 mln zł;
9) w 2032 r. – 3,000 mln zł;
10) w 2033 r. – 3,000 mln zł.

9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 59 – Agencja Wywiadu, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,586 mln zł;
2) w 2025 r. – 4,746 mln zł;
3) w 2026 r. – 4,746 mln zł;
4) w 2027 r. – 4,746 mln zł;
5) w 2028 r. – 4,746 mln zł;
6) w 2029 r. – 4,746 mln zł;
7) w 2030 r. – 4,746 mln zł;
8) w 2031 r. – 4,746 mln zł;
9) w 2032 r. – 4,746 mln zł;
10) w 2033 r. – 4,746 mln zł.

10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 6,586 mln zł;
2) w 2025 r. – 4,746 mln zł;
3) w 2026 r. – 4,746 mln zł;
4) w 2027 r. – 4,746 mln zł;
5) w 2028 r. – 4,746 mln zł;
6) w 2029 r. – 4,746 mln zł;
7) w 2030 r. – 4,746 mln zł;
8) w 2031 r. – 4,746 mln zł;
9) w 2032 r. – 4,746 mln zł;
10) w 2033 r. – 4,746 mln zł.

11. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla podsektora transportu wodnego.

12. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla sektora zaopatrzenia w wodę pitną i jej dystrybucji.

13. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji

wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla sektora infrastruktury cyfrowej.

14. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla sektora transportu z wyłączeniem podsektora transportu wodnego.

15. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw zdrowia wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla sektora ochrony zdrowia.

16. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwarty kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego dla sektora energii.

17. Minister właściwy do spraw aktywów państwowych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw aktywów państwowych wdraża mechanizm korygujący polegający na ograniczeniu finansowania strategicznej sieci bezpieczeństwa.

18. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień

20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Bezpieczeństwa Wewnętrznego wdraża mechanizm korygujący polegający na ograniczeniu finansowania badań urządzenia informatycznego lub oprogramowania, o którym mowa w art. 33 ustawy zmienianej w art. 1. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych.

19. Szef Agencji Wywiadu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Wywiadu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT INT. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych.

20. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 10, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT Telco.

Art. 22. Ustawa wchodzi w życie po upływie 6 miesięcy od dnia ogłoszenia.

Załącznik
do ustawy
z dnia

Załącznik nr 3

KATEGORIE FUNKCJI KRYTYCZNYCH
DLA BEZPIECZEŃSTWA SIECI I USŁUG

LP.	**OPIS FUNKCJI**	**IDENTYFIKACJA POWIĄZANEJ FUNKCJI SIECIOWEJ WG STANDARDÓW 3GPP**
1.	Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.	AMF – Access & Mobility management Function AUSF – Authentication Server Function
2.	Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.	UDM – Unified Data Management
3.	Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych.	5G Radio Base Station Baseband Unit oraz inne funkcje
4.	Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.	UPF – User Plane Function
5.	Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.	SMF – Session Management Function
6.	Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.	PCF – Policy Control Function
7.	Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.	NSSF – Network Slice Selection Function
8.	Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.	NRF – Network Repository Function
9.	Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.	NEF – Network Exposure Function
10.	Zabezpieczenia połączeń z innymi sieciami.	SEPP – Security Edge Protection Proxy

UZASADNIENIE

Spis treści

1 Wstęp....3

2 Uzasadnienie poszczególnych przepisów....19

2.1 Zmiany w ustawie o KSC....19

2.1.1 Zmiany w definicjach, katalogu podmiotów krajowego systemu cyberbezpieczeństwa zakresu przedmiotowego....19

2.1.2 Przepisy o operatorach usług kluczowych oraz SOC....27

2.1.3 Zmiany w przepisach dotyczących dostawców usług cyfrowych....33

2.1.4 Przepisy o obowiązkach przedsiębiorców komunikacji elektronicznej w krajowym systemie cyberbezpieczeństwa....34

2.1.5 Zmiany w przepisach dotyczących podmiotów publicznych....44

2.1.6 ISAC i wykaz ISAC....44

2.1.7 Nowe obowiązki zespołów CSIRT GOV, CSIRT MON i CSIRT NASK....47

2.1.8 Zadania CSIRT INT....53

2.1.9 Ocena bezpieczeństwa....54

2.1.10 Zmiany w przepisach o przetwarzaniu danych....57

2.1.11 Zmiany w przepisach o organach właściwych do spraw cyberbezpieczeństwa....59

2.1.12 Zadania i obowiązki CSIRT sektorowych oraz CSIRT Telco....60

2.1.13 Zmiany dot. systemu S46, zadań MON oraz nadzoru....63

2.1.14 Krajowy system certyfikacji cyberbezpieczeństwa....66

2.1.15 Rekomendacje Pełnomocnika. Nowi członkowie oraz zadania Kolegium....76

2.1.16 Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka....78

2.1.17 Ostrzeżenie....93

2.1.18 Zmiany w przepisach o administracyjnych karach pieniężnych....95

2.1.19 Strategiczna sieć bezpieczeństwa....99

2.1.20 Przyznanie częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz....110

2.1.21 Finansowanie strategicznej sieci bezpieczeństwa....113

2.1.22 Zmiany w art. 93....113

2.1.23 Zmiany w załącznikach do ustawy....114

2.2 Zmiany w innych ustawach 114
2.3 Pozostałe przepisy przejściowe i dostosowujące 115
3 Pozostałe informacje 118

1 Wstęp

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913), zwana dalej „ustawą o KSC", uchwalona w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. Ustawa o KSC jest implementacją dyrektywy NIS[1)].

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym"), który odpowiada za identyfikację i wyznaczanie operatorów usług kluczowych oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze.

Obecnie ani przedsiębiorcy telekomunikacyjni ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej „CSIRT"). Do zadań zespołów CSIRT należy m.in. klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów na poziomie krajowym – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, zwanym dalej „NASK-PIB") oraz CSIRT MON (prowadzonego przez Ministra Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw incydentów krytycznych.

Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za wsparcie obsługi incydentów u operatorów usług kluczowych w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół, tj. CSIRT KNF (zespół dla sektora finansowego), funkcjonujący przy Komisji Nadzoru Finansowego[2)].

[1)] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L z 19.07.2016 , str. 1).

[2)] https://www.knf.gov.pl/dla_rynku/CSIRT_KNF.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (zwany dalej „Pełnomocnikiem") jest odpowiedzialny za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu albo podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy zarówno analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa (dokonywana na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT), jak i nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium do Spraw Cyberbezpieczeństwa

Kolegium do Spraw Cyberbezpieczeństwa (zwane dalej „Kolegium") jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje sprawy planowane do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 118 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (zwane dalej „Prawem telekomunikacyjnym"). Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK-PIB. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów, w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa, może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa.

Potrzeba i cele projektu ustawy nowelizującej

Ustawa, kształtując krajowy system cyberbezpieczeństwa, umożliwiła podjęcie prac nad jego dalszym rozwojem. Doświadczenia zebrane na przestrzeni lat funkcjonowania tego systemu w Polsce wskazują na konieczność wprowadzenia rozwiązań, wymagających dokonania zmian na poziomie ustawowym.

Mimo stworzonej przez obowiązujące przepisy możliwości powoływania sektorowych zespołów cyberbezpieczeństwa, zespoły takie nie były dotychczas powoływane. Wyjątek stanowi zespół, powołany przy Komisji Nadzoru Finansowego, dla najbardziej dojrzałego ze wszystkich sektorów, tj. sektora finansowego – CSIRT KNF. Zespół ten powstał w oparciu o wewnętrzne środki i zasoby kadrowe Urzędu Komisji Nadzoru Finansowego. Funkcjonowanie tego zespołu wskazuje, że ustanowienie CSIRT sektorowych dla każdego z kluczowych sektorów polskiej gospodarki ma kluczowy wpływ na podniesienie skuteczności reagowania na incydenty. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i bardziej efektywnie radzić sobie z incydentami, gdyż otrzymają bezpośrednie wsparcie w reagowaniu na incydenty.

Zauważono także potrzebę zwiększenia zakresu uprawnień Pełnomocnika w obszarze zapewniania koordynacji współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa, której wzmocnienie jest niezbędne z punktu widzenia zwiększenia efektywności odpowiedzi na nowe cyberzagrożenia, a także jest zgodne z oczekiwaniem ustawodawcy co do koordynacyjnej funkcji Pełnomocnika.

Jednym z najczęściej występujących problemów związanych z funkcjonowaniem krajowego systemu cyberbezpieczeństwa jest brak powołania przez operatorów usług kluczowych odpowiednio ukształtowanych struktur odpowiedzialnych za cyberbezpieczeństwo. Do problemów utrudniających skuteczną obsługę incydentów należą także: nieodpowiadający faktycznym potrzebom zakres posiadanych przez pracowników operatora kwalifikacji oraz ograniczony dostęp do informacji o cyberzagrożeniach.

Wyniki przeprowadzonych na zlecenie Ministra Cyfryzacji analiz wskazują na zróżnicowany, często wywołujący zastrzeżenia, poziom zabezpieczeń e-usług oferowanych przez samorządy. Potwierdzeniem są ustalenia pokontrolne zawarte w wystąpieniu pokontrolnym Najwyższej Izby Kontroli z 2019 r., z którego wynika, że negatywnie oceniono aż 70% kontrolowanych jednostek samorządu terytorialnego w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji[3)]. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji.

W kontekście podnoszenia poziomu cyberbezpieczeństwa kluczowe znaczenie ma zapewnienie dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń. Jednym ze sposobów na zapewnienie takiego dostępu jest tworzenie ISAC. Pierwsze ISAC (eng. *Information Sharing and Analysis Center*) powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku. ISAC gromadzi informacje o podatnościach

[3)] Najwyższa Izba Kontroli, *Informacja o wynikach kontroli, Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, Warszawa 2019 r., s. 7.

i cyberzagrożeniach, a następnie przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w systemie wymiany takich informacji. Taka formuła współpracy znacząco wpływa na poprawę cyberbezpieczeństwa i jest praktykowana w państwach Unii Europejskiej.

Przykładem sektorowego ISAC na poziomie europejskim jest *European Energy Information Sharing & Analysis Centre* (EE ISAC)[4]. Został on zorganizowany z inicjatywy przemysłu energetycznego. W ramach EE ISAC wymieniają informacje dostawcy usług, przedsiębiorstwa użyteczności publicznej, instytucje naukowe, organizacje rządowe i pozarządowe (m.in. członkiem EE ISAC są Polskie Sieci Elektroenergetyczne Spółka Akcyjna). W Europie działa również amerykański *Financial Services Information Sharing and Analysis Center*[5], zrzeszający około 7 000 instytucji finansowych z całego świata.

Również zdaniem ENISA do prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym a prywatnym[6]. Centra ISAC stanowią platformę takiej współpracy zapewniając wymianę informacji na temat przyczyn, incydentów, cyberzagrożeń, jak również dzielenie się doświadczeniem, wiedzą i analizami.

Rozporządzenie w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013[7]), zwane dalej „Aktem o cyberbezpieczeństwie", zachęca do tworzenia ISAC[8].

Do tej pory powstało w Polsce tylko jedno centrum wymiany informacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. Wskazane jest, aby w Polsce powstało więcej organizacji ISAC, co zdecydowanie powinno przyczynić się do ułatwienia dostępu do specjalistycznej wiedzy i do wymiany informacji o stosowanych rozwiązaniach, tzw. dobrych praktykach.

Coraz większe znaczenie dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe są uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym

---

[4] https://www.ee-isac.eu/.

[5] https://www.fsisac.com/.

[6] Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa, *Information Sharing and Analysis Center (ISACs) – Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, str. 7.

[7] Dz. Urz. UE L 151 z 07.06.2019, str. 15.

[8] Motyw 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), (Dz. Urz. UE L 151 z 07.06.2019, str. 15).

w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanym jako 5G Toolbox[9)]. Zestaw obejmuje zarówno rozwiązania o charakterze strategicznym, technicznym, jak i o charakterze wspierającym. Celami zestawu narzędzi są, po pierwsze, bezpieczeństwo sieci 5G, a po drugie – uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox definiuje zestaw środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków, niezbędne do ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą „kręgosłupem" Jednolitego Rynku Cyfrowego UE. Wśród opisanych w 5G Toolbox środków są środki o charakterze:

- strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym w zakresie oceny bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
- technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – czego odzwierciedleniem są na gruncie prawa krajowego uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT GOV, CSIRT MON, CSIRT NASK, wynikające z art. 33 ustawy o KSC,
- wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox w Polsce.

Europejski Kodeks Łączności Elektronicznej (EKŁE)[10)] umożliwia (w odróżnieniu od poprzedniej regulacji tzw. dyrektywy ramowej) uspójnienie procedury zgłaszania i reagowania na incydenty na poziomie krajowym. Na możliwość zharmonizowania procedury zgłaszania incydentów w rozumieniu ustawy o KSC z incydentami raportowanymi przez przedsiębiorców telekomunikacyjnych wskazuje się także w opublikowanym eksperckim opracowaniu *Synergies in Cybersecurity Incident Reporting*[11)]. Jest to dokument przygotowany przez Grupę Współpracy NIS we współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (zwaną dalej „ENISA") oraz Komisją Europejską. W opracowaniu tym wprost wskazano, że państwa mogą dokonać harmonizacji procedur z dyrektywy NIS, EKŁE oraz rozporządzenia eIDAS, dzięki m.in. posiadaniu podobnych założeń w klasyfikacji incydentów, określaniu progów

---

9) *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

10) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz. Urz. UE. L 2018 Nr 321, str. 36

11) *Synergies in Cybersecurity Incident Reporting,* NIS Cooperation Group Publication 04/20 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72147

incydentów. Co więcej, podkreślono fakt, że usługi objęte tymi trzema reżimami prawnymi mają krytyczne znaczenie dla społeczeństwa.

Jak już wspomniano wcześniej, sieć 5G będzie jednym z kluczowych elementów mających znaczenie cyberbezpieczeństwa na poziomie państwa. W związku z tym, kwestie związane z budową i funkcjonowaniem sieci 5G nie mogą zostać pominięte w kształtowaniu otoczenia prawnego funkcjonowania krajowego systemu cyberbezpieczeństwa, którego celem jest zapewnienie tego bezpieczeństwa. Ponadto, sieć 5G będzie miała kluczowe znaczenie dla funkcjonowania wszystkich sektorów gospodarki. Pozostawienie jej (podmiotów świadczących dostarczających sieci 5G, czyli operatorów telekomunikacyjnych) poza krajowym systemem cyberbezpieczeństwa znacząco ograniczyłoby możliwość reagowania na pojawiające się cyberzagrożenia.

Obecnie funkcjonują odrębne systemy zgłaszania naruszeń (jak określane są incydenty telekomunikacyjne w obowiązującym Prawie telekomunikacyjnym) przez przedsiębiorców telekomunikacyjnych oraz incydentów przez operatorów usług kluczowych. Przedsiębiorcy telekomunikacyjni zgłaszają naruszenia do Prezesa Urzędu Komunikacji Elektronicznej, podczas gdy operatorzy usług kluczowych zgłaszają incydenty bezpośrednio do właściwych CSIRT'ów. Proponowane w projekcie ustawy zmiany usprawnią przepływ informacji o naruszeniach - incydentach. Stworzony zostanie jednolity system oraz ujednolicone zostaną procedury w zakresie reagowania na incydenty. Rolę koordynacyjną w tym systemie pełnić będą CSIRT poziomu krajowego, każdy w obrębie swojej właściwości podmiotowej.

Bezpieczeństwo sektora telekomunikacji ma wpływ na poprawne funkcjonowanie innych sektorów gospodarki. Incydent telekomunikacyjny może łatwo spowodować np. niedostępność usług bankowych, a więc wstrzymać wykonywanie usług w innym sektorze. W związku z powyższym w projekcie ustawy wprowadzono rozwiązania zwiększające przepływ informacji o incydentach, dzięki którym zarówno CSIRT'y poziomu krajowego, jak i operatorzy usług kluczowych będą sprawniej uzyskiwali informacje o incydentach występujących w innych sektorach. Warto podkreślić, że zespoły CSIRT odpowiadają za szacowanie ryzyka na poziomie krajowym, związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami. Dzięki projektowanym zmianom uzyskają pełen obraz cyberbezpieczeństwa na poziomie krajowym.

Jednocześnie projektowane zmiany umożliwią podłączanie się przedsiębiorców komunikacji elektronicznej do systemu do zgłaszana i reagowania na incydenty, rozwijanego przez ministra właściwego ds. informatyzacji, czyli systemu S46.

<u>Krajowy system certyfikacji cyberbezpieczeństwa</u>

W związku z rosnącą liczbą zagrożeń w cyberprzestrzeni oraz coraz istotniejszą rolą systemów informacyjnych w życiu społeczeństwa, konieczne jest zapewnienie sprawdzonych i bezpiecznych rozwiązań technologicznych zarówno dla sektora publicznego, jak i prywatnego.

Należy także zwrócić uwagę na wzrost liczby cyberprzestępstw, zwłaszcza związanych z wykorzystaniem złośliwego oprogramowania, takiego jak ransomware. Jednym z instrumentów sprzyjających ograniczaniu tego wzrostu jest zapewnienie każdemu zainteresowanemu dostępu do technologii umożliwiających bezpieczne przetwarzanie danych.

Ze względu na wielką różnorodność wykorzystywanych technologii, istotne jest stosowanie jednolitych standardów w zakresie bezpieczeństwa na terenie całej Unii Europejskiej.

Proponowane w ustawie rozwiązania tworzą prawno-organizacyjne warunki funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa, który zapewni wszystkim zainteresowanym podmiotom możliwość testowania, badania produktów ICT, usług ICT i procesów ICT oraz otrzymywania certyfikatów cyberbezpieczeństwa opartych na europejskich programach, a także powszechnie uznawanych na obszarze Unii Europejskiej.

Stworzenie takiego systemu wynika również z bezwzględnie obowiązujących przepisów prawa europejskiego, zawartych w Akcie o cyberbezpieczeństwie. Akt o Cyberbezpieczeństwie z 2018 r. ustanowił europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów.

Akt o cyberbezpieczeństwie nakłada na wszystkie państwa członkowskie obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa, który będzie nadzorował rynek i kontrolował prawidłowość działań w zakresie certyfikacji. W celu wdrożenia rozwiązań przewidzianych w tym akcie normatywnym w Polsce, konieczne jest również wprowadzenie do polskiego systemu prawa przepisów związanych z akredytacją podmiotów uprawnionych do wydawania certyfikatów oraz procedur związanych z działaniem tego systemu, regulujących np. kwestie zatwierdzania certyfikatów o poziomie zaufania „wysoki”.

Przyjęte w ustawie rozwiązania sprawią, że polskie firmy będą mogły swobodnie konkurować na rynku europejskim. Trzeba tu wskazać, że w wielu państwach Europy Środkowej rynek certyfikacji jest mniej rozwinięty niż w Polsce. W związku z tym, przyjęcie procedowanych przepisów może umożliwić polskim przedsiębiorcom przyciągnięcie klientów z regionu.

Przyjęte rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja w dziedzinie cyberbezpieczeństwa będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku.

Certyfikaty

Akt o cyberbezpieczeństwie przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, określające poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. W odniesieniu do każdego z tych poziomów będą określane odrębne wymagania, jakie musi spełniać produkt, by uzyskać certyfikat danego poziomu. Wymagania dla konkretnych produktów będą określane w europejskich lub krajowych programach certyfikacji cyberbezpieczeństwa. Każdy z wydawanych certyfikatów będzie musiał wskazywać jakiego poziomu dotyczy. Również szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji.

Certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym. Ustawa tworzy ramy w jakich będzie wykonywana, równocześnie nie nakładając żadnych obowiązków na podmioty działające na rynku. Każdy chętny będzie więc mógł zarówno rozpocząć działalność w tym zakresie, jak i uzyskać certyfikację swojego produktu, usługi czy procesu ICT, równocześnie nie będąc do tego zobowiązanym.

Przyjęte rozwiązania służą również realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią”. Ustanowienie krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa stanowią działania służące realizacji drugiego celu szczegółowego Strategii – podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. W zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. 2022 r. poz. 1854). Stosowane przepisy proceduralne będą więc dobrze znane i sprawdzone, a nowym elementem będą jedynie wymagania określane dla każdego z poziomów zaufania.

Podjęcie prac związanych z utworzeniem krajowego systemu certyfikacji cyberbezpieczeństwa wynika z jednej strony zarówno z potrzeby dania impulsu do rozwoju rynku w obszarze certyfikacji, jak i zapewnienie bezpiecznych technologii dla zainteresowanych, a z drugiej strony, z konieczności wdrożenia do polskiego porządku prawnego Aktu o cyberbezpieczeństwie.

Strategiczna sieć bezpieczeństwa

Dotychczasowe doświadczenia, jak również różnorodność stosowanych rozwiązań, a co za tym idzie rozproszenie środków, które są wykorzystywane do modernizacji istniejących sieci telekomunikacyjnych,

wykorzystywanych na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego przez kluczowe urzędy i podmioty działające w Rzeczypospolitej Polskiej wskazują na konieczność uruchomienia bezpiecznej sieci telekomunikacyjnej.

Szczególne zasady przeznaczania określonego zasobu z pasma 700 MHz

Decyzja harmonizacyjna (Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii) wskazuje wyraźnie, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa Public Protection & Disaster Relief (PPDR), należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.

Zgodność projektu ustawy z celami strategicznymi Rady Ministrów

Projekt ustawy służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią", jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy Strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

Jednocześnie wprowadzenie w życie projektowanych zmian w ustawie o krajowym systemie cyberbezpieczeństwa zrealizuje kamień milowy reformy C3.1. Krajowego Planu Odbudowy. Zgodnie z tym wymogiem wprowadzone zostaną ramy prawne umożliwiające tworzenie sektorowych sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), tworzenie Centrów Wymiany i Analizy Informacji (ISAC) oraz wzmocni mechanizmy współpracy administracji rządowej z jednostkami samorządu terytorialnego w zakresie reagowania na incydenty bezpieczeństwa.

Zmiany wprowadzane do krajowego systemu cyberbezpieczeństwa

CSIRT sektorowy

Sektorowy zespół cyberbezpieczeństwa zastąpiono CSIRT sektorowymi. W przeciwieństwie do dotychczasowego, fakultatywnego trybu ustanawiania zespołu, w projekcie przewidziano obowiązek ustanowienia przez organ właściwy CSIRT sektorowego dla danego sektora lub podsektora.

CSIRT sektorowy będzie odpowiadał za przyjmowanie zgłoszeń o incydentach pochodzących od operatorów usług kluczowych w danym sektorze lub podsektorze, dla którego został ustanowiony, a także za reagowanie na zgłoszone incydenty. Zakres obowiązków zostanie zatem poszerzony w stosunku do dotychczasowych rozwiązań – obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi kluczowej w reagowaniu na incydenty. CSIRT sektorowy będzie dokonywał również dynamicznej analizy ryzyka i incydentów, a także będzie gromadził informacje o cyberzagrożeniach.

CSIRT INT

W związku z rosnącą liczbą cyberataków na jednostki sektora publicznego konieczne jest dodatkowe wzmocnienie podmiotów z tego sektora. Szczególnie narażone na ataki są placówki dyplomatyczne i konsularne, których położenie i wrażliwy charakter przetwarzanych przez nie informacji sprawia, że udzielenie im wsparcia jest szczególnie utrudnione. Wychodząc naprzeciw tym problemom, powołuje się CSIRT INT, który będzie prowadzony przez szefa Agencji Wywiadu. Jego zadaniem będzie zapewnienie wsparcia placówkom dyplomatycznym i konsularnym w zakresie cyberbezpieczeństwa.

ISAC

Centra Wymiany i Analiz Informacji tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o cyberzagrożeniach i podatnościach oraz wymiana informacji o najlepszych praktykach.

SOC

Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie Operacyjnych Centrów Bezpieczeństwa (zwanych dalej „SOC”). Te nowe podmioty zastąpią dotychczasowe struktury odpowiedzialne za cyberbezpieczeństwo u operatorów usług kluczowych. SOC posiadają ugruntowaną na rynku pozycję zespołów realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek.

Włączenie przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa

Wymaganiami w zakresie cyberbezpieczeństwa zostaną objęci przedsiębiorcy komunikacji elektronicznej przez których rozumie się przedsiębiorców telekomunikacyjnych lub podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów.

Procedura uznania dostawcy za dostawcę wysokiego ryzyka

Odporność na cyberzagrożenia zależy w dużym stopniu od bezpieczeństwa sprzętu ICT, procesów ICT i usług ICT. Dotyczy to zarówno systemów teleinformatycznych, sieci telekomunikacyjnych, jak i przemysłowych systemów sterowania. Z tego względu w projekcie ustawy uwzględniono postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania wykorzystywanego przez kluczowe podmioty gospodarki za dostawcę wysokiego ryzyka. Postępowanie w tej kwestii będzie prowadził minister właściwy do spraw informatyzacji. Postępowanie będzie oparte o transparentną procedurę określoną w Kodeksie postępowania administracyjnego z pewnymi odmiennościami. Każdorazowo, prowadząc postępowanie, minister właściwy do spraw informatyzacji będzie zasięgał opinii Kolegium na temat dostawcy sprzętu lub oprogramowania i dostarczanych przez niego produktów ICT, usług ICT, procesów ICT. W opinii będą uwzględniane zarówno aspekty techniczne, jak i pozatechniczne, mające wpływ na bezpieczeństwo narodowe. Postępowanie będzie kończyło się decyzją administracyjną w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, która będzie podlegać zaskarżeniu do sądu administracyjnego.

Projektowane rozwiązanie nawiązuje do oceny profili ryzyka dostawców, będącej jednym z narzędzi strategicznych (Strategic Measure – SM03), uzgodnionych przez państwa członkowskie Unii Europejskiej, Komisję Europejską i ENISA w 5G Toolbox.

Podmioty krajowego systemu cyberbezpieczeństwa (przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych) oraz przedsiębiorcy telekomunikacyjni będący dużymi przedsiębiorcami, w przypadku wydania decyzji zostaną zobowiązani do wycofania z użycia, określonego w decyzji, w sprzętu lub oprogramowania pochodzące od takiego dostawcy, w terminie 7 lat od wydania decyzji administracyjnej. Natomiast w przypadku gdy produkty, usługi i procesy ICT, objęte decyzją, znajdują się w zakresie objętym wykazem kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług, stanowiącym załącznik nr 3 do ustawy, przedsiębiorcy będą musieli wycofać je w ciągu 5 lat. Podkreślenia wymaga fakt, że obowiązkowi wycofania będą podlegały produkty, usługi i procesy ICT wskazane w decyzji ministra właściwego do spraw informatyzacji – a więc nie wszystkie produkty, usługi i procesy ICT oferowane przez dostawcę wysokiego ryzyka.

Zapobieganie incydentom krytycznym i zwiększenie skuteczności reagowania na incydenty krytyczne

W celu zapobiegania incydentom krytycznym i zwiększenia skuteczności reagowania na nie będą mogły być wydawane ostrzeżenia Pełnomocnika – w przypadku uzyskania informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego.

Krajowe programy certyfikacji cyberbezpieczeństwa

Projekt ustawy przewiduje tworzenie krajowych programów certyfikacji cyberbezpieczeństwa, na podstawie których przeprowadzana będzie certyfikacja. W programach zawarte zostaną techniczne standardy, które będą musiały spełniać produkty, usługi i procesy ICT. Ponadto, programy będą określały

szczegóły związane z procesem certyfikacji, jak również procedury sanacyjne w przypadku, gdy po certyfikacji ujawnią się wady produktów. Wszystkie te elementy muszą być bardzo ściśle dostosowane do konkretnego produktu, usługi czy procesu ICT. Na etapie planowania prac minister właściwy do spraw informatyzacji będzie mógł zlecić przygotowanie ekspertyz, opinii czy projektów dokumentacji podmiotom prywatnym. Pozwoli to wykorzystać wiedzę i doświadczenie podmiotów prywatnych przy przygotowywaniu projektu krajowego programu certyfikacji cyberbezpieczeństwa. Ponadto, narzędzia te będę również służyły zbadaniu czy w danym obszarze przygotowanie takiego programu byłoby w zasadne. W szczególności może on powierzyć przygotowanie takiego projektu jednostkom przez siebie nadzorowanym np. Naukowej i Akademickiej Sieci Komputerowej czy Instytutowi Łączności. Następnie, w ramach zwykłej procedury legislacyjnej, będzie przygotowywane rozporządzenie Rady Ministrów, ustanawiającego dany program. Na tym etapie możliwość wypowiedzenia się o kształcie danego programu będzie miał każdy zainteresowany organ administracji publicznej (art. 59d).

Elementy programu zostały sformułowane na wzór przepisów Aktu o cyberbezpieczeństwie, dotyczących europejskich programów certyfikacji cyberbezpieczeństwa. Dzięki temu wymagania i standardy wobec krajowych i europejskich programów certyfikacji będą bardzo do siebie zbliżone, co sprawi, że nie będzie konieczne tworzenie osobnej terminologii dla krajowych programów certyfikacji. Umożliwi to więc wykorzystanie w jak największym stopniu praktyk wypracowanych w ramach europejskich programów certyfikacji. Ponadto, certyfikaty cyberbezpieczeństwa wydane na podstawie krajowych programów certyfikacyjnych będą mogły, dzięki przyjętym rozwiązaniom, łatwo zostać uznane w innych krajach UE. Możliwe także będzie rozszerzenie rynku certyfikacji przez objęcie programami produktów, usług i procesów ICT nieujętych w europejskich programach certyfikacyjnych. Bliskość z programami europejskimi umożliwi też stosunkowo łatwe przenoszenie programów krajowych na poziom europejski. Będzie to bardzo ważnym narzędziem do kreowania polskiej polityki w zakresie certyfikacji cyberbezpieczeństwa na poziomie europejskim (art. 59 d–g).

Proces certyfikacji będzie prowadzony przez jednostki oceniające zgodność akredytowane przez Polskie Centrum Akredytacji na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i systemach nadzoru rynku. Wykorzystanie już obowiązujących przepisów zapewni możliwie najsprawniejsze wprowadzenie w życie systemu certyfikacji cyberbezpieczeństwa. Polskie Centrum Akredytacji będzie sprawowało nadzór nad akredytacją jednostek oceniających zgodność. Będzie też na bieżąco wymieniać się informacjami z ministrem właściwym do spraw informatyzacji, co zapewni skuteczną kontrolę nad całym systemem (art. 59h).

W przypadku certyfikatów odwołujących się do najniższego z poziomów uzasadnienia zaufania, sami dostawcy sprzętu lub oprogramowania będą mogli wydawać deklaracje zgodności, by wskazać, że ich produkt spełnia dane wymagania (art. 59p–r). Dostawcy sprzętu lub oprogramowania uzyskają zatem możliwość

skorzystania z programów certyfikacyjnych przy jednoczesnym ograniczeniu kosztów uczestnictwa w tych programach.

Strategiczna sieć bezpieczeństwa

W projekcie ustawy przewidziano utworzenie bezpiecznej sieci telekomunikacyjnej na potrzeby realizacji przez kluczowe organy i podmioty działające w Rzeczypospolitej Polskiej zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także określono sposób powołania operatora tej sieci oraz warunki, które musi spełniać ten podmiot.

W tym celu zostanie powołany operator strategicznej sieci bezpieczeństwa, który będzie wyznaczany, przez Prezesa Rady Ministrów spośród podmiotów spełniających łącznie następujące warunki:

a) będących jednoosobową spółką Skarbu Państwa,
b) będących przedsiębiorcą telekomunikacyjnym,
c) posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 76d ust. 1 lub które zobowiązały się do jej pozyskania,
d) posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
e) posiadających świadectwo bezpieczeństwa przemysłowego
f) dających rękojmię należytego wykonywania zadań operatora strategicznej sieci bezpieczeństwa.

Operator ten będzie świadczył usługi telekomunikacyjne, jak również inne usługi dla wskazanych w ustawie podmiotów. Do ustawy wprowadzono możliwość pierwokupu przez OSSB sieci telekomunikacyjnych pozostających we własności Skarbu Państwa lub samorządu terytorialnego. Przyjęcie takiego rozwiązania zapewni sprawną i zoptymalizowaną kosztowo budowę infrastruktury telekomunikacyjnej, wykorzystywanej na potrzeby realizacji zadań, o których mowa powyżej.

Zmiana podziału ustawy w związku z rozbudową aktu normatywnego

Znacznemu poszerzeniu, w stosunku do obowiązującej ustawy, ulega jej zakres przedmiotowy. Wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa przepisów kształtujących krajowy system certyfikacji cyberbezpieczeństwa oraz rozwiązań związanych z utworzeniem i funkcjonowaniem strategicznej sieci bezpieczeństwa, jak również obszerność wprowadzanych zmian, powodują, że niezbędne jest dokonanie podziału ustawy na działy, co służy zachowaniu przejrzystości ustawy. W konsekwencji ustawa została podzielona na cztery działy. Pierwszy dział zawiera ogólne postanowienia, drugi – przepisy dotyczące krajowego systemu cyberbezpieczeństwa, które stanowią niezmiennie podstawową regulację ustawy, wraz z postanowieniami odnoszącymi się do nowego zespołu norm prawnych określających „krajowy system certyfikacji cyberbezpieczeństwa”. Trzeci dział składa się z przepisów dotyczących funkcjonowania strategicznej sieci bezpieczeństwa, zaś czwarty to przepisy końcowe.

Przewidywane skutki społeczne, gospodarcze, prawne i finansowe wprowadzanych zmian

Skutki społeczne

Dzięki wprowadzanym rozwiązaniom, obejmującym utworzenie CSIRT sektorowych, SOC zewnętrznych, SOC wewnętrznych i ISAC, zostanie zwiększona skuteczność funkcjonowania krajowego systemu cyberbezpieczeństwa.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, dzięki którym usprawnione zostanie funkcjonowanie i zwiększona skuteczność systemu reagowania na incydenty. Ponadto, dzięki powołaniu CSIRT sektorowego w każdym sektorze powstanie baza wiedzy o cyberzagrożeniach i podatnościach danego sektora. Funkcjonowanie CSIRT sektorowych wpłynie na skrócenie czasu obsługi incydentów w sektorze, które będą obsługiwane z uwzględnieniem szczególnych uwarunkowań danego sektora. Natomiast centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa.

Przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw i skłoni przedsiębiorców do stosowania bezpieczniejszych, sprawdzonych rozwiązań. To z kolei, dzięki zwiększeniu zakresu wykorzystania rozwiązań odpornych na cyberataki, będzie służyło podniesieniu poziomu bezpieczeństwa obywateli.

Skutki gospodarcze

Celem projektowanych zmian jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wprowadzane projektem ustawy rozwiązania zobowiązują bowiem m.in. przedsiębiorców świadczących usługi kluczowe do dbania o cyberbezpieczeństwo. Skutkiem projektowanych przepisów może być konieczność poniesienia dodatkowych kosztów związanych z dostosowaniem się poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa do wymogów wynikających z ustawy. Na marginesie należy zauważyć, że wielu przedsiębiorców już obecnie posiada operacyjne centra bezpieczeństwa, bowiem podobny do projektowanego wymóg istnieje w obowiązującej ustawie. Dzięki dalszemu inwestowaniu przez podmiot we własne cyberbezpieczeństwo zyskuje on zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom zwiększyć skuteczność działań podejmowanych przez przedsiębiorców w zakresie cyberbezpieczeństwa w ich działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

Dzięki zawartym w ustawie rozwiązaniom podniesione zostaną standardy w zakresie cyberbezpieczeństwa. Prywatni przedsiębiorcy będą mieli ułatwiony wybór bezpiecznych rozwiązań technologicznych. Ponadto, nowe regulacje gwarantują, że certyfikaty uzyskane w ramach systemu certyfikacji dla produktów, usług czy procesów ICT będą honorowane na terenie całej Unii Europejskiej.

Projektowana ustawa zawiera szereg rozwiązań zapewniających właściwe standardy postępowania przy ocenie zgodności, co daje dodatkowe gwarancje jakości.

Krajowy system certyfikacji cyberbezpieczeństwa będzie też stanowił cenne uzupełnienie krajowego systemu cyberbezpieczeństwa. Stworzy bowiem precyzyjny system oceny produktów ICT, dzięki czemu identyfikowane będą produkty spełniające najlepsze standardy w dziedzinie bezpieczeństwa. Projektowane przepisy nie nakładają żadnych dodatkowych obowiązków na podmioty niezainteresowane uczestnictwem w tym systemie. Przyjęty model nie tworzy też barier dostępu do rynku.

Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa będzie wymagało dodatkowych nakładów finansowych. Należy jednak podkreślić, że jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częstsze i bardziej zaawansowane. Drastycznie wzrosła liczba incydentów cyberbezpieczeństwa oraz samych cyberataków, których ofiarami padają urzędy, szpitale, ale także coraz więcej ataków obserwujemy w sektorze prywatnym oraz w stosunku do obywateli. W 2021 r. zespół CSIRT NASK obsłużył 29 483 unikalnych incydentów. Jest to znaczący wzrost w stosunku do 2019 r., w którym CSIRT NASK odnotował 10 420 incydenty. Istnieje także stałe zagrożenie działaniami wywiadowczymi w cyberprzestrzeni.

Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne i bardzo często mają również istotny wymiar finansowy. Inwestycja w dostosowanie krajowego systemu cyberbezpieczeństwa do wyzwań wynikających z postępującej gwałtownie cyfryzacji pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne skutki. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Przyjęcie przepisów o krajowym systemie certyfikacji cyberbezpieczeństwa będzie miało korzystne skutki dla całego sektora przedsiębiorstw. Obecnie firmy ponoszą coraz większe straty w wyniku działalności cyberprzestępców. Wprowadzenie certyfikacji w dziedzinie cyberbezpieczeństwa sprawi, że firmy uzyskają lepszy dostęp do rozwiązań gwarantujących najwyższy poziom bezpieczeństwa. Ponadto, samo zbudowanie systemu certyfikacji cyberbezpieczeństwa przyczyni się do wzrostu świadomości w omawianym obszarze. W efekcie straty ponoszone przez sektor przedsiębiorstw powinny ulec zmniejszeniu.

Skutki prawne

Powstaną nowe rejestry pomagające właściwym instytucjom wykonywać ich zadania ustawowe – wykaz SOC oraz wykaz ISAC.

Minister właściwy do spraw informatyzacji będzie mógł przeprowadzić postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa oraz minister właściwy do spraw informatyzacji uzyskają nowe narzędzia w zakresie zapobiegania cyberzagrożeniom i zwiększenia skuteczności reagowania

na incydenty krytyczne. Również przewodniczący Kolegium do spraw Cyberbezpieczeństwa zostanie wyposażony w szereg nowych kompetencji (m.in. będzie mógł wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1 ustawy; zlecić CSIRT GOV CSIRT MON lub CSIRT NASK przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług albo analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT; będzie również mógł wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka).

Krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował:

- uprawnieniami do nadzoru nad systemem certyfikacji cyberbezpieczeństwa oraz
- narzędziami do usuwania z obiegu prawnego certyfikatów wydanych wbrew przepisom ustawy oraz do kontrolowania podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Ponadto, przepisy ustanawiają podstawę prawną i procedury przyjmowania krajowych programów certyfikacji cyberbezpieczeństwa.

Niniejszą ustawą zostaną zmienione następujące ustawy:

- ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym[12)] – do katalogu spółek w których nie mogą być zbyte akcje lub prawa z akcji należące do Skarbu Państwa zostanie dodana spółka wyznaczona na operatora strategicznej sieci bezpieczeństwa.

Źródła finansowania projektowanych zmian

Wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki z budżetu państwa. Szczegółowy opis źródeł finansowania zawarty jest w ocenie skutków regulacji.

Wyniki przeprowadzonych konsultacji

W dniach 30.06–8.07.2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej.

W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów, wyznaczając termin 14 dni. Jednakże, z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni – łącznie na uwagi było 28 dni.

[12)] Dz. U. 2021 r. poz. 1933 z późn. zm.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, o ile zgłaszający uwagi przekazał informację o zamiarze ich zgłoszenia przed upływem terminu wyznaczonego na przeprowadzenie konsultacji publicznych.

2 Uzasadnienie poszczególnych przepisów

2.1 Zmiany w ustawie o KSC

2.1.1 Zmiany w definicjach, katalogu podmiotów krajowego systemu cyberbezpieczeństwa, zakresu przedmiotowego

Postanowienia ogólne zostają objęte zakresem działu pierwszego (przed art. 1 zostało dodane oznaczenie działu – Postanowienia ogólne). Nowelizacją są również wprowadzane zmiany w poszczególnych przepisach wchodzących w zakres tego działu.

Zmiany w art. 1

Wobec poszerzenia projektowaną ustawą zakresu przedmiotowego ustawy o krajowym systemie cyberbezpieczeństwa w art. 1 wprowadzono odpowiednie zmiany – w ust. 1 tego artykułu zostały dodane pkt 1a oraz 4–6, zgodnie z którymi zakres przedmiotowy ustawy obejmuje także:

- zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa sieci lub usług komunikacji elektronicznej i zgłaszania incydentów telekomunikacyjnych,
- krajowy system certyfikacji cyberbezpieczeństwa,
- zasady i tryb wyznaczania operatora strategicznej sieci bezpieczeństwa oraz jego zadania,
- zasady przyznania zasobów częstotliwości z zakresu 703–733 MHz oraz 758–788 MHz.

Dostosowaniu do projektowanych zmian o charakterze systemowym uległ art. 1 ust. 2. W związku z wynikającym z implementacji art. 40 i 41 EKŁE włączeniem do krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, konieczne jest uchylenie pkt 1 w art. 1 ust. 2, zgodnie z którym przepisów obowiązującej ustawy nie stosuje się do tych przedsiębiorców.

Jednocześnie projekt ustawy przewiduje, że do dostawców usług zaufania będą stosować się przepisy o ostrzeżeniu.

Nowe brzmienie art. 2

Uporządkowany i uzupełniony został słowniczek pojęć używanych w ustawie o krajowym systemie cyberbezpieczeństwa (art. 1 pkt 3 dotyczący art. 2 ustawy o krajowym systemie cyberbezpieczeństwa). Wprowadzone zostały do niego definicje takich pojęć, jak: akredytacja, certyfikat, cyberzagrożenie, deklaracja zgodności, dostawca, incydent telekomunikacyjny, ISAC, jednostka oceniająca zgodność, krajowy

certyfikat cyberbezpieczeństwa, krajowa deklaracja zgodności, krajowy program certyfikacji cyberbezpieczeństwa, krajowy poziom uzasadnienia zaufania, obsługa incydentu, ocena zgodności, proces ICT, produkt ICT, przedsiębiorca komunikacji elektronicznej, SOC wewnętrzny, SOC zewnętrzny, usługa ICT, usługi komunikacji elektronicznej.

Definicja akredytacji (pkt 1) odwołuje się do akredytacji w rozumieniu art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93[13)], zwane dalej „rozporządzeniem 765/2008". Zgodnie z tym rozporządzeniem akredytacja oznacza poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności.

Wprowadza się nową definicję bezpieczeństwa sieci lub usług komunikacji elektronicznej (pkt 2). Pod tym pojęciem rozumie się zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność integralność lub poufność tych sieci lub usług, jak i przetwarzanych informacji objętych tajemnicą komunikacji elektronicznej, a także innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy. Przepis stanowi wdrożenie art. 2 pkt 21 EKŁE.

Akt o cyberbezpieczeństwie wprowadził definicję cyberbezpieczeństwa, która różni się od tej stosowanej na gruncie obowiązującej ustawy. Z tego względu wprowadzono nową definicję cyberbezpieczeństwa, zgodną z Aktem o cyberbezpieczeństwie – są to działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami (pkt 11). Natomiast dotychczasowemu brzmieniu definicji cyberbezpieczeństwa odpowiada definicja bezpieczeństwa systemów informacyjnych (art. 2 pkt 3). Zmiany te nie powodują zmian w zakresie konkretnych obowiązków nałożonych obowiązującą ustawą na podmioty krajowego systemu cyberbezpieczeństwa. Nowe definicje są zgodne z przepisami zawartymi w Akcie o cyberbezpieczeństwie. Wprowadzane zmiany definicyjne nie tylko zapewniają zgodność z polskim porządkiem prawnym, ale również odpowiednią przejrzystość przepisów.

Ponadto, projektowana ustawa posługuje się pojęciami certyfikat (pkt 4) oraz krajowy certyfikat cyberbezpieczeństwa (pkt 25). Certyfikat odnosi się do wszystkich certyfikatów w dziedzinie cyberbezpieczeństwa, tj. zarówno tych wydanych w ramach krajowych, jak i europejskich programów

---

[13)] Dz. Urz. UE L 218 z 13.08.2008, str. 30 oraz Dz. Urz. UE L 169 z 25.06.2019, str. 1..

certyfikacji. Z kolei krajowy certyfikat cyberbezpieczeństwa dotyczy tylko dokumentów wydanych na podstawie krajowych programów certyfikacji . Certyfikaty te będą traktowane jednakowo. Wiele kwestii związanych z europejskimi certyfikatami zostało określonych w Akcie o cyberbezpieczeństwie. Przepisy te nie odnoszą się jednak do certyfikatów krajowych. Z tego też względu w projekcie ustawy znalazły się przepisy regulujące kwestie związane z wydawaniem certyfikatów krajowych. Analogiczna sytuacja występuje w przypadku deklaracji zgodności i krajowych deklaracji zgodności (pkt 26). Te ostatnie zostały wprowadzone aby zagwarantować, że również w wypadku certyfikatów krajowych możliwe będzie potwierdzenie zgodności przez samego przedsiębiorcę w określonych przypadkach. Konsekwencją tych zmian była konieczność dostosowania pozostałych przepisów ustawy.

W niezmienionej formie pozostawiono dotychczasowe definicje zespołów CSIRT GOV, CSIRT MON oraz CSIRT NASK (pkt. 5–7).

Wprowadzono definicję CSIRT sektorowego (pkt 9) – przez który należy rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. Definicja ta jest utrzymana w podobnej konwencji jak definicje poszczególnych zespołów CSIRT poziomu krajowego.

Zaproponowano także definicję CSIRT INT (pkt 8) – jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Szefa Agencji Wywiadu na rzecz Agencji Wywiadu oraz jednostek organizacyjnych podległych ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowanych.

Wprowadzono również definicję CSIRT Telco (pkt 10) – jako Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na rzecz przedsiębiorców komunikacji elektronicznej.

Pojęcie „zagrożenie cyberbezpieczeństwa" zostało zastąpione pojęciem „cyberzagrożenia" (art. 2 pkt 12), które zostało wprowadzone w Akcie o cyberbezpieczeństwie, a jego definicja jest bardzo zbliżona do funkcjonującej w naszym systemie prawnym definicji „zagrożenia cyberbezpieczeństwa". Nie jest zasadne utrzymywanie w systemie prawnym obu tych pojęć i dlatego pozostawiono jedynie sformułowanie „cyberzagrożenie". Pojęcie „cyberzagrożenie" jest zgodne z najnowszą terminologią w dziedzinie cyberbezpieczeństwa stosowaną w państwach członkowskich Unii Europejskiej. W związku z tą zmianą dostosowano definicję podatności (art. 2 pkt 31) zastępując wyrazy „zagrożenie cyberbezpieczeństwa" wyrazem „cyberzagrożenie".

Definicja dostarczania sieci telekomunikacyjnej (pkt 14) odwołuje się do definicji z art. 2 pkt 5 ustawy –Prawo komunikacji elektronicznej. Jest ona potrzebna z uwagi na dodawany nowy rozdział 4a.

Definicja deklaracji zgodności została sformułowana analogicznie do definicji deklaracji z ustawy o systemach oceny zgodności i nadzoru rynku.

Nowością jest definicja dostawcy – tutaj projekt odwołuje się do art. 2 pkt 3–6 rozporządzenia 765/2008. Dostawcą jest:

- producent - każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym;
- upoważniony przedstawiciel - osoba fizyczna lub prawna mająca siedzibę w Unii Europejskiej, posiadająca pisemne pełnomocnictwo od producenta do występowania w jego imieniu w zakresie określonych zadań w odniesieniu do obowiązków producentów wynikających z odpowiedniego prawodawstwa wspólnotowego;
- importer - każda osoba fizyczna lub prawna, mająca siedzibę w Unii Europejskiej, wprowadzająca na rynek wspólnotowy produkt z kraju trzeciego;

  lub

- dystrybutor - każda osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt na rynku.

Definicja jest wprowadzana w związku z przepisami dotyczącymi krajowego systemu certyfikacji cyberbezpieczeństwa, a także przepisami odnoszącymi się do postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Dostosowaniu do zmiany wynikającej ze zmiany brzmienia definicji cyberbezpieczeństwa ulega definicja incydentu (pkt 16) – w miejsce wyrazu „cyberbezpieczeństwo" wprowadzane są wyrazy „bezpieczeństwo systemów informacyjnych".

Wobec zmiany zakresu przedmiotowego ustawy, konieczne stało się zdefiniowanie nowego rodzaju incydentu, czyli incydentu telekomunikacyjnego (pkt 20). Jest to każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. Definicja ta nawiązuje do art. 2 pkt 42 EKŁE. Jednocześnie w definicji incydentu krytycznego (pkt 17) uwzględniono, że incydentem krytycznym może być również incydent telekomunikacyjny.

Incydent telekomunikacyjny jest zdarzeniem ściśle związanym z przedsiębiorcami komunikacji elektronicznej. Jego wyodrębnienie obok „incydentu" wynika z konieczności implementacji EKŁE. Akt ten inaczej definiuje incydent telekomunikacyjny niż dyrektywa NIS. Odnosi się bowiem do pojęcia bezpieczeństwa sieci lub usług komunikacji elektronicznej, tymczasem w dyrektywie NIS incydent odnosi się do pojęcia bezpieczeństwa systemów informacyjnych. Incydent telekomunikacyjny wprost, pod kątem językowym, odnosi się do usług komunikacji elektronicznej. Stąd też, aby zapewnić pełne wdrożenie EKŁE w tym zakresie, wprowadzono definicję incydentu telekomunikacyjnego. Wszędzie tam, gdzie przepisy

odnoszą się do przedsiębiorców komunikacji elektronicznej, projekt odnosi się do pojęcia incydentu telekomunikacyjnego. Dzieje się tak nie tylko przy rozdziale 4a, ale np. przy art. 26 dot. właściwości i kompetencji zespołów CSIRT poziomu krajowego, które będą reagować na incydenty telekomunikacyjne zgłaszane przez przedsiębiorców komunikacji elektronicznej.

Pozostawiono dotychczasowe definicje incydentu poważnego (pkt 18) oraz istotnego (pkt 19), oraz incydentu w podmiocie publicznym (pkt 21).

Definicja ISAC (art. 2 pkt 22), czyli centrum wymiany i analizy informacji na temat podatności cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa wprost nawiązuje do angielskiego rozwinięcia tego skrótu – Information Sharing and Analysis Center.

Przy definicji jednostki oceniającej zgodność – projekt odwołuje się do art. 2 pkt 13 rozporządzenia 765/2008. Jednostka oceniająca zgodność to jednostka, która wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, badanie, certyfikację i inspekcję.

Wprowadza się definicję komunikatu elektronicznego (pkt 24) – która odsyła do definicji z art. 2 pkt 19 Prawa komunikacji elektronicznej jest to każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej. Definicja ta nie obejmuje informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania użytkownika otrzymującego informację. Definicja ta jest potrzebna z uwagi na uprawnienie przedsiębiorców telekomunikacyjnych do blokowania komunikatów elektronicznych stwarzających zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej.

Wprowadzone zostały pojęcia produktu ICT (art. 2 pkt 34), usługi ICT (art. 2 pkt 45) oraz procesu ICT (art. 2 pkt 33). Te trzy pojęcia służą objęciu systemem certyfikacji jak największego zakresu dostępnych na rynku świadczeń. Produkt oznacza „element lub grupę elementów systemów informacyjnych". Będzie więc obejmował praktycznie wszystkie przypadki oprogramowania oraz urządzeń podlegających certyfikacji. Usługi ICT to wszelkie działania związane z przetwarzaniem informacji za pośrednictwem systemów informacyjnych. Proces ICT oznacza „zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT". Są to więc wszelkiego rodzaju działania związane z tworzeniem systemów informacyjnych i ich bieżącym utrzymaniem.

W art. 2 pkt 38 i 39 wprowadza się definicję SOC wewnętrznych i SOC zewnętrznych. Są to zespoły pełniące funkcję operacyjnego centrum bezpieczeństwa odpowiednio wewnątrz struktury operatora usługi kluczowej (SOC wewnętrzny) oraz zewnętrzne, działające na jego rzecz (SOC zewnętrzny). Definicja wprost nawiązuje do terminu przyjętego powszechnie w praktyce (Security Operations Center) różnicując jedynie

formę świadczenia usług SOC w zależności od tego, czy operator usługi kluczowej realizuje zadania przy pomocy własnych zasobów, czy też zleca, na podstawie umowy, realizację tych zadań wyspecjalizowanemu podmiotowi zewnętrznemu.

Dodano definicję przedsiębiorcy komunikacji elektronicznej (art. 2 pkt 35) odnosi się do definicji zawartej w art. 2 pkt 39 ustawy – Prawo komunikacji elektronicznej. Jest to przedsiębiorca telekomunikacyjny lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów. Z kolei definicja przedsiębiorcy telekomunikacyjnego (pkt 36) odnosi się do art. 2 pkt 40 ustawy – Prawo komunikacji elektronicznej.

Pozostawiono dotychczasową definicję ryzyka (pkt 37), a także szacowania ryzyka (pkt 40). Zachowano również dotychczasową definicję systemu informacyjnego (pkt 41).

Definicja sytuacji szczególnego zagrożenia (art. 2 pkt 42) odwołuje się do definicji z art. 2 pkt 65 ustawy -Prawo komunikacji elektronicznej. Obejmuje ona sytuacje, które wymagają współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy, zarządzania kryzysowego, utrzymania porządku publicznego oraz obronności i bezpieczeństwa państwa:

- w przypadku wystąpienia sytuacji kryzysowej, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2023 r. poz. 122),

- w czasie obowiązywania stanów nadzwyczajnych,

- w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,

Ponadto, definicja ta obejmuje sytuację stanowiącą bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej.

Definicja telekomunikacyjnego urządzenia końcowego odwołuje się do definicji z art. 2 pkt 71 ustawy - Prawo komunikacji elektronicznej.

Definicja usługi komunikacji elektronicznej (art. 2 pkt 47) odwołuje się do definicji z art. 2 pkt 76 ustawy - Prawo komunikacji elektronicznej. Określa te usługi jako usługi świadczone za pośrednictwem sieci telekomunikacyjnej, zwykle za wynagrodzeniem, z wyłączeniem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci telekomunikacyjnych lub usług komunikacji elektronicznej. Usługi komunikacji elektronicznej obejmują:

a) usługi dostępu do Internetu w rozumieniu art. 2 akapit drugi pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego Internetu i dotyczące opłat detalicznych za uregulowane usługi łączności wewnątrzunijnej oraz

zmieniającego dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012 (Dz. Urz. UE L 310 z 26.11.2015, str. 1–18, z późn. zm.),

b) usługi komunikacji interpersonalnej,

c) usługi polegające całkowicie lub głównie na przekazywaniu sygnałów, w tym usługi transmisyjne stosowane na potrzeby świadczenia usług komunikacji maszyna - maszyna oraz na potrzeby nadawania.

Pozostawiono dotychczasowe brzmienie definicji zarządzania incydentem (pkt 48) oraz zarządzania ryzykiem (pkt 49).

Po art. 2 zostanie dodane oznaczenie działu II – Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa (art. 1 pkt 4 projektu ustawy).

Zmiany w art. 3

Dotychczasową treść art. 3 oznaczono jako ustęp pierwszy. Dodano ustęp drugi zgodnie z którym ustawa ma zastosowanie we wszystkich stanach gotowości obronnej państwa. Uzupełnienie ustawy o powyższe sformułowanie pozwoli uniknąć wątpliwości co do ograniczeń w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. Tym samym wzmocniony zostanie defensywy potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa. Zapis ten zapewni ciągłość realizacji kompetencji przez krajowy system cyberbezpieczeństwa w stanach pokoju, kryzysu i wojny. Umożliwi współdziałanie lub współpracę podmiotów krajowego systemu cyberbezpieczeństwa w realizacji zadań operacyjnych związanych z zabezpieczeniem potrzeb obronnych w stanie pokoju jak i ich realizacji w wyższych stanach gotowości obronnej państwa.

Nowy art. 3a

W związku z pojawiającymi się wątpliwościami dotyczącymi uprawnień podmiotów krajowego systemu cyberbezpieczeństwa przy obsłudze incydentu został dodany art. 3a, w którym doprecyzowano, że w przypadku wystąpienia incydentu podmioty te mogą, w ramach obsługi incydentów, w szczególności podejmować działania w celu: wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu oraz czasowego ograniczenia ruchu sieciowy z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu. W przypadku wielu cyberataków takie działania są niezbędne w celu ochrony systemu, przy czym w praktyce działania te mogą naruszyć okresowo prawa określonych użytkowników. Z powyższych względów konieczne jest wskazanie wprost, że takie działania są dopuszczalne prawnie, jednakże wyłącznie w określonej sytuacji.

Zmiana art. 4

W nowelizacji art. 4, który zawiera katalog podmiotów krajowego systemu cyberbezpieczeństwa wprowadza się szereg zmian. Proponuje się także dodanie nowych podmiotów: przedsiębiorców komunikacji

elektronicznej, CSIRT Telco, CSIRT INT oraz ISAC znajdujące się w wykazie ISAC. Ponadto w katalogu uwzględniono:

- Urząd Komisji Nadzoru Finansowego (UKNF pierwotnie znajdował się w krajowym systemie cyberbezpieczeństwa jako jednostka budżetowa; jednakże w związku ze zmianą ustawy o nadzorze nad rynkiem finansowym zmienił formę prawną działania – stał się państwową osobą prawną, wobec czego już nie był w systemie [14)]),
- uczelnie, Polską Akademię Nauk i jej instytuty, międzynarodowe instytuty naukowe, Centrum Łukasiewicz wraz z instytutami oraz Polską Akademię Umiejętności, odwołując się do ustawy z 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce.

W konsekwencji wprowadzonych w art. 2 zmian, w art. 4 pkt 16 zamieniono wyrazy „podmiotów świadczących usługi cyberbezpieczeństwa" na wyrazy „SOC zewnętrzne". Z kolei sektorowe zespoły cyberbezpieczeństwa zastąpiono CSIRT sektorowymi.

Funkcjonujący obecnie krajowy system cyberbezpieczeństwa nie obejmuje innych istotnych dla funkcjonowania państwa podmiotów, takich jak:

- Państwowe Gospodarstwo Wodne Wody Polskie,
- instytucje rozwoju:
    - Polski Fundusz Rozwoju,
    - Polska Agencja Rozwoju Przedsiębiorczości,
    - Korporacja Ubezpieczeń Kredytów Eksportowych Spółka Akcyjna,
    - Polska Agencja Inwestycji i Handlu Spółka Akcyjna,
    - Agencja Rozwoju Przemysłu Spółka Akcyjna.

Państwowe Gospodarstwo Wodne Wody Polskie jako podmiot zajmujący się gospodarką wodną realizuje ważne zadania publiczne – zapobieganie suszom i powodziom oraz zapewnianie dobrej jakości wody dla mieszkańców Polski, zapewniając również Informatyczny System Osłony Kraju (ISOK). Z kolei instytucje rozwoju realizują zadania w obszarze wsparcia lub usług świadczonych przedsiębiorcom. W szczególności Polski Fundusz Rozwoju S.A. realizuje program Tarczy Antykryzysowej. Z tych powodów zasadne jest ich dodanie do katalogu podmiotów krajowego systemu cyberbezpieczeństwa.

[14)] Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz. U. poz. 2243 oraz z 2019 r. poz. 875 i 2217).

Do krajowego systemu cyberbezpieczeństwa zostaną dodane także samodzielne publiczne zakłady opieki zdrowotnej, które podczas pandemii COVID-19 pełnią szczególną rolę. Dlatego konieczne jest objęcie tych podmiotów obowiązkami z art. 21–23 ustawy o krajowym systemie cyberbezpieczeństwa, a także zapewnienie im wsparcia właściwego zespołu CSIRT poziomu krajowego w przypadku wystąpienia incydentu w podmiocie publicznym.

2.1.2 Przepisy o operatorach usług kluczowych oraz SOC

Zmiany w art. 7

W art. 7 dodano przepis umożliwiający ministrowi właściwemu do spraw informatyzacji wpisanie z urzędu operatora usługi kluczowej z sektora infrastruktury cyfrowej do wykazu operatorów usług kluczowych. Jest to spowodowane tym, że minister właściwy do spraw informatyzacji jest organem właściwym do spraw cyberbezpieczeństwa dla operatorów usług kluczowych z tego sektora. Jednocześnie minister prowadzi wykaz operatorów usług kluczowych. Na podstawie dotychczasowych przepisów minister musiał składać sam do siebie wnioski o wpisanie do tego wykazu, co nie ma racjonalnego uzasadnienia.

Jak wskazuje doktryna termin sześciu miesięcy na wystąpienie organu właściwego ds. cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych nie gwarantuje aktualności wykazu[15)]. Projektodawca proponuje więc, aby organ właściwy do spraw cyberbezpieczeństwa dokonał tej czynności niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych (zmiana w art. 7 ust. 4). Ponadto w propozycji nowelizacji art. 7 ust. 5 dodaje się możliwość podpisania wniosku o wpisanie operatora usługi kluczowej do wykazu operatorów także podpisem osobistym. Podpis osobisty został uregulowany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych[16)]. Jest to zaawansowany podpis elektroniczny umieszczony w warstwie elektronicznej dowodu osobistego. Podpisanie danych podpisem osobistym ma taki sam skutek wobec podmiotu publicznego co podpis własnoręczny[17)].

Zmiany w art. 8

Art. 8 obecnie obowiązującej ustawy określa wymagania, co do systemu zarządzania bezpieczeństwem informacji (SZBI), który operator usługi kluczowej ma obowiązek wdrożyć w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. SZBI powinno zapewniać stosowanie środków zapobiegających i ograniczających wpływ incydentów na system informacyjny wykorzystywany do świadczenia usługi kluczowej. Jednym z tych środków jest dbałość o aktualizację oprogramowania (art. 8 pkt 5 lit. b). Projektodawca proponuje doprecyzować ten przepis poprzez zastąpienie nieostrego sformułowania „dbałość o aktualizację oprogramowania" sformułowaniem „regularne przeprowadzanie aktualizacji

---

15) G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), Ustawa o krajowym systemie cyberbezpieczeństwa: komentarz, Warszawa 2019., str. 113.

16) Dz. U. 2022 r. poz. 671.

17) Art. 12d ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. 2022 r. poz. 671).

oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji". Operator usługi kluczowej będzie odtąd obowiązany systematycznie przeprowadzać aktualizacje oprogramowania. Przepis ma zapobiegać sytuacji, w której aktualizacje były dokonywane zbyt rzadko. Jednocześnie podejmując decyzję o aktualizacji, operator usługi kluczowej powinien dokonać analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz ocenić poziom krytyczności poszczególnych aktualizacji. Celem tej analizy jest zabezpieczenie przed sytuacją, w której konkretna aktualizacja oprogramowania w istocie zagraża bezpieczeństwu świadczonej usługi kluczowej. Należy podkreślić, że to operator usługi kluczowej jest odpowiedzialny za bezpieczeństwo swoich systemów informacyjnych. Dlatego nie powinien bezrefleksyjnie kierować się zaleceniami producenta sprzętu, ale powinien samodzielnie oceniać wpływ aktualizacji na jego systemy.

Zmiany w art. 9

Do tej pory operatorzy usługi kluczowej mieli obowiązek wyznaczyć jedną osobę do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa oraz przekazać jej dane do organu właściwego do spraw cyberbezpieczeństwa oraz do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa. Proponuje się zmianę polegającą na tym, że operatorzy będą obowiązani wyznaczyć nie jedną, a dwie takie osoby. Dzięki temu zawsze będzie dostępna osoba, z którą zespoły CSIRT będą mogły skontaktować się w razie potrzeby, np. w celu przekazania informacji o zidentyfikowanym cyberzagrożeniu. Proponuje się także uproszczenie sposobu przekazywania danych tych osób. Operator usługi kluczowej przekaże je wyłącznie organowi właściwemu do spraw cyberbezpieczeństwa, który z kolei niezwłocznie przekaże je do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego. Tak więc zamiast wysyłać informacje do 3 instytucji (organ właściwy, CSIRT poziomu krajowego i sektorowy zespół cyberbezpieczeństwa) zgłoszenie zostanie przekazane tylko do jednej – organu właściwego do spraw cyberbezpieczeństwa.

Zmiany w art. 10

W nowelizowanym art. 10 ust. 2 pkt 2 rozszerzono obowiązki nadzoru operatora usługi kluczowej nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego. Do tej pory operator miał chronić dokumenty przed niewłaściwym użyciem lub utratą integralności. Rozszerzono to o ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą oraz nieuprawnionym dostępem. Operator usługi kluczowej zostanie przez to obowiązany zapewnienia pełnej ochrony dokumentacji.

Zmiany w art. 11

Zgodnie z nowymi zmianami w art. 11 operator usługi kluczowej będzie zgłaszał, za pomocą systemu teleinformatycznego, o którym mowa w art. 46, incydenty poważne do CSIRT sektorowego, który następnie niezwłocznie przekaże je do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. W ten sposób

zostanie ograniczony ustawowy obowiązek zgłaszania incydentów poważnych do jednego podmiotu, jednocześnie wzmacniając rolę CSIRT sektorowych. Uprości to procedurę zgłaszania incydentów przez operatorów usług kluczowych.

Operator usługi kluczowej może być także przedsiębiorcą telekomunikacyjnym. Potencjalnie jest możliwa sytuacja, gdy to samo zdarzenie będzie zarówno incydentem poważnym jak i poważnym incydentem telekomunikacyjnym. Dla uproszczenia obowiązków proponuje się (nowe ust. 3a–3b w art. 11), żeby zgłoszenie takiego incydentu było przekazywane do właściwego CSIRT sektorowego. Zespół ten niezwłocznie przekaże zgłoszenie także do CSIRT Telco. Operator usługi kluczowej będzie obowiązany w tej sytuacji współpracować również z CSIRT Telco.

Zmiany w art. 13

Zmiany w artykule 13 wskazują, że co do zasady operator usługi kluczowej będzie przekazywał inne fakultatywne informacje o incydentach, cyberzagrożeniach, podatnościach itd. do właściwego dla niego CSIRT sektorowego. Zespół ten przekaże te informacje dalej do CSIRT poziomu krajowego, jeżeli jest to zasadne. Zmiana wzmacnia pozycję CSIRT sektorowego stawiając go bliżej operatora usługi kluczowej z danego sektora.

Zmiany w art. 14

W nowelizacji zostało zaproponowane zupełnie nowe brzmienie art. 14. Wskazano w nim, że zadania operatorów usług kluczowych w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach SOC wewnętrznych i SOC zewnętrznych. SOC będzie więc:

- wdrażał system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (art. 8),
- wyznaczał osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa (art. 9),
- prowadził i nadzorował dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 10 ust. 1–3),
- obsługiwał incydenty, zgłaszał incydenty poważne do właściwego CSIRT sektorowego (art. 11 ust. 1–3 oraz art. 12),
- przekazywał inne informacje o incydentach, cyberzagrożeniach (art. 13).

Obecnie zadania te wykonują wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Sam zakres zadań nie zmieni się.

Zgodnie z projektowanym ust. 2 SOC może być powołany wewnątrz organizacji danego operatora usługi kluczowej (SOC wewnętrzny) lub stanowić odrębny podmiot (SOC zewnętrzny). W tym drugim przypadku

operator usługi kluczowej jest obowiązany poinformować organ właściwy do spraw cyberbezpieczeństwa o zawarciu umowy z zewnętrznym podmiotem realizującym zadania SOC, jego danych kontaktowych i zakresie świadczonej usługi na rzecz tego operatora.

Należy podkreślić, że każdy z operatorów usług kluczowych może swobodnie wybrać w jakim modelu prowadzony jest SOC zewnętrzny lub SOC wewnętrzny. Nie musi on być jedną konkretną jednostką w jego strukturze, jego zadania mogą być realizowane przez pracowników różnych komórek wewnętrznych danej organizacji. Możliwe jest również zawarcie umowy z kilkoma podmiotami zewnętrznymi w kwestii usług SOC i dowolnie rozdzielić pomiędzy nimi zadania. Możliwy jest także częściowy outsourcing tzn., że część zadań będzie wykonywana w SOC wewnętrznym, a część w SOC zewnętrznym. Niezależnie od wybranego modelu operator usługi kluczowej ponosi odpowiedzialność za zapewnienie ciągłości usługi kluczowej.

Wprowadza się także możliwość, aby SOC zewnętrzny mógł być utworzony na rzecz operatora usługi kluczowej przez organ tworzący lub nadzorujący operatora usługi kluczowej (ust. 3).

Wyraźnie wskazano, że SOC wewnętrzny może świadczyć swoje usługi na rzecz innych podmiotów (ust. 4). Jest to przydatne w sytuacji np. grupy kapitałowej, w której może się znajdować kilku operatorów usług kluczowych. Takie rozwiązanie pomoże zoptymalizować koszty ponoszone przez operatorów usług kluczowych. Należy przy tym zauważyć, że SOC wewnętrzny świadczący usługi również dla innego operatora usługi kluczowej będzie dla niego SOC zewnętrznym i w zakresie tej działalności będzie podlegał nadzorowi ministra właściwego do spraw informatyzacji.

Nowe brzmienie art. 14 ust. 5 nakazuje SOC wewnętrznym i SOC zewnętrznym wprowadzić, na podstawie przeprowadzonego szacowania ryzyka, zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów informacyjnych, a także eksploatacji i architektury systemów informacyjnych. Przepis ten upraszcza obowiązki operatorów usług kluczowych. W obecnym brzmieniu ustawy wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa są obowiązane:

1) spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej;

2) dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi;

3) stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo zostały określone w rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w *sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*[18)]. Proponuje się rezygnację z precyzowania tych warunków w rozporządzeniu – w zamian SOC wewnętrzny czy SOC zewnętrzny będą obowiązane przeprowadzić szacowanie ryzyka i wprowadzić odpowiednie zabezpieczenia, proporcjonalne do oszacowanego ryzyka.

Jeżeli operator usługi kluczowej zawiera z podmiotem trzecim umowę o świadczenie usług SOC to o umowie i jej szczegółach będzie obowiązany niezwłocznie poinformować organ właściwy ds. cyberbezpieczeństwa.

W niezbędnych sytuacjach SOC wewnętrzne i SOC zewnętrzne mają zapewnić bezpieczny zdalny dostęp do swoich systemów informacyjnych dla obsługiwanego operatora usługi kluczowej. Istotne jest, aby opracować procedury i stosować środki, które zminimalizują zagrożenie wycieku danych z SOC. Podobny przepis znajduje się w ww. rozporządzeniu i jego celem jest umożliwienie realizacji zadań zdalnie.

Zgodnie z art. 14 ust. 8 do umów o świadczenie usług SOC stosuje się przepisy prawa polskiego. Przepis ten stanowi gwarancję, że zagraniczne podmioty świadczące usługi z zakresu cyberbezpieczeństwa będą musiały stosować polskie przepisy. Ponadto, infrastruktura SOC powinna znajdować się na terytorium Rzeczypospolitej Polskiej, a personel posiadać odpowiednie poświadczenia bezpieczeństwa osobowego – do poziomu *poufne*. Nakaz posiadania infrastruktury SOC na terytorium RP zapewni możliwość skutecznej kontroli wykonywania obowiązków SOC, a także ograniczy wpływ podmiotów zagranicznych na funkcjonowanie SOC. Z kolei wymóg posiadania przez personel (tj. pracowników i osoby realizujących zadania w SOC na podstawie stosunków cywilnoprawnych) poświadczenia bezpieczeństwa do poziomu poufne umożliwi bezpieczne przekazywanie informacji niejawnych dot. podatności i cyberzagrożeń do SOC.

Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350[19)]) wprowadza się obowiązek, aby SOC zewnętrzne były obowiązane udostępniać na stronie internetowej podstawowe informacje o swojej działalności. W celu

---

[18)] Dz. U. z 2019 r. poz. 2479.

[19)] https://datatracker.ietf.org/doc/html/rfc2350 .
Jako przykłady praktyki można wskazać:
https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf
https://www.csirt.gov.sk/csirt-sk-description-document-according-to-rfc-2350.html
https://www.ncsc.gov.ie/pdfs/RFC2350%20NCSC-IE.txt.

zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej SOC zewnętrznego.

Podsumowując, zmiany w art. 14 mają ułatwić wykonywanie zadań przez operatorów usług kluczowych. Podkreślić przy tym należy, że w związku ze zmianami w art. 14 straci moc rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w *sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo*[20)].

Nowy art. 14a

Aby odpowiednie urzędy i służby miały dostęp do danych SOC w zakresie swoich ustawowych kompetencji, minister właściwy do spraw informatyzacji będzie prowadził wykaz SOC. Zostanie on uregulowany w nowym art. 14a. W wykazie znajdą się zarówno SOC wewnętrzne jak i SOC zewnętrzne.

Głównym celem funkcjonowania wykazu SOC jest ułatwienie ministrowi właściwemu do spraw informatyzacji realizacji funkcji nadzoru na SOC. Obecnie istniejące rejestry czy ewidencje nie pozwalają na dokładne ustalenie podmiotów, które świadczą usługi SOC na rzecz operatorów usług kluczowych. Ponadto obecny art. 14 ust. 3 nie uprawnia do przekazywania informacji o podmiotach świadczących usługi z zakresu cyberbezpieczeństwa do ministra właściwego do spraw informatyzacji od organów właściwych do spraw cyberbezpieczeństwa, CSIRT poziomu krajowego i sektorowych zespołów cyberbezpieczeństwa.

Wykaz będzie zawierał podstawowe dane o podmiocie prowadzącym SOC, na rzecz jakich podmiotów jest prowadzony, siedzibę i adres SOC wewnętrznego lub SOC zewnętrznego, numer NIP, numer we właściwym rejestrze oraz datę wpisania i wykreślenia z wykazu SOC. Wpis do wykazu będzie następował na wniosek organu właściwego do spraw cyberbezpieczeństwa. Organ będzie posiadał o tym informacje, ponieważ operator usługi kluczowej będzie miał obowiązek przekazywać informacje o powołaniu SOC wewnętrznego lub zawarcia umowy z SOC zewnętrznym. W przypadku gdy dla operatora usług kluczowych organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji (który jednocześnie prowadzi wykaz SOC), to ten minister nie będzie składał sam do siebie wniosków tylko wpisze informacje o SOC z urzędu. Oczywiście będzie możliwa zmiana danych w wykazie SOC, jeśli zostanie zmieniona firma podmiotu prowadzącego SOC. Wnioski o wpis, zmianę danych czy wykreślenie danych będą sporządzane w postaci elektronicznej i opatrywane kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Ułatwi to przekazywanie danych do wykazu SOC i usprawni pracę pracowników obsługujących ministra właściwego do spraw informatyzacji.

Wprowadza się regułę zgodnie z którą wpis, wykreślenie oraz zmiana danych w wykazie SOC będą czynnościami materialno-technicznymi, w związku z czym nie będą podlegały zaskarżeniu. Jest to związane

---

[20)] Dz. U. z 2019 r. poz. 2479.

z tym, że czynności te nie kreują żadnych uprawnień i nie nakładają żadnych obowiązków na podmioty wpisane do wykazu. Są one jedynie pochodną zadań ustawowych SOC.

Do wykazu mogą być wpisane podmioty, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk. Muszą one posiadać zdolność do ochrony informacji niejawnych. Dodatkowym wymogiem jest również podpisanie porozumienia z ministrem właściwym do spraw informatyzacji w sprawie korzystania z systemu teleinformatycznego opisanego w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Celem tego przepisu jest możliwość nawiązania współpracy z innym podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, który mógłby przekazywać informacje o cyberzagrożeniach i dzięki temu wspierać rozwój krajowego systemu cyberbezpieczeństwa.

W celu umożliwienia wykonywania swoich zadań dane z wykazu SOC będą udostępniane CSIRT MON, CSIRT NASK, CSIRT GOV i właściwemu ze względu na sektor CSIRT sektorowemu, jak również operatorowi usługi kluczowej w dotyczącym go zakresie. Zakłada się, że będzie to stały dostęp i nie będzie konieczności składania wniosku o dostęp do danych wykazie SOC.

Dane z wykazu SOC mogą być udzielane w zakresie niezbędnym do realizacji ich ustawowych zadań: organowi właściwemu do spraw cyberbezpieczeństwa, Policji, Żandarmerii Wojskowej, Straży Granicznej, Centralnemu Biuru Antykorupcyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, sądom, prokuraturze, organom Krajowej Administracji Skarbowej, Służbie Ochrony Państwa. Udzielenie informacji będzie możliwe po złożeniu stosownego wniosku przez ww. podmioty. Umożliwia się udostępnianie danych z wykazu SOC poprzez system S46, o którym mowa w art. 46 ustawy o KSC.

2.1.3 Zmiany w przepisach dotyczących dostawców usług cyfrowych

Nie wprowadza się szczególnych zmian w rozdziale 4 dotyczącym obowiązków dostawców usług cyfrowych. Jedyne zmiany dotyczą art. 17 ust. 2 - we wprowadzeniu do wyliczenia w zdaniu drugim wyraz „*cyberbezpieczeństwo”* zamienia się na „*bezpieczeństwo systemów informacyjnych”*. Jest to związane ze zmianami definicyjnymi. Z kolei w punkcie 1, który obecnie brzmi: „*bezpieczeństwo systemów informacyjnych i obiektów”*, usuwa się wyrazy „*systemów informacyjnych i”*, ponieważ stanowiłoby to niepotrzebne powtórzenie. Przepis finalnie otrzyma brzmienie:

2. Dostawca usługi cyfrowej podejmuje właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają bezpieczeństwo systemów informacyjnych odpowiednie do istniejącego ryzyka oraz uwzględniają:

1) bezpieczeństwo obiektów.

2.1.4 Przepisy o obowiązkach przedsiębiorców komunikacji elektronicznej w krajowym systemie cyberbezpieczeństwa

Proponuje się dodanie rozdziału 4a „Obowiązki przedsiębiorców komunikacji elektronicznej", w którym będą uregulowane kwestie dotyczące obowiązku stosowania przez przedsiębiorców komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i usług komunikacji elektronicznej.

Nowy art. 20a

Współczesne społeczeństwo informacyjne jest zależne od usług dostarczanych przez przedsiębiorców komunikacji elektronicznej, bez których nie jest możliwy przepływ informacji. Z tego powodu, zarówno na poziomie europejskim jak i krajowym istotne jest, aby sieci telekomunikacyjne i usługi komunikacji elektronicznej zapewniały odpowiednio wysoki poziom bezpieczeństwa.

Obecnie przedsiębiorcy telekomunikacyjni już na podstawie dotychczas obowiązujących przepisów Działu VIIA Prawa telekomunikacyjnego są obowiązani stosować środki techniczne i organizacyjne celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Ponadto byli obowiązani poinformować Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach. Prezes UKE jednak nie posiadał kompetencji reagowania na te naruszenia. Zauważyć należy, że podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów do tej pory w ogóle nie były prawnie obowiązane stosować środki bezpieczeństwa związane z usługami komunikacji interpersonalnej. Wyjątkiem w tym zakresie były wymogi narzucone unijnymi przepisami o ochronie danych osobowych.

Proponowane przepisy z jednej strony stanowią ewolucję przepisów działu VIIA Prawa telekomunikacyjnego, a z drugiej stanowią wdrożenie EKŁE. Przedsiębiorcy telekomunikacyjni od lat są obowiązani do zapewnienia środków bezpieczeństwa świadczonych usług – więc nowe przepisy nie nakładają zupełnie nowych obowiązków. Główną zmianą w tym zakresie będzie obowiązek obsługi incydentów telekomunikacyjnych oraz obowiązek zgłaszania poważnych incydentów telekomunikacyjnych do CSIRT Telco – co jest zgodne z EKŁE. Wzmocniona zostanie rola Prezesa UKE w zakresie badania środków technicznych i organizacyjnych stosowanych przez przedsiębiorców komunikacji elektronicznej.

W tym celu w art. 20a ust. 1 nakładany jest na przedsiębiorcę komunikacji elektronicznej ogólny obowiązek brania pod uwagę w swojej działalności możliwości wystąpienia sytuacji szczególnego zagrożenia. Katalog tych sytuacji obejmuje stan nadzwyczajny, sytuację kryzysową oraz bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej. Przepis ten odzwierciedla obecny art. 176a ust. 1 – ustawy z dnia 16 lipca 2004 r.- Prawo telekomunikacyjne. Przedsiębiorcy komunikacji elektronicznej będą obowiązani do prowadzenia systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia (art. 20 ust. 2 pkt 1). Po zidentyfikowaniu ryzyk będą obowiązani wdrożyć środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych

danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka (art. 20 ust. 2 pkt 2). Przepisy te są implementacją art. 40 ust. 1 EKŁE.

W motywie 95 EKŁE prawodawca unijny zwrócił uwagę, że podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach. Sytuacja taka może również w niektórych sytuacjach dotyczyć dostawcy usług łączności interpersonalnej wykorzystującej numery. W takich sytuacjach środki techniczne i organizacyjne mające zapewnić bezpieczeństwo sieci i usług komunikacji elektronicznej powinny być łagodniejsze. Uwzględniono to w projektowanych przepisach wskazując, że środki techniczne i organizacyjne podejmowane przez przedsiębiorców komunikacji elektronicznej powinny zapewniać poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, co również uwzględnia sytuację dostawcy usług łączności interpersonalnej wykorzystującej numery. Inne środki będą stosować duzi operatorzy sieci mobilnych, dysponujący infrastrukturą telekomunikacyjną, a inne mali przedsiębiorcy jak np. osiedlowi dostawcy usługi dostępu do Internetu.

W art. 20a ust. 2 pkt 2 wskazane zostały obligatoryjne obszary środków technicznych i organizacyjnych, które wynikają z motywu 94 EKŁE. Przykładowo środki te można podzielić na[21)]:

- środki dot. zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, np.:
  - bezpieczeństwo fizyczne i środowiskowe,
  - bezpieczeństwo łańcuchów dostaw,
  - kontrola dostępu do sieci,
  - zapewnienie integralności sieci;
- środki dotyczące postępowania w sytuacji szczególnego zagrożenia:
  - procedury obsługi incydentu telekomunikacyjnego,
  - zdolności w zakresie wykrywania incydentów telekomunikacyjnych,
  - procedury raportowania incydentów telekomunikacyjnych oraz komunikacji;
- środki dotyczące odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej np.:
  - zapewnienie planów ciągłości działania usług,
  - zapewnienie zdolności do odtwarzania awaryjnego usług i sieci;
- środki w zakresie monitorowania, audytowania i testowania np.:
  - przygotowanie polityk monitorowania i logowania,
  - przeprowadzanie ćwiczeń w zakresie planów ciągłości działania,

---

[21)] Środki wskazano za: E. Vytogianni, M. Dekker, *Security Supervision under the EECC,* str. 15–16 European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc. Należy podkreślić, że nie jest to wyczerpująca lista, lecz jedynie przykładowe wskazanie.

- testowanie sieci i usług,
- przeprowadzania oceny bezpieczeństwa sieci i usług komunikacji elektronicznej.

Każdy przedsiębiorca komunikacji elektronicznej będzie dokumentował prowadzenie analizy ryzyka oraz wdrożenie środków bezpieczeństwa (art. 20a ust. 2 pkt 3). Dokumentowanie tych środków jest zgodne z powszechnie uznanymi normami technicznymi (ISO 27001), jak również pozwala na rozliczalność tych działań oraz skuteczne przeprowadzenie audytu i kontroli.

Aby uprościć prowadzenie dokumentacji, w art. 20a ust. 3 wskazano, że przedsiębiorcy komunikacji elektronicznej sporządzający plan działania w sytuacji szczególnego zagrożenia, będą dokumentować w tym planie wdrożenie środków technicznych i organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2.

Bardzo ważne jest zapewnienie przepływu informacji między zespołami CSIRT, Prezesem UKE oraz przedsiębiorcami komunikacji elektronicznej. Dlatego proponuje się, aby co do zasady przedsiębiorcy komunikacji elektronicznej byli obowiązani wyznaczyć dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane tych osób będą przekazywane do Prezesa UKE. Z obowiązku wyznaczenia ww. osób wyłącza się mikroprzedsiębiorców, małych przedsiębiorców oraz średnich przedsiębiorców – mogłoby to być zbyt duże obciążenie dla tej grupy podmiotów.

Podobnie jak w obecnie obowiązujących przepisach (art. 175d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne), proponuje się, aby minister właściwy do spraw informatyzacji mógł określić, dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej, minimalny zakres środków technicznych i organizacyjnych w stosowanych celu zapewnienia bezpieczeństwa sieci i usług komunikacji elektronicznej. Przy wydawaniu rozporządzenia minister weźmie pod uwagę

- rekomendacje międzynarodowe o charakterze specjalistycznym (będą to mogły być w szczególności normy techniczne, dokumenty ENISA, akty wykonawcze Komisji Europejskiej wydane na podstawie art. 40 ust. 5 EKŁE, czy też inne dokumenty specjalistyczne organizacji międzynarodowych);
- skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej;
- potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej.

Podkreślić należy, że przewiduje się możliwość wydawania kilku rozporządzeń na podstawie art. 20a ust. 6 – odrębnie dla każdego rodzaju działalności.

Konieczność zapewnienia ministrowi właściwemu do spraw informatyzacji takiej kompetencji wynika z faktu krytycznego znaczenia usług telekomunikacyjnych dla społeczeństwa informacyjnego. Jak wyżej wspomniano wiele usług jest zależnych od usług telekomunikacyjnych, przykładowo centra przetwarzania

danych potrzebują redundantnych łączy telekomunikacyjnych, aby mogły świadczyć swoje usługi. Dlatego konieczne jest, aby dla tego sektora minister mógł wydać minimalne wymagania co do środków bezpieczeństwa, aby zapewnić jednolity poziom bezpieczeństwa danego rodzaju usług komunikacji elektronicznej.

Nowy art. 20b

W art. 20b ust. 1 uregulowano uprawnienie Prezesa UKE do dokonywania oceny podjętych przez przedsiębiorcę komunikacji elektronicznej środków zapewniający bezpieczeństwo sieci i usług. Na jego żądanie przedsiębiorca poinformuje go o podjętych środkach. Obowiązek ten jest zgodny z art. 41 ust. 2 lit. a EKŁE.

W wyniku przeprowadzonej przez Prezesa UKE oceny mogą powstać uzasadnione wątpliwości co do stosowania przez przedsiębiorcę komunikacji elektronicznej właściwych środków technicznych i organizacyjnych. Proponuje się, żeby w takiej sytuacji Prezes UKE mógł nałożyć, w drodze decyzji, na przedsiębiorcę komunikacji elektronicznej obowiązek:

- właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych[22)], w określonym przez Prezesa UKE terminie (art. 20b ust. 4 pkt 1) co stanowi implementację art. 41 ust. 1 EKŁE lub,
- poddania się audytowi bezpieczeństwa, którego wyniki przedsiębiorca udostępnia Prezesowi UKE (art. 20b ust. 4 pkt 2), co stanowi implementację art. 41 ust. 2 lit. b EKŁE.

Uprawnienie Prezesa UKE do nałożenia, w drodze decyzji administracyjnej, obowiązku właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych służy m. in. przeciwdziałaniu ryzykom związanych z błędną konfiguracją sieci, które może prowadzić do poważnych incydentów telekomunikacyjnych, lub ryzykom związanym z niewystarczającą kontrolą dostępu. O takich ryzykach wspomina Toolbox 5G[23)]. Prezes UKE będzie mógł także, na podstawie tego artykułu nakazać uzupełnić środki organizacyjne, np. związane z bezpieczeństwem fizycznym obiektów infrastruktury telekomunikacyjnej lub dostępem osób z zewnątrz, np. serwisantów dostawcy, do kluczowej infrastruktury. Określając termin na wdrożenie dodatkowych środków Prezes UKE powinien kierować się z jednej strony koniecznością jak najszybszego ich wdrożenia, a z drugiej powinien być to obiektywnie termin realny do wykonania przez przedsiębiorcę.

Celem audytu bezpieczeństwa byłaby ocena zastosowanych przez przedsiębiorcę środków zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej. Audyt będzie musiał być

[22)] Celowo w tym przepisie użyto funktora „lub", ponieważ zależnie od konkretnej sytuacji u przedsiębiorcy komunikacji elektronicznej może zaistnieć potrzeba nakazania uzupełnienia tylko środka technicznego, tylko środka organizacyjnego albo i jednego i drugiego.

[23)] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, str. 43 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

przeprowadzony przez podmiot niezależny od przedsiębiorcy komunikacji elektronicznej, który został zobligowany do przeprowadzenia audytu. Do tego audytu będą stosowane odpowiednio art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5 ustawy o KSC. Odpowiednie stosowanie przepisów art. 15 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa (w zakresie spełniania wymogów formalnych przez podmioty przeprowadzające audyt) wynika z różnic w wymaganych wiedzy i doświadczeniu, w zależności od zakresu przedmiotowego audytu, który ma być przeprowadzony. Przy przeprowadzaniu audytów, o których mowa w art. 20b, nie zawsze wystarczające będzie spełnienie przesłanki „praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych", gdyż niezbędne mogą być wiedza i doświadczenie w zakresie funkcjonowania specyficznych rozwiązań telekomunikacyjnych.

Nowy art. 20c

W art. 20c uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej po wykryciu incydentu telekomunikacyjnego. Będzie obsługiwał każdy incydent telekomunikacyjny, który u niego wystąpi. Dla przykładu oznacza to, że dostawca usługi dostępu do Internetu będzie obowiązany zainterweniować, jeżeli np. z powodów technicznych nastąpi przerwa lub pogorszenie jakości świadczenia tej usługi. Oczywiście rodzaje podejmowanych działań w ramach obsługi incydentu telekomunikacyjnego będą się różniły w zależności od przyczyny incydentu telekomunikacyjnego czy sieci lub usług dotkniętych tym incydentem. Obowiązek ten zwiększy bezpieczeństwo świadczonych usług komunikacji elektronicznej.

Przedsiębiorca komunikacji elektronicznej zapewni dostęp do rejestrowanych incydentów zespołom CSIRT poziomu krajowego i CSIRT Telco. Jest to związane z tym, że CSIRT poziomu krajowego może zmienić klasyfikację konkretnego incydentu telekomunikacyjnego, a także z uprawnieniami zespołów CSIRT w związku z reagowaniem na incydenty telekomunikacyjne.

Równocześnie będzie mógł przekazywać do zespołów CSIRT informacje o cyberzagrożeniach, podatnościach i incydentach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci lub usług komunikacji elektronicznej także o wykorzystywanych technologiach. Uprawnienie to wzmacnia przepływ informacji między przedsiębiorcami komunikacji elektronicznej a zespołami CSIRT. W oparciu o tą wiedzę zespoły CSIRT będą mogły dokonać analizę podatności czy analizę zagrożeń co zwiększy ich możliwości reagowania na incydenty telekomunikacyjne. Wiąże się to także z zadaniem zespołów CSIRT wskazanym w art. 32 ust. 4.

Nowy art. 20d

Przepis art. 20d reguluje zasady zgłaszania incydentów telekomunikacyjnych przez przedsiębiorców komunikacji elektronicznej. Obowiązkowemu zgłoszeniu będzie podlegał poważny incydent telekomunikacyjny. Przedsiębiorca komunikacji elektronicznej będzie obowiązany uznać incydent telekomunikacyjny za poważny incydent telekomunikacyjny, jeżeli spełni on progi określone w rozporządzeniu ministra właściwego do spraw informatyzacji (art. 20d ust. 1 pkt 1). Innymi słowy obowiązek informacyjny będzie dotyczył szczególnego rodzaju incydentów telekomunikacyjnych, które w

znaczny i istotny sposób oddziałują na funkcjonowania społeczeństwa – z tego powodu państwo powinno być poinformowane o tym fakcie oraz powinno mieć odpowiednie możliwości reakcji na tego rodzaju zdarzenie.

Przedsiębiorcy telekomunikacyjni będą przekazywać do zespołu CSIRT Telco informację o wystąpieniu poważnego incydentu telekomunikacyjnego nie później niż w ciągu 8 godzin od chwili jego wystąpienia, według aktualnej wiedzy, jaką dysponują w tym czasie (art. 20d ust. 1 pkt 2 oraz 20e ust. 3). Informację tę uzupełnią w trakcie obsługi incydentu telekomunikacyjnego. Co do zasady zgłoszenie będzie przekazywane w postaci elektronicznej, a jeżeli nie będzie to możliwe – przy użyciu innych dostępnych środków komunikacji.

Podczas obsługi poważnego incydentu telekomunikacyjnego przedsiębiorcy komunikacji elektronicznej będą obowiązani współpracować z zespołami CSIRT Telco i właściwym zespołem CSIRT GOV, CSIRT MON lub CSIRT NASK. W ramach tej współpracy będą przekazywać niezbędne dane do tych zespołów, aby ułatwić reagowanie na incydent telekomunikacyjny.

Zespół CSIRT Telco przekaże niezwłocznie, w ciągu ośmiu godzin, informację o tym zgłoszeniu do właściwego dla danego przedsiębiorcy komunikacji elektronicznej zespołu CSIRT GOV, CSIRT MON lub CSIRT NASK. Rozwiązanie to zapewni jeden punkt kontaktowy dla zgłoszeń incydentów telekomunikacyjnych, z drugiej strony zapewni obieg informacji między zespołami CSIRT. Przewiduje się, że przekazywanie informacji między CSIRT będzie odbywało się poprzez system teleinformatyczny, o którym mowa w art. 46 ustawy o KSC.

Art. 20d ust. 3 przewiduje, że minister właściwy do spraw informatyzacji określi w rozporządzeniu progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny. Tworząc upoważnienie ustawowe wzięto pod uwagę parametry istotności wpływu incydentu telekomunikacyjnego wskazane w art. 40 ust. 2 EKŁE. Progi te można podzielić na:

1. ilościowe:
    a. liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ,
    b. czas trwania skutków incydentu telekomunikacyjnego,
    c. obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego;
2. jakościowe:
    a. zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług,
    b. wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej,
    c. wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
    d. wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych,
    e. wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wydając rozporządzenie minister weźmie pod uwagę rekomendacje ENISA – agencja ta wydaje rekomendacje celem wsparcia organów regulacyjnych państw UE.

Nowy art. 20e

Przepis art. 20e zawiera szczegóły dotyczące zawartości zgłoszenia poważnego incydentu telekomunikacyjnego. Pozwolą one zebrać podstawowe dane o tym incydencie takie jak dane o podmiocie dotkniętym incydentem, liczbę użytkowników, na których poważny incydent telekomunikacyjny miał wpływ oraz wpływ na usługi kluczowe, usługi cyfrowe czy obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Dane te są niezbędne, aby CSIRT Telco mógł skutecznie reagować na poważne incydenty telekomunikacyjne. Ponadto dzięki tym informacjom CSIRT poziomu krajowego zyskają informacje niezbędne do bieżącego szacowania ryzyka na poziomie krajowym.

Przede wszystkim zgłoszenie musi zawierać informacje od kogo pochodzi – od jakiego podmiotu. Potem muszą być wskazane dane osoby (imię, nazwisko, numer telefonu, adres poczty elektronicznej) zgłaszającej incydent oraz dane osoby uprawnionej do zgłaszania wyjaśnień – to mogą być dwie różne osoby albo jedna, która wypełnia dwie funkcje. Istotne jest, aby CSIRT Telco wiedział kto zgłasza incydent telekomunikacyjny i kto może udzielić wyjaśnień.

Następnie muszą być wskazane sieci i usługi komunikacji elektronicznej oraz liczba użytkowników na które poważny incydent telekomunikacyjny miał wpływ a także zasięg geograficzny obszaru, na który incydent telekomunikacyjny miał wpływ.

Projekt zakłada, że zgłoszenie poważnego incydentu telekomunikacyjnego będzie zawierało opis wpływu tego zdarzenia na świadczenie usługi kluczowej przez operatorów usług kluczowych oraz usług cyfrowych przez dostawców usług cyfrowych, jeżeli ten wpływ jest znany. Interpretować to należy w ten sposób – jeżeli przedsiębiorca komunikacji elektronicznej uzyskał informację (np. w drodze negocjacji biznesowych) od swojego usługobiorcy, że jest operatorem usługi kluczowej – to powinien wskazać w zgłoszeniu czy poważny incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej. To samo w przypadku dostawców usług cyfrowych – szczególnie tych dostawców świadczących usługi przetwarzania w chmurze – centra przetwarzania danych wymagają, do swojego codziennego funkcjonowania, niezawodnych, redundantnych łączy telekomunikacyjnych. Natomiast jeśli przedsiębiorca komunikacji elektronicznej obiektywnie nie jest w stanie wskazać, czy poważny incydent telekomunikacyjny wpłynął na operatorów usług kluczowych czy dostawców usług cyfrowych to wtedy nie musi wypełniać tej części zgłoszenia. Podobny przepis znajduje się w art. 12 ust. 1 pkt 4 lit. e ustawy o KSC.

W zgłoszeniu powinien być także opisany wpływ poważnego incydentu telekomunikacyjnego na:

- połączenia z numerami alarmowymi – o każdym przypadku niedostępności numerów ustalonych w ustawie lub w planie numeracji krajowej dla publicznych sieci telekomunikacyjnych

udostępnianych służbom ustawowo powołanym do niesienia pomocy państwo powinno wiedzieć, ponieważ numery te służą pomocy obywatelom;

- możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego – chodzi o obowiązki określone obecnie w dziale VIII. *Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego* ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne a później w art. 39 i następnych ustawy –Prawo komunikacji elektronicznej; są to m. in. zadania i obowiązki w zakresie przygotowania i utrzymywania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym. Są to kluczowe obowiązki z punktu widzenia obronności państwa, dlatego jeżeli wydarzył się poważny incydent telekomunikacyjny to państwo powinno wiedzieć w jaki sposób wpływa to na realizację tych obowiązków.

Ze względu na współzależność sieci telekomunikacyjnych incydenty telekomunikacyjne w jednym państwie mogą mieć wpływ na usługi w drugim państwie Unii Europejskiej – np. w przypadku tranzytu połączeń. Dlatego zgłoszenie poważnego incydentu telekomunikacyjnego powinno zawierać informację o transgranicznych skutkach tego zdarzenia – dzięki temu CSIRT MON, CSIRT NASK lub CSIRT GOV będą w stanie ocenić czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej.

W zgłoszeniu powinno być także wskazane jakie działania zapobiegawcze i naprawcze podjął przedsiębiorca komunikacji elektronicznej w związku z poważnym incydentem telekomunikacyjnym. Przykładowo – czy np. dokonano zabezpieczenia logów. Jest to istotne, ponieważ dzięki temu CSIRT Telco czy CSIRT poziomu krajowego będą wiedziały co zostało zrobione, a w czym należy pomóc zgłaszającemu podczas reagowania na to zdarzenie.

Oczywiście przewiduje się, że zgłoszenie może zawierać inne istotne informacje – pozostawia się to do decyzji zgłaszającego.

Ważne jest samo zgłoszenie poważnego incydentu telekomunikacyjnego, nawet jeżeli przedsiębiorca nie ma pełnej informacji o tym zdarzeniu. Jest to naturalne, dopiero po dłuższej analizie można uzyskać informacje o np. przyczynie tego zdarzenia. Dlatego wprowadza się regułę, że zgłaszający ma przekazać informacje znane mu w chwili dokonywania zgłoszenia, ale w trakcie obsługi incydentu telekomunikacyjnego musi uzupełnić te zgłoszenie.

Uprawnia się przedsiębiorcę komunikacji elektronicznej do przekazywania w niezbędnym zakresie w zgłoszeniu poważnego incydentu telekomunikacyjnego informacji mających charakter tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa, jeżeli są one konieczne do obsługi incydentu

telekomunikacyjnego. Informacje te powinny być wyraźnie oznaczone w zgłoszeniu, aby zespół CSIRT miał świadomość, że informacja ta podlega szczególnej ochronie.

Nadaje się uprawnienie dla CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco do zwrócenia się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

Nowy art. 20f

Art. 20f reguluje obowiązki informacyjne przedsiębiorcy komunikacji elektronicznej wobec użytkowników końcowych. Przepis ust. 1 nakłada obowiązki dotyczące wzmacniania świadomości użytkowników z zakresu bezpieczeństwa. Na stronie internetowej przedsiębiorcy komunikacji elektronicznej będą więc publikowane podstawowe informacje o:

- potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej;
- rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
- przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Dzięki temu użytkownicy będą mieli dostęp do wiedzy, która umożliwi im bezpieczne korzystanie z usług komunikacji elektronicznej.

Kolejne ustępy dotyczą już sytuacji, w której doszło do wystąpienia szczególnego i znacznego[24] zagrożenia wystąpienia incydentu telekomunikacyjnego. W takiej sytuacji przedsiębiorca komunikacji elektronicznej będzie miał obowiązek informować użytkowników, na których takie zagrożenie może mieć wpływ, o możliwych środkach, które użytkownicy ci mogą podjąć oraz związanych z tym kosztach. Przedsiębiorca poinformuje tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. Obowiązek ten spowoduje, że uprzedzeni wcześniej użytkownicy będą w stanie zabezpieczyć się przed zagrożeniem.

Podkreślić przy tym należy, że nie jest intencją projektodawcy nakładanie obowiązku informowania użytkowników o każdym zagrożeniu wystąpienia incydentu telekomunikacyjnego. Takie podejście spowodowałoby znaczne obciążenie działów bezpieczeństwa przedsiębiorców. Ponadto, po pewnym czasie

---

[24)] Jako szczególne zagrożenie należy uznać takie, które nie jest typowym lub generalnie występującym zagrożeniem. Jako znaczne zagrożenie należy uznać takie, które stwarza ryzyka dla użytkownika. Por. European Union Agency for Cybersecurity, *Cyber threats outreach in telecom: guidelines for national authorities and telecom providers on outreach to users about cyber threats.*, 2022, s. 21. https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.

wysyłania częstych wiadomości o drobnych zagrożeniach użytkownicy mogliby zacząć je ignorować, co byłoby niepożądane. Tak jak wyżej wspomniano – obowiązki te będą się pojawiały w sytuacji szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego. Pomocą dla przedsiębiorcy komunikacji elektronicznej przy dostosowaniu się do tych wymogów będą publikacje ENISA[25)].

Ponadto, przedsiębiorca komunikacji elektronicznej będzie zobowiązany poinformować o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny, co stanowi implementację art. 40 ust. 3 zdanie drugie EKŁE.

Nowy art. 20g

W art. 20g uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej do blokowania komunikatu oraz ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej. Takie działanie możliwe jest w przypadku stwierdzenia zagrożenia dla bezpieczeństwa sieci i usług oraz tylko w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny zagrożenia. W ten sposób utrzymuje się dotychczasowe obowiązki z art. 175c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Dotychczasowy art. 175c ust. 4 stanowił, że przedsiębiorca telekomunikacyjny nie odpowiada za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych w zakresie wynikającym z art. 175c ust. 1. Zdecydowano się zrezygnować z tego rodzaju wyłączenia odpowiedzialności z mocy ustawy. Blokowanie komunikatu elektronicznego tudzież przerwanie świadczenia usługi komunikacji elektronicznej powinno być środkiem ostatecznym mającym zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorca komunikacji elektronicznej, aby zwolnić się z odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi powinien móc wykazać, że zastosowanie środków z art. 20g było niezbędne, konieczne oraz nie było innych środków umożliwiających w danej sytuacji zareagowanie na zagrożenie.

Nowy art. 20h

W art. 20h uregulowano obowiązki informacyjne Prezesa UKE. Prezes UKE m. in. przekazuje informację o wystąpieniu incydentu telekomunikacyjnego do organów regulacyjnych innych państw członkowskich oraz sprawozdania roczne, zawierające informacje o incydentach telekomunikacyjnych, zgodnie z art. 40 ust. 2 ostatnie zdanie EKŁE. Przepis ten wypełnia więc obowiązki informacyjne Polski wobec Unii Europejskiej, której jednym z celów jest zapewnienie wysokiego poziomu odporności sieci i usług komunikacji elektronicznej na swoim terytorium. Bez tych danych nie jest możliwe prowadzenie ewaluacji dotychczasowej polityki w tym obszarze.

Ponadto, zgodnie z art. 40 ust. 2 zdanie trzecie EKŁE umożliwiono Prezesowi UKE publikowanie informacji w Biuletynie Informacji Publicznej o wystąpieniu poważnego incydentu telekomunikacyjnego,

[25)] https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom.

jeżeli jest to uzasadnione interesem publicznym. Przedsiębiorca komunikacji elektronicznej będzie musiał opublikować tą informację na swojej stronie internetowej po poinformowaniu przez Prezesa UKE.

Prezes UKE będzie mógł nałożyć, w drodze decyzji, na przedsiębiorcę komunikacji elektronicznej obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób jej publikacji, jeżeli sposoby opublikowania informacji na Biuletynie Informacji Publicznej UKE czy na stronie przedsiębiorcy komunikacji elektronicznej w niewystarczającym stopniu służą ochronie interesu publicznego.

Celem tych przepisów jest zapewnienie możliwości poinformowania społeczeństwa np. o przyczynach nagłej niedostępności usług komunikacji elektronicznej, która dotknęłaby duże miasto czy nawet większy obszar. Brak informacji o przyczynach takich zdarzeń mógłby doprowadzić do paniki czy do niezadowolenia społecznego, co byłoby niepożądane.

2.1.5 Zmiany w przepisach dotyczących podmiotów publicznych

Zmiany w art. 21

Zmiana w art. 21 polega na wprowadzeniu obowiązku wyznaczenia przez podmioty publiczne nie jednej, a dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Pozwoli to na zapewnienie sprawnej komunikacji między zespołami CSIRT poziomu krajowego a podmiotami publicznymi podczas trwania incydentu w podmiocie publicznym, a także na co dzień, bowiem zespoły CSIRT przesyłają często ostrzeżenia o cyberzagrożeniach.

Zmiany w art. 22

W art. 22 dodane zostały ust. 1a oraz 3–7, które regulują zgłaszanie incydentów w podmiocie publicznym przez Agencję Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym . Wskazane podmioty będą zgłaszały incydenty oraz przekazywały dane osób do kontaktu do nowo utworzonego CSIRT INT. Specyfika tych jednostek, zwłaszcza ich działanie poza granicami RP, sprawia, że konieczne jest zapewnienie im dodatkowego wsparcia. To wsparcie zostanie zapewnione przez CSIRT INT prowadzony przez Agencję Wywiadu. Będzie on wspierał te jednostki w obsłudze incydentów oraz przekazywał informacje o ich sytuacji do CSIRT GOV. W związku z tym został on również wyposażony w uprawnienia do przetwarzania odpowiednich danych. Tak ukształtowane rozwiązanie zwiększy cyberbezpieczeństwo szczególnie wrażliwych podmiotów publicznych.

2.1.6 ISAC i wykaz ISAC

Po rozdziale 5 zostanie dodany rozdział 5a dotyczący ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Do tej pory nic nie stało na przeszkodzie, aby były tworzone podmioty na wzór

ISAC, na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji, partnerstw publiczno-prywatnych lub luźnych jednostek organizacyjnych. Nowelizacja tego nie zmienia, daje jedynie możliwość funkcjonowania ISAC w ramach krajowego systemu cyberbezpieczeństwa.

Przepis umożliwia zawarcie porozumienia między ISAC a ministrem właściwym do spraw informatyzacji o korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 uKSC. System ten pozwala na wymianę informację o podatnościach, incydentach i cyberzagrożeniach między podmiotami krajowego systemu cyberbezpieczeństwa. Korzyścią dla ISAC z podpisania porozumienia byłoby uzyskanie informacji z systemu S46, które będzie mógł wykorzystać w swojej działalności. Z drugiej strony będzie obowiązany również do współpracy z zespołami CSIRT poziomu krajowego i wymiany informacji.

Podpisanie porozumienia z ministrem należy traktować jako akt wpisania się ISAC do krajowego systemu cyberbezpieczeństwa. Uprawnienie do jego podpisania ma charakter całkowicie fakultatywny – zarówno po stronie ISAC jak i ministra. Należy tutaj zauważyć, że minister właściwy do spraw informatyzacji jest odpowiedzialny za utrzymanie systemu S46 – w tym również za jego bezpieczeństwo i ten fakt powinien minister wziąć pod uwagę decydując się na podpisanie porozumienia z ISAC.

ISAC często nie mają osobowości prawnej. Zazwyczaj mają charakter porozumienia. Dlatego wprowadzono obowiązek, aby podmioty tworzące ISAC wyznaczyły przedstawiciela w celu zawarcia porozumienia z ministrem, oraz do informowania ministra o zmianach dot. ISAC czy też jego rozwiązania (ust. 3).

W celu promocji formuły ISAC prowadzony będzie wykaz ISAC przez ministra właściwego do spraw informatyzacji. W wykazie będą publikowane dane o ISAC, które podpisały porozumienie z ministrem (ust. 4). Wykaz będzie zawierał podstawowe informacje o ISAC, nazwę, siedzibę, numer w rejestrze, dane o osobie reprezentującej ISAC[26], dane kontaktowe (ust. 5).

Wprowadza się rozwiązania mające na celu zapewnienie aktualności wykazu:

- wpis do wykazu nastąpi niezwłocznie, najpóźniej w ciągu 7 dni od zawarcia porozumienia (ust. 6),
- ISAC będzie wykreślany z wykazu ISAC w przypadku rozwiązania porozumienia albo rozwiązania ISAC (ust. 7),

[26)] Dane o osobie reprezentującej ISAC wpisanego do wykazu są niezbędne dla ministra właściwego do spraw informatyzacji celem skontaktowania się np. przy okazji kontroli ISAC.

- zmiana danych w wykazie ISAC będzie następowała na wniosek[27)] jednego z podmiotów tworzących ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu (ust. 8).

Czynnością konstytutywną jest podpisanie porozumienia między ISAC a ministrem. Rozwiązanie porozumienia oraz rozwiązanie ISAC będzie powodowało zaprzestanie korzystania z systemu S46 przez ISAC. Stąd też wykaz ISAC odzwierciedla tylko stan faktyczny, wpis oraz wykreślenie z wykazu nie kreuje praw i obowiązków. Dlatego wprowadzono przepis zgodnie z którym wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno–technicznymi (ust. 10).

Wykaz będzie publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, z wyjątkiem danych osobowych osoby reprezentującej ISAC. Takie rozwiązanie zapewni dostęp do wykazu dla obywateli (ust. 11).

W przepisie ust. 12 wprowadza się obowiązek współpracy ISAC wpisanego do wykazu ISAC z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów. Istotą tego obowiązku jest to, aby nastąpiła swego rodzaju ekwiwalentność – w zamian za dostęp do systemu S46 i informacji w nim zgromadzonych ISAC będzie dzielił się wynikami swojej działalności i w ten sposób wspierał zespoły CSIRT.

Minister będzie mógł przeprowadzić kontrolę działalności ISAC (ust. 13). Wzorcem kontroli będą:

- przepisy prawa – przepisy ustawy o krajowym systemie cyberbezpieczeństwa oraz inne przepisy dotyczące funkcjonowania ISAC czy też dotyczące bezpieczeństwa informacji,
- zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa określone w porozumieniu z ministrem.

Jeżeli ISAC nie będzie realizował swoich obowiązków lub naruszał zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa to minister właściwy ds. informatyzacji będzie mógł zwrócić się do ISAC o usunięcie nieprawidłowości w określonym terminie lub wykreślić taki podmiot z wykazu ISAC (ust. 15). Celowo tutaj użyto funktora „lub” – celem jest umożliwienie ministrowi dokonanie samego wystąpienia czy też od razu wypowiedzenia porozumienia. Możliwa jest również sytuacja, w której minister najpierw występuje o usunięcie nieprawidłowości, a następnie widząc, że ISAC ich nie usunął – wypowiedzieć porozumienie.

[27)] Przewiduje się obowiązkową elektronizację tych wniosków.

2.1.7 Nowe obowiązki zespołów CSIRT GOV, CSIRT MON i CSIRT NASK

Zmiany w art. 26

Zgodnie z nową treścią art. 26 ust. 2 zespoły CSIRT GOV, CSIRT MON i CSIRT NASK będą mogły udzielić wsparcia w obsłudze incydentów i incydentów telekomunikacyjnych wszystkim podmiotom krajowego systemu cyberbezpieczeństwa oraz operatorom infrastruktury krytycznej.

Ponadto w nowym ust. 2a wprowadza się również nowe uprawnienie Pełnomocnika. Będzie mógł zlecić zapewnienie ww. wsparcia:

- CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji;
- CSIRT GOV – za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego;
- CSIRT MON – za zgodą Ministra Obrony Narodowej.

Obydwie zgody będą mogły być wyrażone z wykorzystaniem środków porozumiewania się na odległość. Powyższe rozwiązanie umożliwi udzielenie najlepszego możliwego wsparcia określonemu podmiotowi w przypadku wystąpienia incydentu, który będzie wymagał szczególnych kompetencji do jego obsługi. Dzięki temu Pełnomocnik będzie dysponował skutecznym narzędziem do reagowania na incydenty.

W art. 26 ust. 3 dodane zostały nowe zadania zespołów CSIRT poziomu krajowego.

Będą to:

- gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych
- przygotowywanie
    - na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych,
    - na zlecenie Pełnomocnika analiz skutków incydentów i incydentów telekomunikacyjnych oraz przebiegu obsługi incydentów i incydentów telekomunikacyjnych,
    - rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa.

Zadania te pozwolą zespołom CSIRT na gromadzenie informacji niezbędnych dla ich codziennego funkcjonowania. Zespoły CSIRT staną się również zapleczem analitycznym dla Pełnomocnika oraz przewodniczącego Kolegium, dzięki czemu uzyskają oni pełny obraz cyberbezpieczeństwa na poziomie krajowym. Zespoły CSIRT posiadają unikalną wiedzę na temat tego jak faktycznie funkcjonuje krajowy system cyberbezpieczeństwa – dlatego też powinny otrzymać kompetencję do przygotowywania rekomendacji w zakresie usprawniania tego systemu.

W związku z dodaniem przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa zachodzi konieczność uzupełnienia zadań CSIRT poziomu krajowego w tym zakresie. Dlatego zespoły te będą zajmować się monitorowaniem incydentów telekomunikacyjnych na poziomie krajowym, szacowaniem ryzyka związanego z zaistniałymi incydentami telekomunikacyjnymi,

przekazywaniem informacji dotyczących incydentów telekomunikacyjnym podmiotom krajowego systemu cyberbezpieczeństwa, reagowaniem na incydenty telekomunikacyjne, klasyfikowaniem incydentów telekomunikacyjnych jako incydenty krytyczne.

Zespoły CSIRT poziomu krajowego będą również uprawnione do prowadzenia działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa poprzez

- wykonywanie oceny bezpieczeństwa – szczegółowe przepisy dot. tej kompetencji zawiera nowy rozdział 6b Ocena bezpieczeństwa,
- identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych[28].

W cyberbezpieczeństwie bardzo istotny jest ciągły rozwój kadry z uwagi na zmieniające się zagrożenia. Dlatego do zadań CSIRT poziomu krajowego dodaje się również udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRT GOV, CSIRT MON lub CSIRT NASK, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.

Wprowadzono nowe brzmienie art. 26 ust. 4. Celem tych zmian jest, aby CSIRT GOV, CSIRT MON oraz CSIRT NASK wspólnie z CSIRT sektorowymi, CSIRT INT czy CSIRT Telco porozumiały się i opracowały procedury koordynacji obsługi incydentów i incydentów telekomunikacyjnych, przy których potrzebne są działania wielu zespołów CSIRT. Przykładowo może się zdarzyć sytuacja, że incydent poważny jest także incydentem istotnym jak również poważnym incydentem telekomunikacyjnym – sytuacja ta będzie angażowała właściwy CSIRT sektorowy, CSIRT Telco oraz jeden z CSIRT poziomu krajowego. Dlatego CSIRT powinny mieć opracowaną wspólną procedurę obsługi takich przypadków.

W związku z dodaniem nowych podmiotów w skład krajowego systemu cyberbezpieczeństwa należało ustalić, który z zespołów CSIRT poziomu krajowego będzie przyjmował od nich zgłoszenia incydentów. Proponuje się, że CSIRT GOV będzie właściwy dla przyjmowania incydentów zgłaszanych przez:

- Państwowe Gospodarstwo Wodne Wody Polskie,
- instytucje rozwoju,
- Urzędu Komisji Nadzoru Finansowego.

Natomiast CSIRT NASK będzie przyjmował zgłoszenia incydentów zgłaszanych przez

[28] Chodzi o umożliwienie takich działań jak np. ARTEMIS - https://www.nask.pl/pl/aktualnosci/5137,Artemis-CERT-Polska-bada-bezpieczenstwo-polskiego-internetu.html.

- Centrum Łukasiewicz,
- instytutów działających w ramach Centrum Łukasiewicz,
- instytutów badawczych,
- międzynarodowych instytutów badawczych,
- Polskiej Akademii Nauk,
- Polskiej Akademii Umiejętności,
- samodzielnych publicznych zakładów opieki zdrowotnej,
- uczelni.

Do CSIRT MON będą zgłaszali incydenty telekomunikacyjne ci przedsiębiorcy komunikacji elektronicznej, którzy są:

- podmiotami podległymi Ministrowi Obrony Narodowej lub przez niego nadzorowanymi,
- przedsiębiorcami realizującymi zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny.

Natomiast do CSIRT GOV będą zgłaszali incydenty telekomunikacyjne przedsiębiorcy komunikacji elektronicznej, którzy są wymienieni w art. 26 ust. 7.

Dla pozostałych przedsiębiorców komunikacji elektronicznej właściwym CSIRT będzie CSIRT NASK.

W związku z pismem Komisji Europejskiej Ref. Ares(2019)2130481 z dnia 26 marca 2019 r. w zakresie zmiany terminu przekazania przez państwa członkowskie sprawozdania rocznego dotyczącego informacji o zgłoszonych przez operatorów usług kluczowych incydentach poważnych i zgłoszonych przez dostawców usług cyfrowych incydentach istotnych, informacje o zgłoszonych incydentach od roku 2020, dane za rok poprzedni muszą być przekazywane do dnia 15 lutego każdego roku. Dlatego też zmieniono termin przekazania tych danych przez zespoły CSIRT poziomu krajowego do Pojedynczego Punktu Kontaktowego z 30 maja na 31 stycznia (zmiana w art. 26 ust. 3 pkt 12).

W art. 26 dodano ust. 9a, wedle którego rozbudowa i modernizacja infrastruktury teleinformatycznej CSIRT NASK służącej realizacji jego zadań może być dofinansowana w formie dotacji celowej ze środków budżetu państwa, z części której dysponentem jest minister właściwy do spraw informatyzacji.

W ust. 11 poprawia się błąd zawarty w ustawie – zamienia się wyrazy „Ministra Cyfryzacji” na wyrazy „ministra właściwego do spraw informatyzacji” co zapewni zgodność z ustawą z dnia 4 września 1997 r. o działach administracji rządowej[29)].

W art. 26 dodaje się ust. 12, zgodnie z którym Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy ds. informatyzacji poinformują Pełnomocnika o zawarciu przez CSIRT poziomu krajowego porozumienia w sprawie powierzenia sobie wzajemnie wykonywania zadań w stosunku do niektórych rodzajów podmiotów krajowego systemu cyberbezpieczeństwa. Pełnomocnik opublikuje komunikat o zawarciu porozumienia na stronie podmiotowej w Biuletynie Informacji Publicznej.

Zmiany w art. 31

Zgodnie z nowym ust. 1a CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgodnią sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej przez przedsiębiorców komunikacji elektronicznej. Ponadto dodaje się obowiązek publikacji przez Pełnomocnika komunikatu o sposobie dokonywania zgłoszeń incydentów do CSIRT poziomu krajowego.

Zmiany w art. 32

Zmiana w art. 32 ust. 4 ma charakter redakcyjny. Dodaje się CSIRT sektorowy oraz CSIRT Telco a także zastępuje się wyrazy „operatora usługi kluczowej, dostawcy usługi cyfrowej lub podmiotu publicznego, o którym mowa w art. 4 pkt 7–15” pojęciem podmiotów krajowego systemu cyberbezpieczeństwa.

Zmiany w art. 33

W art. 33 dodaje się w ust. 1a obowiązek przeprowadzenia przez CSIRT poziomu krajowego badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT. Podkreślić należy, że zespoły CSIRT miały uprawnienie do przeprowadzenia takiego badania od początku obowiązywania ustawy o KSC.

W art. 33 w ust. 1b–1e dodaje się również przepisy precyzujące uprawnienia CSIRT poziomu krajowego przy przeprowadzaniu badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, których wykorzystanie może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

Zmiany te uprawniają zespół CSIRT poziomu krajowego, prowadzący badanie, do podejmowania technik mających na celu: obserwację i analizę pracy, uzyskanie dostępu do przetwarzanych danych,

[29)] Dz. U. 2022 r. poz. 2512.

odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez urządzenie informatyczne lub oprogramowanie.

Takie szczególne uprawnienia są konieczne, aby zespoły CSIRT poziomu krajowego mogły skutecznie przebadać urządzenia i oprogramowanie pod kątem zagrożeń bezpieczeństwa narodowego.

Ponadto CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie będą związane postanowieniami umów licencyjnych badanych urządzeń i oprogramowania, które ograniczają możliwość przeprowadzenia badania.

Wskazane wyżej uprawnienia zespołu prowadzącego badanie są konieczne do zapewnienia ochrony bezpieczeństwa państwa. Niektóre postanowienia umów licencyjnych mogłyby uniemożliwić realizację tego zadania. Zespół CSIRT prowadzący badanie nie powinien być ograniczony licencją twórcy złośliwego oprogramowania, którego wykorzystanie zagraża bezpieczeństwu państwa w tym np. bezpieczeństwu infrastruktury krytycznej. W zakresie badania sprzętu lub oprogramowania należy zwrócić uwagę, że standardowe umowy licencyjne nie przewidują możliwości dokonywania badania sprzętu pod kątem jego bezpieczeństwa ani też testowania konkretnych rozwiązań zastosowanych w danym produkcie. Konieczność uzyskania zgody właściciela licencji na takie działania często jest niemożliwa do uzyskania w drodze umowy zawieranej na ogólnych zasadach. Producenci nie mają bowiem interesu w umożliwianiu podmiotom zewnętrznym takich działań. Równocześnie rosnąca liczba cyberzagrożeń oraz zależność kluczowych usług od systemów teleinformatycznych sprawia, że konieczne jest by administracja publiczna dysponowała narzędziem, które pozwoli jej przeprowadzić takie badanie. Brak tych przepisów mógłby prowadzić do powstania sytuacji, w której CSIRT poziomu krajowego musiałby uzyskać zgodę dostawcy potencjalnie niebezpiecznego sprzętu na przeprowadzenie jego badania, nawet w wypadku gdyby powstało uzasadnione podejrzenie, że dany produkt może być wykorzystany do wywołania incydentu. W związku z powyższym przepis ten jest niezbędny dla zapewnienia bezpieczeństwa podmiotom krajowego systemu cyberbezpieczeństwa.

W obecnym art. 33 uKSC nie zostało wskazane w jaki sposób powinny być publikowane rekomendacje Pełnomocnika dotyczące stosowania urządzeń informatycznych lub oprogramowania. Dlatego proponuje się, aby były one publikowane w Biuletynie Informacji Publicznej (BIP) na stronie podmiotowej Pełnomocnika (nowy ust. 4c). W ślad za tą zmianą proponuje się zmianę w ust. 5 – termin 7 dni na złożenie przez podmiot krajowego systemu cyberbezpieczeństwa zastrzeżenia do rekomendacji będzie liczony od momentu opublikowania rekomendacji w BIP, a nie od momentu otrzymania przez podmiot tych rekomendacji.

Zmiany w art. 34

Art. 34 ust. 1 dostosowano do zmian instytucjonalnych – dodano w nim obowiązek współpracy CSIRT INT, CSIRT sektorowego, CSIRT Telco oraz SOC zewnętrznych z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań

Nowy art. 34a

Art. 34a zapewnia wymianę informacji o incydentach telekomunikacyjnych pomiędzy zespołami CSIRT poziomu krajowego, CSIRT Telco z Prezesem UKE. Przepis ten umożliwia realizację obowiązku informowania organów regulacyjnych w innych państwach członkowskich UE w związku z wystąpieniem incydentu telekomunikacyjnego, jeśli Prezes UKE uzna charakter tego incydentu za istotny. Ponadto Prezes UKE otrzyma informacje umożliwiające przygotowanie sprawozdań do Komisji Europejskiej i ENISA o poważnych incydentach telekomunikacyjnych. Z kolei zespoły CSIRT poziomu krajowego muszą uzgodnić z Prezesem UKE sposób i tryb przekazywania informacji o incydentach telekomunikacyjnych. Przepis ten jest implementacją art. 40 ust. 2 EKŁE.

Nowy art. 34b

Zgodnie z nowym art. 34b na CSIRT MON, CSIRT NASK i CSIRT GOV zostanie nałożony obowiązek współpracy z Prezesem UKE oraz z CSIRT Telco przy wykonywaniu ustawowych zadań.

Zmiany w art. 35

Zmiana w art. 35 ust. 5 polega na tym, że CSIRT GOV, CSIRT MON i CSIRT NASK będą mogły przekazywać informacje o podatnościach, incydentach krytycznych i cyberzagrożeniach do publikacji w Biuletynie Informacji Publicznej Pełnomocnika. Do tej pory informacje takie mogły być publikowane w Biuletynie Informacji Publicznej na stronie podmiotowej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego. Nie zmieniają się za to przesłanki w których taka publikacja jest możliwa. Publikacja takich informacji powinna przyczynić się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów oraz nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych. Podobny charakter (dot. incydentów poważnych i istotnych) mają zmiany w art. 37 ustawy o KSC.

Zmiany w art. 36

W art. 36 ust. 2 rozszerza się skład Zespołu do spraw Incydentów Krytycznych (dalej: „Zespół”). W skład Zespołu wejdą także przedstawiciele Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Związane jest to z nowymi zadaniami: Pełnomocnika – wydawanie ostrzeżeń, oraz ministra właściwego do spraw informatyzacji. Ponadto umożliwia się Pełnomocnikowi uczestnictwo w posiedzeniach Zespołu.

Nowy art. 36a

Zmiana w art. 36a umożliwia Prezesowi Rady Ministrów zobowiązanie, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego (RZZK), Ministra Obrony Narodowej do udzielenia wsparcia zespołowi CSIRT poziomu krajowego koordynującemu obsługę incydentu krytycznego, przez jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Obecne przepisy przewidują, że Dyrektor Rządowego Centrum Bezpieczeństwa, działając na podstawie decyzji Zespołu, może zwrócić się do Prezesa Rady Ministrów o zwołanie RZZK. Może się tak wydarzyć, jeżeli incydent krytyczny jest sytuacją kryzysową, wymagającą działania na poziomie rządowym. Proponowany artykuł wpisuje się w ten model działania, umożliwiając udzielenie wsparcia zespołowi CSIRT przez wyspecjalizowane w zakresie cyberbezpieczeństwa jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Decydującą rolę będzie miał tutaj Prezes Rady Ministrów, działający w oparciu o opinię RZZK. Podkreślić należy, że dotychczasowa praktyka wskazuje, że zarówno Zespół do spraw Incydentów Krytycznych jak i RZZK są ciałami, które w sytuacjach nagłych są w stanie zebrać się szybko. Zaproponowane rozwiązanie jest zatem adekwatne.

2.1.8 Zadania CSIRT INT

Nowy art. 36b

W nowym art. 36b wprowadzony został CSIRT INT, który będzie wspierał placówki dyplomatyczne i konsularne. Przepis ten reguluje zadania jakie zostały wskazane dla nowego CSIRT'u. Przede wszystkim będzie on wspierał ww. podmioty w reagowaniu na incydenty. Zadania te są analogiczne do zadań CSIRT'ów sektorowych. Wprowadzenie tego nowego CSIRT-u zwiększy cyberbezpieczeństwo podmiotów publicznych, które ze względu na swoje szczególne położenie są szczególnie narażone na ataki. Nowy Zespół reagowania na incydenty komputerowe, prowadzony przez Agencję Wywiadu, będzie dysponował najlepszymi dostępnymi środkami do udzielania wsparcia podmiotom położonym poza granicami kraju. CSIRT INT będzie również blisko współpracował w tym zakresie z CSIRT GOV. Art. 36b reguluje podstawowe zadania jakie zostały postawione przed CSIRT INT. Będzie on pełnił rolę analogiczną do roli CSIRT sektorowych dla podmiotów podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych. Najważniejszym zadaniem będzie przekazywanie zgłoszeń o incydentach do CSIRT GOV. Ponadto CSIRT INT będzie wspierał te podmioty przy obsłudze incydentów oraz przekazywał im informacje o najlepszych praktykach w dziedzinie cyberbezpieczeństwa. Będzie on również mógł prowadzić testy bezpieczeństwa.

Nowy art. 36c

Art. 36c reguluje szczegółowo kwestię przesyłania zgłoszeń podmiotów publicznych przez CSIRT INT do CSIRT GOV. Zgłoszenia te muszą być przesłane do CSIRT GOV w ciągu 8 godzin od ich otrzymania. Jest to niezbędne ze względu na koordynacyjną rolę CSIRT GOV. By sprawnie koordynować obsługę incydentów u wszystkich podlegających mu podmiotów musi mieć aktualne dane o ich sytuacji. To rozwiązanie jest

kluczowe dla zapewnienia prawidłowego przepływu informacji między podmiotami krajowego systemu cyberbezpieczeństwa, uwzględniając jednocześnie, aby obowiązek nałożony na ww. rodzaj podmiotów publicznych odbywał się jednotorowo.

2.1.9 Ocena bezpieczeństwa

Nowy art. 36d

Wprowadzono nowy rozdział 6b, który dotyczy możliwości przeprowadzania przez CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT sektorowe, CSIRT INT lub CSIRT Telco oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Przepisy tego rozdziału były wzorowane na art. 32a ustawy z dnia 24 maja 2002 r. o *Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[30)], zwana dalej „ustawa o ABW i AW". Wprowadzono jednak kilka istotnych zmian w stosunku do pierwowzoru. Przede wszystkim wyłącza się stosowanie tego przepisu do ocen bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy o ABW i AW. Bez tego wyłączenia powstałyby dwie podstawy prawne do przeprowadzania ocen bezpieczeństwa wobec podmiotów krajowego systemu cyberbezpieczeństwa, które są jednocześnie operatorami infrastruktury krytycznej. Nie jest to sytuacja pożądana.

Ponadto wyłącza się stosowanie rozdziału 6b do systemów teleinformatycznych akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych. Są to systemy służące przetwarzaniu informacji niejawnych i tutaj pierwszeństwo powinny mieć przepisy ustawy o ochronie informacji niejawnych.

Wprowadzono jasne określenie właściwości CSIRT poziomu krajowego do przeprowadzania ocen bezpieczeństwa – nawiązuje ono do ogólnej właściwości zespołów CSIRT określonej w art. 26 ust. 5–7. CSIRT sektorowe będą mogły przeprowadzać ocenę bezpieczeństwa wobec operatorów usług kluczowych w danym sektorze. CSIRT INT będzie mógł przeprowadzić ocenę bezpieczeństwa wobec jednostek podległych lub nadzorowanych przez Ministra Spraw Zagranicznych. CSIRT Telco będzie mógł przeprowadzić ocenę bezpieczeństwa wobec przedsiębiorców komunikacji elektronicznej.

Wprowadza się również regułę, że przeprowadzanie oceny bezpieczeństwa powinno być uzgodnione z właściwym CSIRT poziomu krajowego. Jest to po to, aby w tym samym czasie nie były prowadzone oceny bezpieczeństwa przez kilka zespołów. Jednocześnie wprowadza się obowiązek poinformowania odpowiednio

---

[30)] Dz. U. 2023 r. poz. 1136.

Syntetyczne podsumowanie ocen bezpieczeństwa wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego znajduje się w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* str. 43–52 https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html.

organu właściwego do spraw cyberbezpieczeństwa czy Prezesa UKE o zamiarze wykonania oceny bezpieczeństwa.

Nowy art. 36e

Ocena bezpieczeństwa będzie mogła być przeprowadzona wyłącznie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w postaci pisemnej lub elektronicznej pod rygorem nieważności. Jest to duża różnica względem art. 32a ustawy o ABW i AW, gdzie to Szef ABW decyduje o włączeniu systemu teleinformatycznego operatora infrastruktury krytycznej do rocznego planu przeprowadzania ocen bezpieczeństwa.

Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny. Jednakże prowadzenie tej oceny nie może zaszkodzić systemowi informacyjnemu, a szerzej podmiotowi, który korzysta z tego systemu i świadczy usługi dla swoich klientów. Dlatego wprowadza się zasadę, zgodnie z którą czynności przeprowadzane w ramach oceny bezpieczeństwa powinny w jak najmniejszym stopniu zakłócać funkcjonowanie tego systemu lub ograniczać jego dostępność (art. 36e ust. 2). Tym bardziej nie jest dopuszczalne, aby działania te doprowadziły do nieodwracalnego zniszczenia danych w systemie poddanym ocenie. Przepis ten stanowi więc ogólną dyrektywę dla osób przeprowadzających ocenę bezpieczeństwa i stanowi gwarancję dla podmiotu krajowego systemu cyberbezpieczeństwa wobec którego prowadzona jest ocena bezpieczeństwa.

Po uzyskaniu zgody od podmiotu krajowego systemu cyberbezpieczeństwa, CSIRT przeprowadzający ocenę bezpieczeństwa będzie obowiązany uzgodnić tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa (art. 36e ust. 3).

Zespół CSIRT przeprowadzający ocenę bezpieczeństwa otrzyma dwa ważne uprawnienia, które są niezbędne do skutecznego przeprowadzenia takiej oceny (art. 36e ust. 4 i 5).

Po pierwsze będzie uprawniony do wytworzenia lub pozyskania urządzeń lub oprogramowania przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4[31)], art. 267 § 3[32)], art. 268a[33)] §

[31)] Przestępstwo polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach w ramach którego sprawca zakłóca, uniemożliwia lub w inny sposób wpływaj na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

[32)] Przestępstwo w którym sprawca w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

[33)] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

1 albo § 2 w związku z § 1, art. 269 § 1[34)] lub 2 albo art. 269a[35)] Kodeksu karnego aby móc sprawdzić, czy oceniany system jest podatny na tego rodzaju oprogramowanie.

Po drugie używając ww. urządzeń lub programów zespół CSIRT będzie uprawniony do dostępu do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Będzie mógł uzyskać dostęp do całości lub części ocenianego systemu. Wprowadza się przy tym kontratyp zgodnie z którym osoba wykonująca te czynności nie popełnia przestępstwa, o którym mowa w art. 267 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

Bez tego rodzaju szczególnych uprawnień zespół CSIRT nie będzie w stanie zidentyfikować podatności, które mogą być wykorzystane przez przestępców komputerowych do zaatakowania podmiotu krajowego systemu cyberbezpieczeństwa.

Aby zapewnić gwarancje dla podmiotu, u którego jest przeprowadzana ocena wprowadza się przepis na mocy którego informacje uzyskane w wyniku oceny stanowią tajemnicę prawnie chronioną (art. 36e ust. 6). Zespół CSIRT nie będzie mógł wykorzystać ich do realizacji innych zadań ustawowych. Informacje te będą podlegały niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Końcowym etapem oceny bezpieczeństwa będzie sporządzenie przez CSIRT raportu, który będzie zawierał podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego (art. 36e ust. 7). Raport będzie przekazany do podmiotu, którego system był poddany ocenie bezpieczeństwa. Dzięki temu podmiot będzie mógł przeanalizować np. jak jego personel, odpowiedzialny za bezpieczeństwo systemu, zachowywał się podczas oceny bezpieczeństwa; czy procedury bezpieczeństwa zadziałały prawidłowo, a także czy i jakie podatności zostały wykryte podczas oceny bezpieczeństwa.

Nowy art. 36f

W wyniku prowadzonej przez zespół CSIRT oceny bezpieczeństwa może zostać zidentyfikowana podatność, która może występować w innych systemach informacyjnych, które np. wykorzystują to samo oprogramowanie zawierające podatność. W takiej sytuacji zasadne jest, aby zespół CSIRT był obowiązany poinformować o tym:

[34)] Przestępstwo w którym sprawca niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych.

[35)] Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej.

- ministra właściwego do spraw informatyzacji – z uwagi na to, że minister jest właściwy w sprawach systemów i sieci teleinformatycznych administracji publicznej[36)]
- Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa – z uwagi na to, że do zadań Pełnomocnika należy ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, a także może on przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie (art. 63 ustawy o KSC).

Nowy art. 36g

Artykuł 36g zawiera upoważnienie ustawowe dla Rady Ministrów do określenia w drodze rozporządzenia sposobu niszczenia materiałów zawierające informacje, które zespół CSIRT uzyskał w trakcie przeprowadzania oceny bezpieczeństwa, a także tryb działania komisji jak i wzór protokołu. Przy wydaniu rozporządzenia powinien być wzięty pod uwagę rodzaj materiałów podlegających zniszczeniu. W szczególności chodzi tutaj o tajemnice prawnie chronione, zgodnie z art. 36e ust. 6.

2.1.10 Zmiany w przepisach o przetwarzaniu danych

Zmiany w art. 37

W art. 37 dodano wyłączenie stosowania ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[37)], do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów. Wskazać należy, że zgłoszenie incydentu może zawierać wrażliwe dane dot. kluczowych dla państwa podmiotów gospodarczych, takich właśnie jak operatorzy usług kluczowych czy dostawcy usług cyfrowych. Udostępnienie informacji o tym, że u konkretnego operatora usługi kluczowej, np. elektrociepłowni, szpitalu czy kopalni, wystąpiły podatności w systemach informacyjnych czy incydenty poważne może zachęcić przestępców lub podmioty nieprzychylne Państwu do dokonania cyberataku na te podmioty. Z tego też powodu projektodawca uważa, że znajdzie zastosowanie artykuł 1 ust. 2 dyrektywy 2019/1024[38)] ze względu na konieczność ochrony bezpieczeństwa narodowego.

[36)] Art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. 2022 r. poz. 2512).

[37)] Dz. U. 2021 r. poz. 1641 oraz z 2022 r. poz. 1700.

[38)] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego.

Zmiany w art. 39

Zmiany w art. 39 umożliwią przetwarzanie danych pozyskanych w związku z incydentami i cyberzagrożeniami przez odpowiednio CSIRT sektorowe i CSIRT INT. W przypadku CSIRT sektorowych jest to zmiana wynikająca z zamiany pojęcia „sektorowy zespół cyberbezpieczeństwa" na CSIRT sektorowy.

Projekt umożliwia również przetwarzanie danych w tym danych osobowych pozyskanych przez CSIRT Telco w związku z wykonywaniem zadań związanych z reagowaniem na incydenty telekomunikacyjne. Należy wskazać, że modyfikacja przepisów polega na dopisaniu CSIRT Telco – nie są zmienione ogólne zasady przetwarzania danych przez zespoły CSIRT.

Wyjaśnienia wymaga konieczność nadania uprawnienia CSIRT Telco do przetwarzania danych osobowych pozyskanych w związku z incydentami telekomunikacyjnymi.

Incydenty telekomunikacyjne mogą być związane z różnymi rodzajami danych, w tym z danymi osobowymi. Jako przykład można wskazać zdarzenie, w którym dzienniki połączeń konsumentów zostały wykradzione lub numery telefonów użytkowników końcowych oraz numery IMSI zostały upublicznione. Atak na sieć, z której korzysta podmiot świadczący usługi OTT może spowodować utratę poufności i dostęp do wiadomości o użytkownikach np. komunikatorów internetowych. Z kolei wskutek ataku mogłaby zostać zaszyfrowana baza abonentów przedsiębiorcy komunikacji elektronicznej, wskutek czego tymczasowo niemożliwe lub utrudnione może być świadczenie usług komunikacji elektronicznej.

Aby skutecznie zareagować na tego rodzaju zdarzenia, zespoły CSIRT Telco oraz zespoły CSIRT poziomu krajowego muszą otrzymać niezbędne dane m. in. po to, aby dokonać czynności z zakresu informatyki śledczej. Niezbędne będzie przekazanie dzienników zdarzeń (logów), które mogą zawierać informacje kto, kiedy, jakiej czynności dokonał. Innym przykładem będzie przekazanie zaszyfrowanej bazy danych abonentów. Wśród tych danych często będą znajdować się dane osobowe, jak wskazano wyżej. Może być też tak, że w skład tych danych będą znajdować się informacje umożliwiające identyfikację osób, które przyczyniły się do powstania incydentu telekomunikacyjnego. W tej sytuacji niezbędne jest zapewnienie możliwości przetwarzania przez ww. zespoły CSIRT danych osobowych. Podkreślić należy, że zarówno prawodawstwo unijne jak i proponowane przepisy nakazują zgłaszanie incydentów telekomunikacyjnych spełniających określone progi ilościowe i jakościowe. Progi te będą określone w rozporządzeniu. Obecnie przedsiębiorcy telekomunikacyjni zgłaszają do Prezesa UKE naruszenia bezpieczeństwa lub integralności sieci lub usług. Liczba tych zgłoszeń nie przekracza obecnie kilkudziesięciu rocznie. Projektowane przepisy są ewolucją obecnych rozwiązań z działu VIIA ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne i ostrożnie można założyć, że liczba zgłaszanych poważnych incydentów telekomunikacyjnych będzie podobna do obecnej liczby zgłoszeń poważnych naruszeń bezpieczeństwa lub integralności sieci lub usług. Co za tym idzie ww. zespoły CSIRT będą przetwarzać dane osobowe pozyskane dopiero przy zaistnieniu szczególnego rodzaju zdarzenia, jakim będzie poważny incydent telekomunikacyjny.

Dane te będą usuwane niezwłocznie po stwierdzeniu, że nie są one konieczne do wykonywania zadań. Ustawa o KSC wprowadziła również obowiązek zachowania w tajemnicy przez zespoły CSIRT informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań, o których mowa w ustawie. Tajemnica ta będzie się również odnosić do danych osobowych pozyskanych w związku ze zgłoszeniem incydentu telekomunikacyjnego.

Podsumowując zespół CSIRT Telco oraz CSIRT poziomu krajowego będą przetwarzały w niezbędnym zakresie dane osobowe pozyskane w trakcie reagowania na poważny incydent telekomunikacyjny. Dane te będą podlegały ochronie i będą usuwane niezwłocznie po stwierdzeniu braku niezbędności przetwarzania.

Wprowadza się również możliwość przetwarzania danych osobowych pozyskanych w związku ze zgłoszeniem incydentu telekomunikacyjnego przez Prezesa UKE. Jest to związane z uprawnieniami kontrolnymi Prezesa UKE wobec przedsiębiorców komunikacji elektronicznej w zakresie wypełniania obowiązków wynikających z rozdziału 4a ustawy o KSC. Tytułem przykładu Prezes UKE będzie mógł w trakcie kontroli sprawdzić czy rzeczywiście przedsiębiorca komunikacji elektronicznej obsługiwał incydenty telekomunikacyjne – będzie mógł to ustalić przeglądając dokumentację wykrytych incydentów telekomunikacyjnych.

Wprowadza się jeszcze dodatkowy przepis regulujący zasady usuwania danych osobowych pozyskanych przez ministra właściwego do spraw informatyzacji, Pełnomocnika, Dyrektora Rządowego Centrum Bezpieczeństwa, Prezesa UKE w związku z wykonywaniem zadań wynikających z ustawy o KSC. Przepis wypełnia lukę prawną, która obecnie występuje w ustawie o KSC.

Zmiany w art. 40

Z kolei zmiany w art. 40 umożliwią przetwarzanie informacji stanowiących tajemnice prawnie chronione przez CSIRT sektorowe, CSIRT INT, CSIRT Telco. Jednocześnie zespoły te zostaną obowiązane do zachowania w tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań ustawowych.

2.1.11 Zmiany w przepisach o organach właściwych do spraw cyberbezpieczeństwa

Zmiana w art. 42

Zmiana w art. 42 polega na tym, że wnioski organu właściwego do spraw cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych będą składane niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Obecnie organ właściwy do spraw cyberbezpieczeństwa ma 6 miesięcy na przekazanie tych danych. Zmiana ta zapewni aktualność danych zawartych w wykazie operatorów usług kluczowych.

2.1.12 Zadania i obowiązki CSIRT sektorowych oraz CSIRT Telco

Zmiany w art. 44

Proponowana w nowelizacji nowa treść art. 44 wprowadza obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał operatorów usług kluczowych tego sektora w obszarze reagowania na incydenty.

Do obligatoryjnych zadań CSIRT sektorowego będzie należało przyjmowanie zgłoszeń o incydentach oraz reagowanie na incydenty. Dotychczas sektorowe zespoły cyberbezpieczeństwa miały za zadanie przyjmować zgłoszenia o incydentach poważnych i reagować na nie. Zmiana ta pozwoli CSIRT sektorowemu uzyskiwać więcej zgłoszeń o incydentach, dzięki czemu zespół będzie mógł szybciej zdobywać doświadczenie i wiedzę w ciągle zmieniającej się sytuacji w cyberprzestrzeni. Przełoży się to na skuteczną pomoc dla operatorów usług kluczowych zmagających się z incydentami. Podkreślić przy tym należy, że nadal operatorzy usług kluczowych będą prawnie obowiązani zgłaszać tylko incydenty poważne do CSIRT sektorowego. Dobrowolnie będą mogli zgłosić każdy incydent, nawet ten który nie spełnia progów incydentu poważnego.

Innymi zadaniami CSIRT sektorowego będzie:

- gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;
- współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
- współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; przepis podkreśla nadrzędną rolę zespołów CSIRT poziomu krajowego;
- współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze a także będą mogły, w uzgodnieniu z operatorem usługi kluczowej, wspierać go w wykonywaniu jego obowiązków określonych w art. 11 ust. 1–3, art. 12 i art. 13 ustawy o KSC. Będą one również uprawnione do przeprowadzania w określonych sytuacjach (zgodnie z rozdziałem 6b) testów bezpieczeństwa. Nie bez powodu wprowadzenie do wyliczenia w ust. 1b brzmi „CSIRT sektorowy może, w szczególności:" – katalog zadań CSIRT sektorowego jest katalogiem otwartym. CSIRT sektorowy powinien być dostosowany do sektora, do podmiotów które wspiera. Zależnie od oceny organu właściwego

do spraw cyberbezpieczeństwa ustawowe zadania CSIRT sektorowego mogłyby być uzupełnione o inne np. o wsparcie operatorów usług kluczowych w zakresie zarządzania ciągłością działania, czy o zadania związane z proaktywnym przeciwdziałaniem incydentom, np. tworzeniem oprogramowania bezpieczeństwa czy monitoring technologii[39]. Otwartość katalogu jest spowodowana także tym, że nie ma CSIRT, który zapewniałby wszystkie usługi zawarte w metodykach[40)], dlatego niezbędna jest tutaj zdrowa elastyczność. Projekt zakłada, że część zadań CSIRT sektorowego może być ustalona w akcie tworzącym CSIRT (np. w statucie jednostki budżetowej działającej jako CSIRT). Oczywiście te fakultatywne zadania nie mogą prowadzić do nałożenia pozaustawowych obowiązków na operatorów usług kluczowych. Organ właściwy do spraw cyberbezpieczeństwa ustanawiając te zadania powinien się kierować uznanymi metodykami tworzenia takich zespołów oraz koniecznością zapewnienia jak najlepszego wsparcia operatorom usług kluczowych.

CSIRT sektorowy będzie niezwłocznie (maksymalnie w ciągu 8 godzin) przekazywał zgłoszenie o incydencie poważnym do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK. Takie rozwiązanie gwarantuje, że zespoły CSIRT poziomu krajowego będą posiadały aktualną wiedzę o występowaniu incydentów w systemie. Za nieprzestrzeganie tego obowiązku będzie możliwe ukaranie kierownika danego CSIRT sektorowego.

Dzięki wprowadzonym zmianom operatorom usług kluczowych zostanie zapewnione najlepsze możliwe wsparcie przy obsłudze incydentów. Ponadto nowy system zgłaszania incydentów zmniejsza obciążenia administracyjne ciążące na operatorach usług kluczowych.

Należy przy tym wskazać na doświadczenia płynące z funkcjonowania CSIRT KNF – jedynego obecnie sektorowego zespołu cyberbezpieczeństwa. W 2021 r. CSIRT KNF przekazał podmiotom rynku finansowego 22 ostrzeżenia o zagrożeniach cyberbezpieczeństwa wraz z sugerowanymi działaniami mitygującymi te zagrożenia. Zespół ten systematycznie monitoruje kampanie złośliwego oprogramowania ukierunkowane na instytucje i klientów polskiego rynku finansowego. Prowadzi działalność edukacyjną poprzez szkolenia dla podmiotów nadzorowanych, publikowanie artykułów w prasie czy w mediach społecznościowych[41)]. Niezależnie od tego zespół ten wspiera 20 operatorów usług kluczowych w sektorze bankowości

---

[39)] Por. Martijn van der Heide, *Establishing a CSIRT*, str. 25.
https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf

[40)] *Ibidem.*

[41)] Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku, str. 151–154,
https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie_z_dzialalnosci_UKNF_oraz_KNF_w_2021_roku_78361.pdf.

i infrastrukturze rynków finansowych w obsłudze incydentów poważnych. W 2021 r. w tym sektorze doszło do 30 incydentów poważnych[42], a od 1 stycznia do 8 grudnia 2022 r. do 21 incydentów poważnych[43]. Dzięki istnieniu wyspecjalizowanego dla tego sektora zespołu CSIRT podmioty rynku finansowego mogły liczyć na szybką i konkretną pomoc przy incydentach poważnych związanych ze świadczeniem usług bankowości elektronicznej.

Opierając się na tych doświadczeniach projektodawca jest zdania, że powołanie analogicznych zespołów w innych sektorach gospodarki pozytywnie wpłynie na zdolności operatorów usług kluczowych w zakresie cyberbezpieczeństwa.

Uchyla się art. 44 ust. 2 ponieważ główną rolę w przekazywaniu informacji o incydentach o charakterze transgranicznym powinny być zespoły CSIRT poziomu krajowego, które są członkami sieci CSIRT Network.

Zmiana art. 44 ust. 4 oraz dodanie ust. 5–11

Zmiana w art. 44 ust. 4 polega na zmianach terminologicznych – wyrazy „sektorowy zespół cyberbezpieczeństwa" zastępuje się wyrazami „CSIRT sektorowy".

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł powierzyć realizację zadań CSIRT sektorowego jednostkom podległym lub nadzorowanym[44] albo organowi przez niego nadzorowanemu.

Przykładowo zadania CSIRT sektorowego będą mogły być powierzone jednostce budżetowej podległej danemu organowi właściwemu do spraw cyberbezpieczeństwa. Finansowanie CSIRT sektorowego odbędzie się co do zasady z budżetu państwa – jednostka budżetowa będąca CSIRT sektorowym powinna być ustanowiona dysponentem[45] środków budżetu państwa drugiego lub trzeciego stopnia z części budżetowej, której dysponentem jest organ właściwy do spraw cyberbezpieczeństwa. Do decyzji organu właściwego do spraw cyberbezpieczeństwa należeć będzie czy zadania CSIRT sektorowego zostaną powierzone istniejącej jednostce budżetowej czy też zostanie w tym celu utworzona nowa jednostka budżetowa zgodnie z art. 12 lub 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Projekt przewiduje możliwość powierzenia zadań także jednostce nadzorowanej przez organ właściwy do spraw cyberbezpieczeństwa. W szczególności CSIRT sektorowy mógłby zostać utworzony w państwowym instytucie badawczym. Zgodnie z art. 22 pkt 2 lit b ustawy z 30 kwietnia 2010 r. o instytutach badawczych do zadań państwowego instytutu badawczego należy wykonywanie m. in. zadań szczególnie ważnych dla

---

[42] Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/35639/table.

[43] Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/43252/table.

[44] Należy przy tym podkreślić, że chodzi tutaj o jednostki organizacyjne, o których mowa w art. 33 ust. 1d ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2022 r. poz. 1188).

[45] Zgodnie z rozporządzeniem Ministra Finansów z dnia 15 stycznia 2014 r. w sprawie szczegółowego sposobu wykonywania budżetu państwa (Dz. U. z 2021 r. poz. 259 z późn. zm.)

planowania i realizacji polityki państwa, których wykonanie jest niezbędne dla zapewnienia obronności i bezpieczeństwa publicznego które dotyczą monitoringu i zapobiegania skutkom zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne. Niewątpliwie zapobieganie i reagowanie na incydenty poważne stanowi materię bezpieczeństwa publicznego. Z tego powodu zasadne jest powierzenie zadań CSIRT sektorowego państwowemu instytutowi badawczemu. Zgodnie z art. 21 ust. 6 ustawy o instytutach badawczych państwowy instytut badawczy otrzymuje dotację celową na finansowanie realizacji zleconych zadań - w tej formie odbyłoby się finansowanie zadań CSIRT sektorowego.

Wprowadza się także możliwość porozumienia się organów właściwych ds. cyberbezpieczeństwa i wyznaczenia wspólnego CSIRT sektorowego dla kilku sektorów. Organ właściwy będzie mógł także, alternatywnie, porozumieć się z organami prowadzącymi CSIRT GOV, CSIRT MON, CSIRT NASK i powierzyć im realizację zadań CSIRT sektorowego. Tego rodzaju przepisy zapewnią elastyczność i efektywne wykorzystanie zasobów przy powoływaniu zespołów CSIRT sektorowych. Komunikaty o tych porozumieniach będą publikowane w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa oraz w Biuletynie Informacji Publicznej Pełnomocnika.

Nowy art. 44a

W art. 44a uregulowano obowiązki zespołu CSIRT Telco. Funkcjonowanie zespołu CSIRT Telco zapewnia Prezes UKE. Będzie on mógł powierzyć prowadzenie zespołu jednostce podległej lub nadzorowanej przez ministra właściwego do spraw informatyzacji. Zadania CSIRT Telco są analogiczne do zadań CSIRT sektorowego, ale odnoszą się do działań w zakresie wsparcia przedsiębiorców komunikacji elektronicznej w obsłudze incydentów telekomunikacyjnych.

Nowy art. 44b

Organy właściwe do spraw cyberbezpieczeństwa i Prezes UKE będą raz w roku, do 31 stycznia przedkładać sprawozdania z funkcjonowania CSIRT sektorowych i CSIRT Telco Pełnomocnikowi (art. 44b). Zapewni to Pełnomocnikowi niezbędne informacje do prowadzenia oceny funkcjonowania krajowego systemu cyberbezpieczeństwa zgodnie z art. 62 ust. 1 pkt 1 ustawy o KSC.

Art. 45 ust. 1 pkt 6 lit. c – dodanie pkt 7 i 8

Zmiana art. 45 ust. 1 w pkt 6 w lit. c polegająca na dodaniu pkt 7 jest konsekwencją wprowadzenia nowych uprawnień dla ministra właściwego do spraw informatyzacji, tj. prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.

2.1.13 Zmiany dot. systemu S46, zadań MON oraz nadzoru

Zmiany w art. 46

Proponowana w nowelizacji zmiana art. 46 określa dostęp podmiotów krajowego systemu cyberbezpieczeństwa do tworzonego na podstawie tego samego artykułu systemu teleinformatycznego (tzw.

systemu S46). Pełnomocnik oraz zespoły CSIRT poziomu krajowego będą miały stały i nieograniczony dostęp do tego systemu. Prezes UKE oraz zespoły CSIRT sektorowe będą miały dostęp do systemu w obszarze swojej właściwości. Wprowadza się obligatoryjne korzystanie przez operatorów usług kluczowych z tego systemu (od 1 stycznia 2024 r., za wyjątkiem zasady, zgodnie z którą w przypadku wyznaczenia operatora usługi kluczowej od 1 lipca 2023 r., obowiązek ten aktualizuje się w ciągu 6 miesięcy). Pozostałe podmioty krajowego systemu cyberbezpieczeństwa będą mogły uzyskać dostęp do systemu po podpisaniu porozumienia z ministrem właściwym do spraw informatyzacji. Wprowadza się przy tym przepis dostosowujący, zgodnie z którym dotychczas zawarte porozumienia w sprawie korzystania z systemu S46 zachowują ważność po wejściu w życie niniejszej nowelizacji, co zapewni ciągłość korzystania z tego systemu po nowelizacji. Ponadto wprowadza się możliwość, aby system umożliwiał wymianę danych kontaktowych o zespołach CSIRT, SOC, ISAC, a także wymianę danych o osobach wyznaczonych do kontaktu przez podmioty krajowego systemu cyberbezpieczeństwa. Zapewni to płynność informacji w ramach krajowego systemu cyberbezpieczeństwa.

Nowy art. 47a

Zgodnie z tym artykułem narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK-PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała. Narzędzia te przekazywane są przez NASK-PIB najważniejszym osobom w państwie w ramach szkoleń z cyberbezpieczeństwa. Narzędzia te są ściśle spersonalizowane i ich ponowne wykorzystanie przez inne osoby nie będzie możliwe. W związku z tym należy uregulować kwestie własności tych przedmiotów. Jako że nie da się ich ponownie wykorzystać powinny przejść na własność osób, które je otrzymały. Przepis precyzuje też, skutki prawne tego przekazania w prawie podatkowym.

Zmiana art. 48 pkt 1

Zmiana art. 48 pkt 1 polega na dodaniu CSIRT INT do grona podmiotów, które będą informowane przez Pojedynczy Punkt Kontaktowy o zgłoszonym incydencie poważnym lub incydencie istotnym dotyczącym dwóch lub więcej państw członkowskich Unii Europejskiej.

Zmiany w art. 51

W art. 51 pkt 5 w prowadza się dwie zmiany. Zgodnie z obecnym przepisem Minister Obrony Narodowej kieruje działaniami związanymi z obsługą incydentów w czasie stanu wojennego. Trzeba jednak zauważyć, że działania wojenne mogą się rozpocząć zanim zostanie wprowadzony stan wojenny. Proponuje się, żeby Minister kierował tymi działaniami również w czasie wojny. Zgodnie z art. 2 pkt 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny[46)] czas wojny jest to czas działań wojennych prowadzonych na terytorium

[46)] Dz. U. 2022 r. poz. 2305 oraz z 2023 r. poz. 347 i 641.

Rzeczypospolitej Polskiej, których początek i koniec jest określany w trybie postanowienia Prezydenta Rzeczypospolitej Polskiej wydanego na wniosek Rady Ministrów. Będzie więc precyzyjnie określony moment, w którym Minister Obrony Narodowej rozpoczyna realizację tej kompetencji. Inną zmianą w tym przepisie jest doprecyzowanie, że Minister Obrony Narodowej kieruje działaniami związanymi z obsługą incydentów a także koordynuje działania CSIRT NASK i CSIRT GOV w czasie stanu wojennego oraz czasie wojny poprzez CSIRT MON.

Zgodnie z dotychczasowym punktem 8 Minister Obrony Narodowej koordynuje we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji realizację zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa. Zakres koordynacji rozszerzono o czas wojny.

Nowy art. 52a

Proponuje się dodanie nowego art. 52a. Funkcjonowanie CSIRT MON zapewnia Minister Obrony Narodowej – w praktyce poprzez podległe mu jednostki, jak Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni czy Służbę Kontrwywiadu Wojskowego.

Zgodnie z art. 17 ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2022 r. poz. 2091) – z chwilą mianowania przez Prezydenta Rzeczypospolitej Polskiej, o ile Prezydent RP nie określi innego terminu przejęcia dowodzenia, Naczelny Dowódca Sił Zbrojnych przejmuje dowodzenie Siłami Zbrojnymi oraz jednostkami organizacyjnymi, podporządkowanymi mu zgodnie z narodowymi planami użycia Sił Zbrojnych do obrony państwa. Natomiast w myśl art. 23 ust. 1 pkt 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny, Dowódca KWOC jest właściwy w zakresie dowodzenia jednostkami wojskowymi i związkami organizacyjnymi Wojsk Obrony Cyberprzestrzeni i podlega Naczelnemu Dowódcy Sił Zbrojnych z chwilą jego mianowania i przejęcia przez niego dowodzenia Siłami Zbrojnymi.

Proponowany przepis zabezpiecza realizację zadań Ministra Obrony Narodowej wynikających z ustawy o krajowym systemie cyberbezpieczeństwa - od chwili mianowania Naczelnego Dowódcy Sił Zbrojnych.

Zmiany w rozdziale 11

Zmiany w rozdziale 11 umożliwią Prezesowi UKE nadzór i kontrolę na przedsiębiorcami komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz zgłaszania incydentów telekomunikacyjnych. Prezes UKE będzie mógł wydawać zalecenia pokontrolne wobec przedsiębiorców komunikacji elektronicznej. Ponadto będzie mógł wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego. Zmiany te pozwolą Prezesowi UKE na skutecznie badanie, czy

przedsiębiorcy komunikacji elektronicznej rzeczywiście wykonują swoje obowiązki z zakresu bezpieczeństwa sieci lub usług komunikacji elektronicznej.

2.1.14 Krajowy system certyfikacji cyberbezpieczeństwa

Po rozdziale 11 zostaje dodany rozdział 11a, zawierający przepisy 59a–59z regulujące krajowy system certyfikacji cyberbezpieczeństwa.

Nowy art. 59a

Projektowany art. 59a wyznacza zakres podmiotowy nowego systemu oraz wskazuje organ nadzoru nad jego działaniem. Do systemu będą należały Polskie Centrum Akredytacji, minister właściwy do spraw informatyzacji oraz zainteresowane jednostki oceniające zgodność i przedsiębiorcy certyfikujący swoje produkty. Należy tu podkreślić, że podmioty prywatne nie będą w żaden sposób zmuszone do dołączenia do tego systemu. Obowiązki z niego wynikające będą więc dotyczyć tylko tych, którzy dobrowolnie się im poddadzą. Tyczy się to zarówno jednostek oceniających zgodność jak i wytwórców.

Nowy art. 59b

Art. 59b wyznacza zadania dla ministra właściwego do spraw informatyzacji. Zadania te wynikają wprost z przepisów Aktu o cyberbezpieczeństwie i dotyczą nadzoru i kontroli nad podmiotami tego systemu jak również współpracy międzynarodowej w tym zakresie.

Minister właściwy do spraw informatyzacji będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w ustawie o krajowym systemie cyberbezpieczeństwa. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania nowej ustawy.

W ramach obowiązków krajowego organu minister właściwy do spraw informatyzacji będzie prowadzić szereg postępowań administracyjnych dotyczących m.in.:

- zatwierdzania certyfikatów odwołujących się do poziomu zaufania wysoki,
- wydawania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność,
- cofania i ograniczania, zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność,
- cofnięcia certyfikatu wydanego wbrew przepisom ustawy lub wbrew postanowieniom programu certyfikacyjnego,
- nakładania kar pieniężnych.

Wszystkie rozstrzygnięcia w tym zakresie będą wydawane zgodnie z przepisami Kodeksu postępowania administracyjnego, z zastrzeżeniem, że wydawania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających odbędzie się w tzw. postępowaniu uproszczonym, a pozostałe – w ogólnym.

Do obowiązków krajowego organu będą również należeć kwestie współpracy z analogicznymi organami w innych państwach Unii Europejskiej, jak również będzie przeprowadzał wzajemne przeglądy z tymi organami (art. 59b ust. 1 pkt 4). W ramach tych działań organy będą nawzajem oceniać swoje działania i funkcjonowanie krajowych systemów certyfikacji cyberbezpieczeństwa. Konieczność wdrożenia tej procedury wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

Nowy art. 59c

Projektowany art. 59c wyznacza rolę Polskiego Centrum Akredytacji (dalej „PCA"), które będzie nadzorowało jednostki oceniające zgodność pod kątem spełnienia przez nie wymogów akredytacji. PCA będzie tu pełniło taką samą rolę jaką pełni w ogólnym systemie oceny zgodności. Zapewni to szybkie wdrożenie nowych przepisów w praktyce.

Nowy art. 59d

Zgodnie z projektowanym art. 59d krajowe programy certyfikacji będą określane w drodze rozporządzeń Rady Ministrów. Przy ich tworzeniu będzie brany pod uwagę obecny stan wiedzy w dziedzinie techniki oraz kwestia potrzeb rynku w zakresie cyberbezpieczeństwa. Dzięki temu programy certyfikacyjne będą brały pod uwagę konkretne potrzeby przedsiębiorców oraz promować w tym zakresie najlepsze rozwiązania z tej dziedziny. Podstawą działania krajowego systemu certyfikacji cyberbezpieczeństwa będą jednak europejskie programy certyfikacyjne, dlatego też niniejszy przepis został ukształtowany jako fakultatywny. Dzięki temu organy będą mogły przygotowywać krajowe programy certyfikacyjne w sytuacji, gdy uznają to za korzystne dla rozwoju certyfikacji w Polsce. Przygotowanie projektu krajowego programu certyfikacji cyberbezpieczeństwa jest zadaniem ministra właściwego do spraw informatyzacji. Ze względu na konieczność szerokiego wykorzystania wiedzy specjalistycznej w ramach tych prac minister będzie mógł zlecić przygotowanie takiego dokumentu jednostkom przez siebie nadzorowanym, np. instytutom badawczych takim jak NASK- PIB czy Instytut Łączności. Przepis ten określa również elementy krajowych programów certyfikacji.

Celem krajowych programów certyfikacji cyberbezpieczeństwa jest zapewnienie, by produkty ICT, usługi ICT i procesy ICT, certyfikowane zgodnie z takimi programami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe na poziomie ustawy szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT,

usług ICT i procesów ICT. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane. W szczególności mając na uwadze, że dotyczy to tak różnych produktów jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych, w przypadku, gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów zapewni skuteczność tych programów. Trzeba wskazać, że ta różnorodność wpływa na wszelkie aspekty tych programów np. w przypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady przez jego aktualizacje podczas gdy wykrycie określonej podatności w przenośnej pamięci USB może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w programie może wymagać zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.

Nowy art. 59e

Projektowany art. 59e wprowadza obowiązek dostawcy, który poddaje swój produkt, usługę lub proces ICT ocenie zgodności, do udostępnienia jednostce prowadzącej ten proces wszelkich informacji niezbędnych do zbadania czy produkt ten spełnia wymagania zawarte w odpowiednim procesie certyfikacji. Przepis ten gwarantuje, że jednostki oceniające zgodność będą w stanie zebrać wszystkie informacje niezbędne do sprawnego realizowania ich działań.

Nowy art. 59f

Art. 59f wyznacza elementy krajowych programów certyfikacji oraz określa poziomy uzasadnienia zaufania do których będą odwoływać się certyfikaty. Przepisy te zostały przygotowane na wzór odpowiednich przepisów Aktu o cyberbezpieczeństwie przewidujących trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania jakie musi spełniać produkt by uzyskać certyfikat danego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Dzięki temu możliwa będzie promocja krajowych programów certyfikacyjnych w całej Unii Europejskiej i stosunkowo łatwe przenoszenie ich na poziom europejski. Ponadto takie rozwiązanie zapewni porównywalność certyfikatów krajowych z dokumentami z innych państw członkowskich oraz sprawi, że certyfikaty będą bardziej

przejrzyste dla zagranicznych klientów. Ust. 3 tego artykułu precyzuje podstawowe metody oceny czy produkt, usługę lub proces ICT spełnia wymagania określone w programie certyfikacji. Dla każdego z poziomów uzasadnienia zaufania zostały określone odrębne podstawowe metody oceny, w taki sposób by były one proporcjonalne do wymagań jakie będą dotyczyły tych produktów, usług czy procesów ICT.

Nowy art. 59g

Art. 59g wprowadza wyraźny obowiązek spełniania wymagań przez produktu, usługi lub procesy ICT, które uzyskały odpowiedni certyfikat lub ocenę zgodności. Przepis ten odnosi się do, określonych wcześniej, poziomów uzasadnienia zaufania wskazując ogólnie jakie wymagania muszą być spełnione przez te produkty, usługi czy procesy ICT. Szczegółowe wymagania będą określane w odpowiednich krajowych programach certyfikacji cyberbezpieczeństwa.

Nowy art. 59h

Projektowany art. 59h wyznacza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji. Aby prowadzić badania produktów, usług i procesów ICT podmioty będą musiały uzyskać akredytację PCA. Wymagania dla zainteresowanych zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. PCA będzie procedować na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Są to przepisy, na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania z ich strony.

Sprawna wymiana informacji między PCA sprawującym nadzór nad akredytacją oraz ministrem właściwym do spraw informatyzacji jest niezbędna do sprawnego działania nowego systemu. W związku z tym PCA będzie informować ministra o dokonanych akredytacjach oraz o odmowie ich dokonania. Proponowane rozwiązania gwarantują, że minister właściwy do spraw informatyzacji będzie należycie poinformowany o wszystkich podmiotach wydających certyfikaty oraz będzie posiadał informacje niezbędne do prowadzenia nadzoru nad tym rynkiem.

Nowy art. 59i

Projektowany art. 59i reguluje sytuację, gdy europejski program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku, oprócz akredytacji, te jednostki będą musiały uzyskać zezwolenia ministra właściwego do spraw informatyzacji. Zezwolenia określone w projektowanym art. 59i wynikają wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Jeśli bowiem europejskie programy certyfikacyjne będą zawierały postanowienia o szczególnych wymaganiach w zakresie jednostek oceniających zgodność musi istnieć organ sprawdzający te wymagania oraz zezwalający na ich działanie w ramach określonego programu certyfikacji. Taka regulacja wynika wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Należy podkreślić, że w związku z tym, iż postępowanie to dotyczy spełnienia formalnych kryteriów, zdecydowano o zastosowaniu w tym przypadku

przepisów o postępowaniu uproszczonym. Pozwoli to maksymalnie przyśpieszyć to postępowanie oraz ograniczy formalności. Minister w ramach sprawowanego nadzoru będzie mógł również zmieniać zakres tego zezwolenia jak i cofnąć je w przypadku, gdyby określona jednostka przestała spełniać określone wymagania. Gwarantuje to zachowanie odpowiedniej jakości usług świadczonych przez jednostki oceniające zgodność.
Ust. 4–7 tego artykułu określają precyzyjnie postępowanie w przypadku stwierdzenia, że podmiot, który otrzymał zezwolenie ministra na prowadzenie oceny zgodności w przypadku wprowadzenia w europejskim programie certyfikacji dodatkowych wymogów dla jednostek oceniających zgodność. W przypadku stwierdzenia naruszenia przepisów lub postanowień programu minister będzie mógł zawiesić wydane zezwolenie na określony czas, dając jednostce czas na usunięcie naruszeń. W przypadku gdy, w określonym terminie, naruszenia nie zostaną usunięte minister cofa wydane zezwolenie. Taki sposób postępowania gwarantuje ochronę interesu publicznego, równocześnie dając przedsiębiorcy czas na usunięciu naruszeń nie wymuszając na nim ponownego przechodzenia postępowania o wydanie zezwolenia.

Nowy art. 59j–k

Nowo dodane przepisy art. 59j–k wyznaczają ogólne zasady związane z oceną zgodności i zasadami wydawania certyfikatów. Są one utworzone w sposób analogiczny do przepisów dot. systemu oceny zgodności. Wskazują one wyraźnie, że poddanie produktów, usług i procesów ICT ocenie zgodności jest całkowicie dobrowolne. Warunki przeprowadzania oceny zgodności będą określane w europejskich i krajowych programach certyfikacji. Wskazano również, że tylko pozytywny wynik oceny zgodności jest podstawą do wydania certyfikatu.

Przepisy te określają, kiedy otrzymuje się certyfikat oraz kiedy możliwe jest wydanie deklaracji zgodności. W przypadku najniższego poziomu zaufania producent może sam przeprowadzić badanie produktu, a następnie wskazać w deklaracji zgodności, że produkt spełnia wymagania. Takie rozwiązanie stanowi ważne ułatwienie dla przedsiębiorców chcących uzyskać certyfikację przy możliwie najmniejszych kosztach. Będą mogli bowiem sami przeprowadzić niezbędne badania i wystawić deklarację zgodności. Równocześnie należy tu wspomnieć, że dalsze przepisy penalizują wprowadzanie w błąd w zakresie spełniania wymagań certyfikacyjnych. W związku z tym istnieje zabezpieczenie przed nadużywaniem tego rozwiązania. Otrzymanie certyfikatu wymaga przeprowadzenia badań produktu, usługi lub procesu ICT przez niezależny podmiot. Jest to niezbędna gwarancja dla prawidłowego przebiegu procesu certyfikacji. Należy nadmienić, że możliwość wystawienia deklaracji zgodności dotyczy jedynie najniższego poziomu uzasadnienia zaufania.

Nowy art. 59l

Projektowany art. 59l określa zagadnienia związane z wnioskiem o certyfikację w szczególności minimalne wymagania co do treści takiego wniosku. W celu usprawnienia działań podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa wszystkie dokumenty relewantne dla tego wniosku powinny zostać

złożone wraz z nim. Projektowane przepisy mają zabezpieczyć prawidłowe i sprawne prowadzenie oceny zgodności.

Nowy art. 59m

Projektowany art. 59m wyznacza obowiązek jednostki oceniającej zgodność do przekazania ministrowi właściwemu do spraw informatyzacji danych podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jej cofnięcia. Obowiązek ten jest konieczny, gdyż umożliwia ministrowi sprawowanie skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa.

Nowy art. 59n

Projektowany art. 59n daje dodatkową gwarancję dla certyfikatów najwyższego poziomu. Taki certyfikat musi być zatwierdzony przez ministra właściwego do spraw informatyzacji. Dotyczy to zarówno certyfikatów wydanych na podstawie europejskich jak i krajowych programów certyfikacji cyberbezpieczeństwa. Odmowa zatwierdzenia jest możliwa w przypadku, gdy certyfikat został wydany wbrew przepisom lub postanowieniom programu certyfikacyjnego w ramach, którego prowadzona była ta procedura. Do tego postępowania będą stosowane przepisy Kodeksu postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe dla ich stron. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające przebieg procesu oceny zgodności. Przepisy przewidują też, że w przypadku, gdy będzie to konieczne, minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów naukowych o wypowiedzenie się w kwestii danego programu certyfikacji. Wymóg ten służy do przyśpieszenia postępowania przez przekazanie do organu potrzebnych mu dokumentów wraz z wnioskiem wszczynającym postępowanie. Bez tego przepisu organ musiałby wystąpić o te dokumenty co przedłużyłoby cały proces. Przepis ten reguluje również kwestie cofania certyfikatów wydanych niezgodnie z ustawą lub przepisom programu certyfikacyjnego. Obowiązek wprowadzenia takiej procedury wynika z Aktu o cyberbezpieczeństwie.

Nowy art. 59o

Art. 59o wskazuje, że jednostka oceniająca zgodność odmawia dokonania tej oceny, o ile dostawca nie dostarcza wszystkich informacji niezbędnych czy dany produkt, usługa pub proces ICT spełnia wymagania określone w odpowiednim programie certyfikacji. Dzięki temu te jednostki będą miały wyraźną podstawę do odmowy działań w przypadku stwierdzenia, że dostawca działa w złej wierze

Nowy art. 59p

Art. 59p precyzuje kwestie związane z certyfikatami wskazując na ich role w tym systemie. Ust. 2 określa co musi być wskazane w treści certyfikatu. Szczególnie ważne jest tu wskazanie poziomu uzasadnienia zaufania, oznaczenie podmiotu, który wydał certyfikat i okresu na jaki został wydany. Przy określaniu okresu ważności certyfikatu będzie brana pod uwagę specyfikacja techniczna określonego produktu, usługi lub procesu ICT.

Nowy art. 59q

Projektowany art. 59q reguluje sytuację, gdy produkt, usługa lub proces ICT przestają spełniać wymagania już po otrzymaniu certyfikatu. Programy certyfikacyjne będą przewidywać zasady monitorowania produktów, usług i procesów, które uzyskały certyfikaty. W ramach tego monitoringu właściciele certyfikowanych produktów będą musieli wykazać, że ich towar wciąż spełnia wymagania określone w programie. W przypadku gdy przestanie je spełniać jednostka oceniająca zgodność obowiązana jest do cofnięcia certyfikatu. Musi również o tym poinformować ministra właściwego do spraw informatyzacji. Otrzymywanie takich informacji jest niezbędne by minister mógł wykonywać swoje obowiązki związane z nadzorem nad rynkiem certyfikacji.

Nowy art. 59r

Projektowany art. 59r wprowadza obowiązek jednostek oceniających zgodność w zakresie monitorowania zgodności produktów, które otrzymały certyfikaty, z wymogami wskazanymi w programie certyfikacji przez cały okres na jaki został wydany certyfikat. Aby zapewnić im możliwość realizacji tego obowiązku przyznano im uprawnienie do żądania niezbędnych informacji od dostawców produktów.

Nowy art. 59s

Reguluje sytuację, gdy produkt przestaje spełniać wymagania już po uzyskaniu certyfikatu. W takim przypadku, jeśli dostawca sam poinformuje jednostkę oceniającą zgodność o tej sytuacji, będzie miał 2 miesiące na przywrócenie zgodności z wymaganiami. Jeśli zaś taka niezgodność zostanie wykryta w ramach kontroli to certyfikat od razu zostaje cofnięty. Taka regulacja ma promować współpracę między jednostkami oceniającymi zgodność a dostawcami produktów i zachęcać ich do informowania o kwestiach problematycznych. Pozwoli to im utrzymać certyfikat i nie ponosić kosztów ponownej certyfikacji.

We wskazanym wyżej okresie dostawca nie może powoływać się na posiadany certyfikat.

Nowy art. 59t

Projektowany art. 59t reguluje kwestie związane z deklaracjami zgodności. Możliwość ich wydawania dotyczy tylko najniższego poziomu uzasadnienie zaufania i daje szansę skorzystania z programów certyfikacyjnych przy minimalnych kosztach. Producenci będą mogli sami wskazać, że ich produkty spełniają wymagania bez potrzeby przechodzenia przez proces certyfikacji co pozwoli im znacząco ograniczyć posiadane koszty. Przepis ten precyzuje również elementy jakie deklaracja zgodności musi zawierać. Te zasady gwarantują transparentność przy wystawianiu deklaracji zgodności.

Nowy art. 59u

Projektowany art. 59u nakłada na podmioty krajowego systemu certyfikacji cyberbezpieczeństwa obowiązek przesyłania kopii wystawionych deklaracji zgodności do ministra właściwego do spraw informatyzacji. Przepis ten gwarantuje, że minister będzie zdolny do wykonywania nadzoru nad tym rynkiem. Reguluje, kiedy jednostka oceniająca zgodność odmawia dokonania certyfikacji.

Nowy art. 59v

Projektowany art. 59v ustanawia domniemanie zgodności z wymogami produktów, dla których wystawione zostały deklaracje zgodności.

Nowy art. 59w

Zgodnie z projektowanym art. 59w podmiot, którego produkt, usługa czy proces ICT został certyfikowany jest obowiązany zapewnić by spełniał on wymogi określone w programie certyfikacji przez cały cykl życia danego produktu. Musi on również udostępniać użytkownikom wszelkie informacje niezbędne do bezpiecznego z nich korzystania. Postanowienia te są niezbędne do właściwego funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa. Produkty wymagają bowiem odpowiednio wyszkolonego personelu wsparcia by pełnić przypisaną im funkcję. Ponadto, w przypadku wielu produktów, usług i procesów ICT ciągłe aktualizacje są niezbędnym elementem zapewnienia bezpieczeństwa. Wiele z najbardziej skutecznych cyberprzestępstw dotykało urządzeń, które nie przeszły niezbędnych aktualizacji oprogramowania jak np. w czasie rozprzestrzeniania się wirusa WannaCry. Dlatego zagwarantowanie bezpieczeństwa systemów informacyjnych wymaga nałożenia takich obowiązków na ich dostawców.

Nowy art. 59x

Projektowany art. 59x określa obowiązki udostępniania informacji nałożone na dostawców certyfikowanych produktów. Regulacje te są niezbędne dla zapewnienia skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa.

Nowy art. 59y

Projektowany art. 59y dodaje kolejną metodę sprawowania nadzoru przez ministra właściwego do spraw informatyzacji. Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa będą musiały przekazywać ministrowi wyjaśnienia w kwestiach związanych z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa. Daje to ministrowi możliwość sprawdzania otrzymywanych informacji bez konieczności stosowania długotrwałej i uciążliwej dla przedsiębiorcy procedury kontrolnej. Umożliwi to również ministrowi zbieranie informacji o zjawiskach zachodzących na rynku certyfikacji.

Nowy art. 59z

Omawiany art. 59z daje podstawę prawną dla prowadzenia kontroli u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji. Do kontroli będą stosowane dotychczasowe przepisy ustawy o krajowym systemie cyberbezpieczeństwa. Dzięki temu organ będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli. Pozwoli to na najszybsze wdrożenie się organu do nowych obowiązków. W przypadku kontroli u podmiotów administracyjnych będzie stosowana ustawa o kontroli w administracji rządowej, a w przypadku przedsiębiorców stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2023 r. poz. 221, z późn. zm.). W związku z tym wszelkie gwarancje dla przedsiębiorców będą

zachowane w tej procedurze. Ponadto będą stosowane przepisy art. 55–59 ustawy. W art. 55 w punktach od 1 do 6 wskazano zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zauważyć, że w celu uniknięcia sytuacji, w której podmiot kontrolowany zwleka z wydaniem przepustki osobie przeprowadzającej kontrolę, przesądzono, że osoba prowadząca czynności kontrolne, legitymująca się odpowiednimi dokumentami upoważniającymi do kontroli, ma prawo do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki. Warto zaznaczyć, że uprawnienia wynikające z art. 55 dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że uprawnienia te nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli.

Art. 57 wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58). W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, iż protokół podpisują osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany, osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole.

W art. 59 wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie, poinformować organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń. Wskazana powyżej regulacja jest istotna z punktu widzenia regulacji zawartych w rozdziale 14 dotyczących nakładania administracyjnych kar pieniężnych. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej. Zgodnie z obowiązującymi regulacjami w podobnych dziedzinach, od zaleceń pokontrolnych nie przysługują środki odwoławcze, natomiast wymierzanie kar pieniężnych będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych (z możliwością zaskarżenia w toku administracyjnym

i sądowym).

Nowy art. 59za

Ponadto, dla zapewnienia realnej kontroli, nad jakością produktów, które otrzymały certyfikaty, minister właściwy do spraw informatyzacji został wyposażony w uprawnienia do przeprowadzania badań produktów (art. 59z). W zakresie analizy technicznej produktów będzie mógł zwrócić się do nadzorowanych przez siebie instytutów badawczych o wykonanie określonych czynności. Tego typu uprawnienie jest niezbędne dla zapewnienia realnego nadzoru nad jakością produktów na rynku.

Nowy art. 59zb

Art. 59zb określa procedurę przeprowadzania badań produktów, o których mowa w art. 59z oraz konsekwencje wykrycia, że produkt nie spełnia wymagań określonych w odpowiednim programie certyfikacji. Przepisy te precyzują kwestie takie jak protokół z pobrania próbki oraz określają kto ponosi koszt przeprowadzanych badań.

Nowy art. 59zc

Art. 59zc określa uprawnienia ministra właściwego do spraw informatyzacji w przypadku, gdy okaże się, że określony produkt ICT, usługa ICT lub proces ICT nie spełnia wymogów. W szczególności może on cofnąć certyfikat, jeśli tak przewiduje właściwy europejski program certyfikacyjny.

Nowy art. 59zd

Projektowany art. 59zd wskazuje, że minister właściwy do spraw informatyzacji jest też organem właściwym do rozpatrywania skarg na unijne i krajowe deklaracje zgodności dotyczące cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt, dla którego wystawiono deklarację zgodności nie spełnia wymagań określonych w programie certyfikacji. To uprawnienie dla ministra wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

Należy zauważyć, że przepisy dotyczące skarg tworzą tylko ogólne ramy dla rozpatrywania skarg. Szczegółowo kwestie te będą regulowane w aktach implementujących wydawanych przez Komisję dla poszczególnych programów certyfikacyjnych. Należy podkreślić, że będą one odrębnie określane dla każdego kolejnego programu co sprawia, że konieczne jest pozostawienie wielu kwestii nieuregulowanych w przepisach krajowych.

Skargi składane do ministra właściwego do spraw informatyzacji rozpatrywane będą zgodnie z przepisami Kodeksu postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra wskazano, że przepisy te będą stosowane odpowiednio.

2.1.15 Rekomendacje Pełnomocnika. Nowi członkowie oraz zadania Kolegium

Nowy art. 62a

Nowy artykuł 62a umożliwi wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Ten dokument będzie publikowany na stronie podmiotowej Pełnomocnika w Biuletynie Informacji Publicznej. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej, a także inne zbiory dobrych praktyk. Podkreślić należy, że rekomendacje będą formalnie niewiążące, jednak podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić je w ramach procesu zarządzania ryzykiem. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne do oszacowanego ryzyka zabezpieczenia.

Zmiana w art. 64

Zmiana w art. 64 wskazuje, że Kolegium do Spraw Cyberbezpieczeństwa jest organem opiniodawczo-doradczym również w sprawach dotyczących działalności zespołu CSIRT INT.

Zmiany w art. 64a

W nowym art. 64a określone zostały nowe rodzaje analiz jakie będą mogły być zlecane CSIRT GOV CSIRT MON lub CSIRT NASK. Będą to analizy dotyczące wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1 oraz analizy dotyczące trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. Analizy te będą wykonywane na wniosek Przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa i będą mogły posłużyć jako dowód w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka.

Zmiany w art. 65

W projektowych zmianach art. 65 rozszerzono katalog zadań Kolegium do Spraw Cyberbezpieczeństwa m. in. o wyrażanie opinii o decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie także wyrażało opinię w sprawie wyznaczenia Operatora strategicznej sieci bezpieczeństwa.

Zmiany w art. 66

W art. 66 proponuje się rozszerzenie składu Kolegium. Nowym członkiem Kolegium będzie minister właściwy do spraw energii, z uwagi na to, że sektor energii jest jednym z największych sektorów.

W posiedzeniach Kolegium będą mogli także uczestniczyć:

- Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca,

- Przewodniczący Komisji Nadzoru Finansowego,
- Prokurator Generalny albo jego zastępca,
- Szef Agencji Wywiadu albo jego zastępca,
- Szef Centralnego Biura Antykorupcyjnego albo jego zastępca,
- Szef Służby Wywiadu Wojskowego albo jego zastępca.

Ponadto, umożliwiono, aby pozostali szefowie służb (wymienieni w ust. 4) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

W ślad za odpowiednimi zmianami w innych przepisach, uzupełniono katalog kompetencji przewodniczącego Kolegium o możliwość:

- wnioskowania o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;
- zlecenia zespołom CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;
- zlecenia CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;
- wnioskowania o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1.

Przewodniczący Kolegium otrzyma także kompetencję do powołania zespołu opiniującego, o którym mowa w art. 66a ust. 10 pkt 1, oraz będzie mógł wskazać przedstawicieli członków Kolegium wchodzących w jego skład. Będzie mógł również rozstrzygnąć spór, o którym mowa w art. 66a ust. 10 pkt 2, wskazując właściwego członka zespołu opiniującego.

Ustawa o krajowym systemie cyberbezpieczeństwa nie przewiduje sytuacji nieobecności Sekretarza Kolegium do Spraw Cyberbezpieczeństwa na przykład spowodowanej czasowymi problemami zdrowotnymi. Aby zapewnić ciągłość obsługi Kolegium proponuje się wprowadzenie instytucji zastępcy Sekretarza Kolegium. Sekretarz Kolegium jest powoływany przez Przewodniczącego Kolegium - czyli Prezesa Rady Ministrów. Aby nie nakładać nadmiernych obowiązków na Prezesa Rady Ministrów zastosowano zasadę pomocniczości - zastępcę Sekretarza Kolegium będzie powoływał jak również odwoływał Sekretarz Kolegium. Będzie to też oznaczało, że Sekretarz Kolegium odpowiada przed Przewodniczącym Kolegium za wybór danej osoby na zastępcę. Kryteria wyboru zastępcy Sekretarza będą takie same, jak dla Sekretarza - zastępca będzie musiał spełniać wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”.

W przepisie wskazano jasno, że zastępca Sekretarza Kolegium wykonuje obowiązki Sekretarza w razie nieobecności tego ostatniego, w szczególności zastępuje go na posiedzeniu Kolegium.

2.1.16 Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka

Nowy art. 66a

Zawarty w rozdziale I Konstytucji[47)] art. 20 stanowi o ustroju gospodarczym Rzeczypospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości: podejmowania działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym[48)]. Państwo może więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[49)]. Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłaby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego a także prawno-międzynarodowym zobowiązaniom państwa[50)]. W tym kontekście należy wskazać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji).

Opierając się na powyższych przesłankach, projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Rozwiązanie to ma na celu zapewnienie ochrony ważnego interesu państwowego w postaci bezpieczeństwa państwa.

---

47) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. poz. 483, z 2001 r. poz. 319, z 2006 r. poz. 1471 oraz z 2009 r. poz. 946).

48) Wyrok Trybunału Konstytucyjnego z dnia 8 kwietnia 1998 r., sygn. K 10/97.

49) Ibidem.

50) Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01.

Obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi w oparciu o mobilne sieci 5G[51)]. Sieć 5G będzie oferowała możliwość przetwarzania znacznie większej liczby danych oraz wyższe prędkości przekazywania danych w porównaniu do dotychczasowej sieci 3G oraz 4G. Dzięki sieci 5G możliwe będzie podłączenie znacznie większej liczby urządzeń Internetu Rzeczy niż do tej pory. Umożliwi to znacznie większe możliwości przekazywania danych pomiędzy obywatelami oraz wpłynie pozytywnie na rozwój gospodarki.

Wdrożenie sieci 5G wiąże się z ryzykami, szczególnie tymi związanymi z bezpieczeństwem. Dzięki tym sieciom będzie możliwe świadczenie wielu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Potencjalny cyberatak mógłby doprowadzić do naruszenia dostępności danej usługi na niespotykaną dotąd skalę. Możliwy byłby atak na sieć 5G, który doprowadziłby do przejęcia kontroli nad infrastrukturą krytyczną jak np. sieci energetyczne. Przejęcie kontroli nad siecią 5G mogłoby doprowadzić do naruszenia poufności ogromnej liczby przesyłanych danych. Skutki takich incydentów byłyby bardzo poważne.

Kwestia bezpieczeństwa sieci 5G została podjęta na poziomie unijnym. W motywie 3 i 4 zaleceń Komisji (UE) 2019/534 wskazano, że:

(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane.

(4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie

---

[51)] Jako sieci 5G Komisja Europejska zdefiniowała: *zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci*. Pkt II.2.a Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz. Urz. UE L 88 z 29.3.2019, s. 42.)

członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.

Komisja zaleciła, aby państwa członkowskie przeprowadziły krajową ocenę ryzyka bezpieczeństwa sieci 5G je Komisji oraz ENISA. Ponadto Komisja zaleciła, aby w oparciu o krajową ocenę ryzyka państwa członkowskie powinny:

a) zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G,

b) zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i 13b dyrektywy 2002/21/WE,

c) obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE,

d) stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

Środki te powinny obejmować obowiązki nakładane na dostawców oraz operatorów celem zapewnienia bezpieczeństwa sieci 5G.

W wyniku powyższych zaleceń powstała unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci 5G[52)] oraz Unijny zestaw środków dla cyberbezpieczeństwa sieci 5G – tzw. Toolbox 5G[53)]. W dokumentach tych wskazano na ryzyka związane z sieciami 5G w tym także tymi związanymi z dostawcami sprzętu i oprogramowania dla tej sieci.

Jedno ze wskazanych ryzyk dotyczy dostawców, którzy znajdują się pod wpływem państw prowadzących agresywne działania w cyberprzestrzeni. Takie państwo może wpływać na dostawcę, aby wykorzystał ukryte podatności w sprzęcie lub oprogramowaniu dostarczonemu innemu państwu, aby uzyskać dostęp do

---

[52)] Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049 , zwana dalej Unijną oceną cyberbezpieczeństwa sieci 5G".

[53)] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

wrażliwych danych przesyłanych przez ten sprzęt czy też wpływać na dostępność usług świadczonych poprzez ten sprzęt. Dostawca taki będzie działał na rzecz interesów państwa, pod którego wpływem znajduje się. Prawdopodobieństwo zaistnienia tej sytuacji zależy od stopnia, w jakim dostawca ma dostęp do sieci, w szczególności jej krytycznych funkcji[54)].

Natomiast ryzyka dotyczą również aspektów technicznych - np. tego czy dostawca jest w stanie zapewnić bezpieczeństwo swoich produktów, jak reaguje na incydenty związane z tymi produktami, jak zarządza podatnościami własnych produktów. Niska jakość sprzętu i oprogramowania dostarczanego przez dostawcę, w tym ukryte podatności, może umożliwić cyberatak na sieć dokonywany przez agresywne państwa w cyberprzestrzeni, grupy *Advanced Persistent Threat* czy grupy przestępcze[55)].

Z wyżej wskazanych dokumentów wynika więc, że mogą istnieć dostawcy sprzętu lub oprogramowania, którzy poprzez dostarczany sprzęt lub oprogramowanie mogą zagrażać państwom członkowskim UE, w tym także Polsce. Przyjęło się określać takich dostawców jako „dostawców wysokiego ryzyka" (*high risk vendors).*

Toolbox 5G wskazuje środki strategiczne, które będą w stanie zmitygować ryzyka wskazane w Unijnej ocenie cyberbezpieczeństwa sieci 5G. Przede wszystkim Toolbox 5G zaleca środki strategiczne:

- SM01 – wzmocnienie roli władz krajowych – środek ten polega m. in. na wyposażenie władz krajowych w kompetencje do zakazu, ograniczenia lub wprowadzenia wymagań odnośnie produktów dla sieci 5G, biorąc pod uwagę m. in. bezpieczeństwo krytycznych (*critical and sensitive)* części sieci 5G, ryzyka związane z wpływ państw trzecich na łańcuchy dostaw 5G czy ryzyka dla bezpieczeństwa narodowego,
- SM03 – ocena ryzyka dostawców – przeprowadzenie rygorystycznej oceny ryzyka dostawców a następnie wprowadzenie niezbędnych wyłączeń w krytycznych zasobach.

W swoim komunikacie z 29 stycznia 2020 Komisja Europejska potwierdziła, że *państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi[56)].*

[54)] Unijna ocena cyberbezpieczeństwa sieci 5G str. 22, przypis 14 i 15, str. 27; Toolbox str. 43 i 44.

[55)] Unijna ocena cyberbezpieczeństwa sieci 5G pkt 2.51, Toolbox 5G str. 43.

[56)] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&_sm_au_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ

Biorąc pod uwagę powyższe stanowisko unijne zasadne jest wprowadzenie procedury umożliwiającej zbadanie ryzyk związanych z danym dostawcą sprzętu lub oprogramowania. W przypadku, gdyby ryzyka dla bezpieczeństwa państwa okazały się zbyt wysokie, taki dostawca powinien być uznany za stwarzający wysokie ryzyko.

W art. 66a została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Tak jak wyżej wspomniano kwestia cyberbezpieczeństwa sieci 5G jest kwestią strategiczną dla Unii Europejskiej z uwagi na współzależności pomiędzy sieciami telekomunikacyjnymi państw członkowskich UE. Ze względu na potencjalne szkody, które może przynieść zakłócenie funkcjonowania tych sieci jest to również materia dotycząca bezpieczeństwa państwa. Jednakże przepis nie zamyka się wyłącznie do sieci 5G. Postępowaniu będzie mógł być poddany dostawca produktów, usług i procesów ICT nie tylko dla sieci 5G, ale również dla innych systemów informacyjnych – jeżeli będzie spełniona przesłanka zapewnienia ochrony bezpieczeństwa państwa.

W rozumieniu artykułu 66a dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT[57)]. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Dzięki temu postępowaniem będą mogły być objęte wszystkie podmioty kluczowe w łańcuchu dostaw. Postępowanie nie będzie dotyczyło wszystkich produktów, usług i procesów ICT pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, dostawców usług cyfrowych, czy podmiotów publicznych:
    a. operatorzy usług kluczowych świadczą usługi kluczowe, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej,

[57)] Dla przypomnienia: produktem ICT jest element lub grupę elementów systemu informacyjnego, usługą ICT jest usługa polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych, procesem ICT jest zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT.
Zauważyć przy tym należy, że definicja systemu informacyjnego obejmuje także sieć telekomunikacyjną - por. Sejm RP VIII kadencji, druk nr 2505, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, uzasadnienie str. 18-19. https://sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505.

b. dostawcy usług cyfrowych świadczą usługi cyfrowe (internetowa platforma handlowa, usługa przetwarzania w chmurze, wyszukiwarka internetowa), które są niezbędne dla zapewnienia funkcjonowania współczesnego społeczeństwa informacyjnego,

c. podmioty publiczne realizują, za pomocą systemów informacyjnych, zadania publiczne na rzecz obywateli;

2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacji szczególnego zagrożenia (obecnie, na gruncie Prawa telekomunikacyjnego jest to 69 podmiotów):

a. przedsiębiorcy ci mają za zadanie m. in. współpracę z podmiotami i służbami wykonującymi zadania w zakresie

- ratownictwa, niesienia pomocy ludności,
- obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;

3) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej w uzasadnieniu zwani operatorami infrastruktury krytycznej (100-200 podmiotów)). Operatorzy infrastruktury krytycznej zarządzają infrastrukturą krytyczną, którą stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Podmioty te są szczególnie ważne dla zapewnienia bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu lub oprogramowania w trakcie świadczenia usług na rzecz państwa i obywateli. Podkreślić należy, że choć niniejszą nowelizacją dodaje się do podmiotów krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, to niniejsze postępowanie ma dotyczyć sprzętu lub oprogramowania wykorzystywanego przez przedsiębiorców komunikacji elektronicznej sporządzających plany działań w sytuacjach szczególnych zagrożeń.

Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały zastosowanie przepisy Kodeksu postępowania administracyjnego (Kpa). Dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, z odmiennościami wynikających ze szczególnych regulacji wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane przepisy następujących artykułów Kpa:

- Art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.
- Art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
- Art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
- Art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
- Art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu;

Wyłączenia tych przepisów Kpa są niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego.

W celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania.

Wyłączenie art. 28 Kpa jest konieczne, ponieważ postępowanie jest wszczynane z urzędu przez ministra albo na wniosek przewodniczącego Kolegium – co za tym idzie stroną jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Podobne rozwiązanie znajduje się w art. 88 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów.

Z kolei wyłączenie art. 31 Kpa wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego.

Ze względu na ogólnopolski zasięg decyzji jaka ma zostać wydana w tym postępowaniu został wyłączony art. 51 Kpa.

Kwestia metryki sprawy przy tego typu postępowaniu jest złożona. Obowiązkowo w ramach postepowania o uznaniu dostawcy za dostawcę wysokiego ryzyka będą przeprowadzane szerokie analizy podmiotu, którego dotyczy postępowanie oraz jego produktów. Ujawnienie nazwisk osób, które przeprowadzały te analizy mogłoby narazić ich na działania ze strony podmiotów zainteresowanych konkretnym wynikiem sprawy. Ponadto wiele z tych osób to funkcjonariusze, których tożsamość, ze względu na wykonywane zadania, musi być chroniona. Z powyższych względów wyłączony został art. 66a Kodeksu postępowania administracyjnego.

W związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania, konieczne jest wyłączenie udziału strony z przeprowadzanych dowodów.

Jednocześnie umożliwiono przystąpienie do postępowania na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej. Będą to tacy przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. Aby przystąpić do postępowania taki przedsiębiorca będzie obowiązany złożyć stosowny wniosek. Zmiana odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania.

Decyzja ministra właściwego do spraw informatyzacji będzie miała formę decyzji administracyjnej, co pozwoli dostawcy na złożenie skargi do wojewódzkiego sądu administracyjnego.

W przypadku, gdy dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) zawiadomienie o wszczęciu postępowania publikowane jest na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Publikacja ma skutek doręczenia po upływie 14 dni od dnia jej dokonania. Przepis ten stanowi szczególną regulację w stosunku do zasad doręczeń określonych w Kpa.

Zawiadomienie o wszczęciu postępowania wobec dostawcy, który ma siedzibę na terytorium Unii Europejskiej, Konfederacji Szwajcarskiej czy państwa członkowskiego EFTA będzie doręczane na zasadach ogólnych wynikających z Kpa. Natomiast po otrzymaniu potwierdzenia doręczenia informacja o tym będzie publikowana na stronie Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, aby uprawnieni przedsiębiorcy telekomunikacyjni mogli złożyć wniosek o dopuszczenie do postępowania na prawach strony.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek przewodniczącego Kolegium. Minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, stąd też zasadne jest, aby to on prowadził tego rodzaju postępowanie. Przed wydaniem decyzji minister właściwy ds. informatyzacji będzie obowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy.

Art. 66a ust. 10 zawiera wskazanie elementów analizy, która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[58)].

Celem opinii Kolegium jest kompleksowa analiza działalności dostawcy sprzętu lub oprogramowania. W skład Kolegium wchodzą ministrowie kluczowi dla bezpieczeństwa państwa a także szefowie służb specjalnych. Będą więc w stanie pozyskać niezbędne informacje do oceny dostawcy od swoich jednostek podległych lub nadzorowanych.

Zasadne jest, aby opinia podejmowała kwestie zagrożeń, które stwarza dostawca. Nie są to jednak zwykłe zagrożenia, lecz takie, które wpływają na bezpieczeństwo narodowe. Przepis dalej precyzuje, że chodzi o zagrożenia w wymiarze ekonomicznym, wywiadowczym oraz terrorystycznym[59)]. Ponadto konieczna będzie analiza zagrożeń, które stwarza dostawca dla zobowiązań sojuszniczych (np. w ramach NATO czy innych umów międzynarodowych) a także europejskich. Niewątpliwie zobowiązaniem europejskim jest zapewnienie na poziomie unijnym wysokiego poziomu bezpieczeństwa systemów informacyjnych (co wynika z dyrektywy NIS/NIS2) oraz bezpieczeństwa sieci i usług komunikacji elektronicznej (co wynika z EKŁE).

Kolejnym aspektem opinii powinna być analiza prawdopodobieństwa, z jakim dostawca znajduje się pod wpływem państwa. Ta część opinii skupia się na powiązaniach dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej oraz NATO. Wpływ ten może obejmować prawodawstwo danego państwa, które reguluje stosunki między państwem a dostawcą (np. w zakresie swobody działalności gospodarczej czy bezpieczeństwa przetwarzanych danych). Co istotne Kolegium powinno pochylić się także nad praktyką stosowania tych przepisów, aby sprawdzić, jak one funkcjonują - np. czy gwarancje zawarte w tych przepisach rzeczywiście są respektowane przez dane państwo.

Z uwagi na to, że współcześnie coraz więcej danych osobowych jest przesyłanych poza Unię Europejską ważna jest także kwestia ochrony danych osobowych w danym państwie - i kwestia faktycznego stosowania tych przepisów.

Opinia będzie także zawierała analizę struktury własnościowej dostawcy sprzętu lub oprogramowania - chodzi tutaj o ustalenie kto faktycznie sprawuje kontrolę własnościową nad dostawcą. Finalnie powinny być sprawdzone możliwości wpływu danego państwa na dostawcę.

[58)] *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049.

[59)] Np. cyberterroryzm w postaci ataków na infrastrukturę krytyczną państwa.

Opinia będzie więc dotyczyła otoczenia regulacyjnego dostawcy, faktycznego stosowania prawa, struktury własnościowej aż po faktyczny wpływ państwa na dostawcę. Po dokonaniu analiz uzyskany zostanie całościowy obraz relacji między dostawcą a państwem.

Rozporządzeniem wykonawczym Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonującym rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim Unia Europejska wskazała podmioty, które dokonują cyberataków na Unię lub jej państwa członkowskie. Wskazane jest, aby opinia Kolegium dotyczyła również jakie są relacje pomiędzy tymi podmiotami a dostawcą sprzętu lub oprogramowania.

Jak już wyżej wspomniano ryzyka dotyczą również aspektów technicznych produktów, usług i procesów ICT dostarczanych przez dostawcę. Dlatego do technicznych aspektów opinii należy analiza:

1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

2) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt. 1–4 oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

3) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.

Jest to związane z potencjalnymi ryzykami, które wiążą się z niską jakością sprzętu lub oprogramowania. Jak wyżej wspomniano podatności mogą być wykorzystane do cyberataków przez państwa, grupy APT czy grupy przestępcze – dlatego warto zbadać jakość produktów dostarczanych przez dostawcę.

Realizując postulaty strony społecznej dodano wymóg, aby prowadząc opinię Kolegium uwzględniło także certyfikaty produktów, usług i procesów ICT dostarczanych przez dostawcę oraz wyniki analiz łańcuchów dostaw, które przeprowadziły zespoły CSIRT poziomu krajowego oraz CSIRT INT.

Procedura sporządzania opinii Kolegium została określona w art. 66a ust. 12. Opinia zostanie przygotowana przez zespół opiniujący w skład, którego wchodzą przedstawiciele członków Kolegium. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium będzie miał kompetencję do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego. Wprowadzono obowiązek przeprowadzenia analiz łańcuchów dostaw, o których mowa w art. 64a, zanim zostanie sporządzona opinia Kolegium w sprawie dostawcy.

Po przeprowadzeniu postępowania minister właściwy do spraw informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Nie chodzi więc o zwykłe zagrożenie, tylko o jego kwalifikowaną postać. Decyzja będzie zawierać wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka – ponieważ one też stwarzają zagrożenie.

Dzięki prawnemu zidentyfikowaniu dostawcy wysokiego ryzyka będzie możliwe wprowadzenie dodatkowych środków mitygujących zagrożenie, jakie stwarza sprzęt lub oprogramowanie dostarczane przez dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – stwierdzenie poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi – decyzja ta będzie podlegała natychmiastowej wykonalności. Wskazać należy, że zastosowane w przepisie przesłanki w żaden sposób nie odnoszą się do pochodzenia dostawcy. Za dostawcę wysokiego ryzyka może być uznany zarówno podmiot zagraniczny jak również podmiot działający w kraju. Wszyscy przedsiębiorcy są obowiązani do działania w sposób nie zagrażający bezpieczeństwu państwa polskiego.

Jeżeli w trakcie postępowania zostanie stwierdzone, że dostawca nie stanowi poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, to zgodnie z zasadami ogólnymi Kpa zostanie wydana decyzja o umorzeniu postępowania.

Aby podmioty obowiązane do wycofania sprzętu mogły zastosować się do obowiązków wynikających z wydania tej decyzji administracyjnej, minister właściwy do spraw informatyzacji opublikuje ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy. Prawa strony postępowania będą zagwarantowane poprzez możliwość złożenia skargi do sądu administracyjnego.

Nowy art. 66b

Następstwem prawnego zidentyfikowania dostawcy wysokiego ryzyka powinno być zmitygowanie ryzyka, które on stwarza. Art. 66b wprowadza więc niezbędne wymogi bezpieczeństwa dla podmiotów krajowego systemu cyberbezpieczeństwa, operatorów infrastruktury krytycznej czy 69 przedsiębiorców komunikacji elektronicznej w związku z wykorzystywaniem sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.

Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy komunikacji elektronicznej sporządzający plany działań w sytuacji szczególnego zagrożenia,

nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów, usług i procesów, jak i używanych. W tym przypadku chodzi o sytuację, w której w chwili wydania decyzji dany podmiot nie ma danego produktu, usługi lub procesu ICT – nie będzie mógł więc ich używać lub z nich korzystać. Celem jest, aby nie wprowadzać kolejnych produktów, usług, procesów ICT, żeby nie zwiększać już i tak wysokiego ryzyka związanego z nimi.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji. Chodzi tutaj o sytuację, w której w chwili wydania decyzji o uznaniu za dostawcę wysokiego ryzyka dany podmiot już używa lub korzysta z produktów, usług i procesów ICT uwzględnionych w decyzji o uznaniu za dostawcę wysokiego ryzyka. Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów, usług i procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.

Natomiast przedsiębiorcy komunikacji elektronicznej, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3.

Jednocześnie wprowadzono przepis umożliwiający użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją w sprawie uznania za dostawcę wysokiego ryzyka, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji. Będzie to możliwe wyłącznie, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. Te same przepisy zostały zastosowane do podmiotów publicznych, które już zakupiły określony sprzęt w drodze zamówienia publicznego. Jest to niezbędne rozwiązanie zarówno dla zapewnienia ciągłości świadczenia usług jak również ochrony dyscypliny finansów publicznych.

Wyżej zaproponowana interwencja prawodawcy jest konieczna ze względu na istotność dla bezpieczeństwa państwa usług świadczonych przez podmioty obowiązane do wycofania sprzętu lub oprogramowania. Podmioty te mogą być związane wieloletnimi umowami z dostawcą wysokiego ryzyka na dostarczanie sprzętu lub oprogramowania czy świadczenie usług serwisowych. Bez prawnego obowiązku

stopniowego wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka podmioty te nie wycofają sprzętu lub oprogramowanie m. in. z uwagi na ryzyko odpowiedzialności kontraktowej wobec dostawcy. W konsekwencji ryzyko związane ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka nie zostanie skutecznie zmitygowane.

Podkreślić należy, że jest to wyjątek od podstawowej reguły zakazu wprowadzania do użytkowania i obowiązku wycofania ww. sprzętu lub oprogramowania w ciągu 5-7 lat. Wyjątek ten nie może być interpretowany rozszerzająco.

Wyjaśnienia wymaga termin *użytkowania* użyty w tym przepisie. Nie należy go utożsamiać z użytkowaniem z Kodeksu cywilnego, które jest ograniczonym prawem rzeczowym. Użytkowanie w rozumieniu art. 66b oznacza każdy przypadek używania czy korzystania z produktu, usługi, procesu ICT do świadczenia usług przez dany podmiot.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W proponowanych przepisach jest mowa o 5-7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia.

Proponowane rozwiązania mają wpływ na swobodę działalności gospodarczej podmiotów zobowiązanych do wycofania sprzętu – wpływają bowiem na wolność podejmowania decyzji gospodarczych. Mają także wpływ na wykonywanie niektórych atrybutów prawa własności tj. prawa do używania produktów. Wskazać należy, że przepisy te mają na celu mitygację ryzyk związanych ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka. Tak jak wyżej wspomniano korzystanie z takiego sprzętu mogłoby doprowadzić do poważnych ryzyk naruszenia poufności danych oraz naruszenia dostępności usługi. Co za tym idzie doprowadziłoby to do poważnego utrudnienia funkcjonowania obywateli - współczesnego społeczeństwa informacyjnego - a także do ryzyka przejęcia kontroli nad infrastrukturą krytyczną państwa. Wycofanie sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka jest zatem konieczne do zapewnienia funkcjonowania demokratycznego państwa prawnego.

Proponowane rozwiązania nie naruszają istoty swobody prowadzenia działalności gospodarczej. Ogranicza się wykorzystywanie przez przedsiębiorców konkretnego sprzętu lub oprogramowania do świadczenia usług - w pozostałym zakresie przedsiębiorcy będą mogli swobodnie podejmować decyzje biznesowe. Przepisy te nie naruszają również istoty prawa własności. Tak jak wyżej wspomniano nie ma mechanizmu natychmiastowego wycofania sprzętu lub oprogramowania - przez czas wycofywania z użytkowania podmioty te będą mogły w pełni wykonywać prawo własności. Ponadto w czasie wycofywania będzie można wprowadzić dotychczas posiadany sprzęt lub oprogramowanie pochodzący od dostawcy

wysokiego ryzyka, aby dokonać niezbędnych napraw usterek czy awarii, aby zapewnić ciągłość świadczenia usługi – pokazuje to, że istota prawa własności nie została naruszona. Co ważne sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka i tak podlegałby stopniowej wymianie ze względu na zużycie czy postęp technologiczny. Proponowane rozwiązanie wpisuje się więc w mechanizm stopniowej wymiany sprzętu.

Proponowane rozwiązanie wpłynie na swobodę prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka. Należy jednak podkreślić, że będzie to związane z poważnym zagrożeniem dla państwa, które stwarza ten dostawca. Jednakże istota prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka nie zostanie naruszona. Taki dostawca nadal będzie mógł prowadzić działalność gospodarczą.

Podkreślić należy, że wartością konstytucyjną, która w tej sytuacji powinna być bardziej chroniona od swobody prowadzenia działalności gospodarczej czy prawa własności jest bezpieczeństwo państwa. Państwo powinno odpowiednio zaadresować problem dostawcy wysokiego ryzyka, który może, dzięki podatnościom w sprzęcie lub oprogramowaniu które dostarczył, doprowadzić do ataku na infrastrukturę krytyczną państwa (np. inteligentne sieci energetyczne, sieci telekomunikacyjne), zakłócać funkcjonowanie organów państwa (np. poprzez ataki *man in the middle*, kradzież danych) czy zakłócić działanie kluczowych dla społeczeństwa usług (np. poprzez atak na systemy i urządzenia szpitalne, bez których znacznie utrudnione jest wykonywanie operacji ratujących życie). Może to się odbyć poprzez celowo zaprojektowane ukryte podatności lub również ukryte podatności powstałe w wyniku aktualizacji oprogramowania dostarczonego przez dostawcę wysokiego ryzyka. Wykorzystanie podatności w infrastrukturze telekomunikacyjnej, której elementy dostarczył taki dostawca, mogłoby utrudnić lub uniemożliwić funkcjonowanie usług komunikacji elektronicznej na danym obszarze.

Demokratyczne państwo prawne nie może być bezbronne i musi zawczasu identyfikować poważne zagrożenia dla jego funkcjonowania oraz skutecznie je mitygować. Ryzyka stwarzanego przez dostawcę wysokiego ryzyka (który działa pod wpływem obcych służb wywiadowczych lub grup przestępczych) oraz jego sprzęt lub oprogramowanie nie da się inaczej zmitygować, jak tylko poprzez stopniowe wycofanie takiego sprzętu. Podmioty korzystające z tych produktów, usług, procesów nie będą w stanie zidentyfikować ukrytych podatności, poprzez które dostawca wysokiego ryzyka będzie mógł dokonywać ataków. W związku z tym nie jest możliwe zmitygowanie ryzyka stwarzanego przez dostawcę wysokiego ryzyka poprzez wprowadzenie dodatkowych środków bezpieczeństwa, innych niż wycofanie sprzętu lub oprogramowania, ponieważ będą one nieskuteczne wobec ukrytych podatności pozwalających np. nagle wyłączyć sprzęt czy zakłócić telekomunikację między podmiotami.

Zmitygowanie ryzyka sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nie jest także możliwe poprzez obowiązkową certyfikację sprzętu lub oprogramowania. Standardy certyfikacyjne

nie zawsze będą w stanie pomóc przy wykryciu ukrytych podatności, zwłaszcza jeśli sam producent chce je ukryć. Ponadto standardy te są znane samemu producentowi, który może to wykorzystać.

Warto raz jeszcze podkreślić, że postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będzie postępowaniem administracyjnym. Dostawca będzie mógł przedstawić swoje racje w postępowaniu zanim zostanie uznany za dostawcę wysokiego ryzyka. Decyzja będzie mogła być zaskarżona do sądu administracyjnego, co zapewnia dostawcy możliwość obrony swoich praw. Dostawca będzie mógł być uznany za dostawcę wysokiego ryzyka, jeżeli będzie spełniał szczególnego rodzaju przesłanki - będzie stwarzał poważne zagrożenie dla obronności, bezpieczeństwa państwa.

Podsumowując - zanim dostawca zostanie uznany za dostawcę wysokiego ryzyka jego sprawa zostanie wszechstronnie wyjaśniona - nastąpi to poprzez opinię Kolegium oraz czynności przeprowadzone przez ministra właściwego do spraw informatyzacji. Dostawca będzie mógł przedstawić swoje stanowisko a w przypadku uznania za dostawcę wysokiego ryzyka - kwestionować to przed sądem administracyjnym.

Nowy art. 66c

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Podobne kompetencje będzie miał w stosunku do przedsiębiorców telekomunikacyjnych Prezes UKE. Przepis wzmocni kompetencje organów i zapewni im możliwość monitorowania procesu wycofywania produktów ICT, usług ICT i procesów ICT.

Nowy art. 66d

W artykule 66d wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze *lex specialis* do ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2023 r. poz. 259 i 803) (dalej – PPSA). Jest on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756), która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[60)]. Przepis stanowi niezbędne

[60)] Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14.

odstąpienie od zasady ustności i jawności, jednakże strona będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym.

Rozwiązanie to jest konieczne dla zapewnienia bezpieczeństwa demokratycznego państwa prawnego – ujawnienie informacji niejawnych wykorzystanych w postępowaniu o uznaniu za dostawcę wysokiego ryzyka mogłoby narazić Rzeczpospolitą na niepowetowane szkody. Nie została naruszona istota prawa do sądu, ponieważ w zakresie w jakim uzasadnienie nie zawiera informacji niejawnych (uzasadnienie prawne, kwestia wykładni, ustalenia organu niepodlegające utajnieniu) zostanie doręczone skarżącemu, dzięki czemu będzie mógł złożyć skargę kasacyjną. Rozwiązanie jest też proporcjonalne sensu stricto, bowiem sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Na poparcie tego rozwiązania warto tutaj odwołać się do wyroku Naczelnego Sądu Administracyjnego z 8 marca 2017 r. sygn. akt I OSK 1312/15: *strona skarżąca – z istoty sprawy mająca ograniczony dostęp do szeregu informacji z nią związanych – powinna móc działać w zaufaniu, że zasadniczo pełny dostęp do informacji posiada sąd, do którego zwraca się ona o kontrolę działania organu administracji publicznej, i że tę kontrolę sąd ten dokona w sposób niezależny i niezawisły w oparciu o pełną wiedzę wynikającą z ustaleń organu, w tym także niejawnych.*

Nowy art. 66e

Projektowany art. 66e określa, że minister właściwy do spraw informatyzacji będzie prowadził wykaz decyzji o uznaniu za dostawcę wysokiego ryzyka w podziale na produkty, usługi i procesy w nich wskazane. Ułatwi to dostęp do informacji o niebezpiecznych produktach, usługach i procesach ICT.

2.1.17 Ostrzeżenie

Nowy art. 67a

Przepisy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zawierają dodanie szczególnego środka – ostrzeżenia (art. 67a). Jego stosowanie będzie ograniczone do niektórych grup podmiotów gospodarki i społeczeństwa. Będzie mogły być stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) incydentu krytycznego. Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie – po przeprowadzeniu należytej oceny – może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.

Obecnie państwo nie dysponuje środkami prawnymi, które umożliwiałyby skuteczną reakcję na incydent krytyczny. Oczywiście za obsługę incydentu krytycznego odpowiada jeden z zespołów CSIRT poziomu krajowego, który będzie współpracował z podmiotem, u którego wystąpił incydent krytyczny. Podkreślić jednak należy, że cyberataki mogą nie dotyczyć jednego podmiotu, a skutki takich ataków mogą się rozszerzać na inne podmioty w bardzo szybkim czasie. Zespoły CSIRT mogą nie nadążyć w obsłudze takiego incydentu krytycznego, który dotyczy wielu podmiotów. Jako przykład można podać sytuację, gdy cały świat zmagał się z podatnością Log4Shell. Była to krytyczna podatność, która mogła być wykorzystywana przez grupy *advanced persistent threat*[61)]. Innym przykładem są ataki na wiele podmiotów administracji rządowej na Ukrainie.

Przed wydaniem ostrzeżenia niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.

Pełnomocnik będzie mógł wydać ostrzeżenie, które będzie miękkim, niewiążącym środkiem wskazującym na ryzyko związane z możliwością wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko wystąpienia tego incydentu. Instrument ten jest wzorowany na ostrzeżeniach wydawanych przez czeską Narodową Agencję Bezpieczeństwa Cybernetycznego i Informacji. Ostrzeżenie jako miękki środek będzie zawierało zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu. Katalog możliwych zaleceń został wskazany w art. 67a ust. 9. Może to być m.in. zalecenie zastosowania określonej poprawki bezpieczeństwa, szczególnej konfiguracji sprzętu lub oprogramowania lub zalecenie zaprzestania korzystania z określonego sprzętu lub oprogramowania. Decyzja o zastosowaniu się do ostrzeżenia będzie należała do adresatów ostrzeżenia.

Nowy art. 67b

Z uwagi na konstytucyjną niezależność Narodowego Banku Polskiego nie będą do niego stosowały się przepisy dotyczące wycofania produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka. Minister właściwy do spraw informatyzacji będzie informował Prezesa Narodowego Banku Polskiego o wydaniu decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka. Prezes Narodowego Banku Polskiego zdecyduje zatem czy wycofa produkty ICT, usługi ICT oraz procesy ICT wskazane w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka.

[61)] https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/

Nowy art. 67c

W art. 67c dodano opcjonalną możliwość przekazania zadań zespołów CSIRT, określonych w art. 26, Ministrowi Obrony Narodowej. Decyzję w tej sprawie podejmie Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa oraz w uzgodnieniu z Ministrem Obrony Narodowej. W decyzji zostaną określone m.in. zakres, czas powierzenia zadań a także fakultatywnie szczegóły współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV. Zadania te będą realizowane przez Ministra Obrony Narodowej za pomocą jego jednostek podległych lub przez niego nadzorowanych. Decyzja będzie ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". Ponadto celem poinformowania podmiotów krajowego systemu cyberbezpieczeństwa informacja o ogłoszeniu decyzji będzie publikowana na stronach internetowych CSIRT GOV, CSIRT MON, CSIRT NASK lub jest udostępniania w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

2.1.18 Zmiany w przepisach o administracyjnych karach pieniężnych

W związku ze zmianami w przepisach materialnych należało odpowiednio zmodyfikować przepisy o karach administracyjnych. Kary administracyjne pełnią w systemie prawa przede wszystkim funkcję prewencyjną oraz represyjną[62)], dlatego niezbędne jest ich prawidłowe ustanowienie oraz zapewnienie skutecznego stosowania. W art. 73 ustawy, będącym przedmiotowo-podmiotowym katalogiem kar pieniężnych, wprowadzono zmiany zarówno techniczne, ujednolicające jak i dodano przesłanki ponoszenia odpowiedzialności przez operatora usługi kluczowej. Nadto wprowadza się w ustawie o Krajowym Systemie Cyberbezpieczeństwa karę na operatora usługi kluczowej, który z własnej winy nie korzysta z systemu S46 w celu realizacji obowiązków z art. 11, czyli przekazywania zgłoszeń incydentów poważnych. Kara nie będzie więc nakładana np. w sytuacjach siły wyższej, gdy z powodów technicznych nie było możliwości przekazania zgłoszenia. Ponadto wprowadza się karę za brak współdziałania operatora usługi kluczowej z CSIRT sektorowym podczas obsługi incydentu poważnego, a także za niezapewnienie temu zespołowi dostępu do informacji o rejestrowanych incydentach.

Co więcej nowelizacja przewiduje poszerzenie katalogu podmiotów, które będą podlegały obligatoryjnej odpowiedzialności karnoadministracyjnej. W szczególności przewidziane zostały kary za posługiwanie się certyfikatem lub deklaracją zgodności w przypadku niespełniania przez dany produkt warunków określonych w programie certyfikacji. Zapewnia to, że próby nadużycia systemu będą spotykały się ze zdecydowaną

---

62) H. Kisilowska, G. Zieliński, *Administracyjne kary pieniężne – funkcja prewencyjna i represyjna,* Prawo w działaniu, Sprawy Karne, 43/2020, s. 160.

reakcją. Odpowiedzialności podlegać będą też m.in. osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, które utrudniają lub uniemożliwiają właściwym organom prowadzenie czynności kontrolnych. Wysokość kar administracyjnych została odpowiednio zróżnicowana tak by były one skuteczne, proporcjonalne do czynu oraz odstraszające (art. 73 ust.1a–1c).

Przewidziano także kary dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka. Kara dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka będzie nakładana w sytuacji naruszenia przez te podmioty obowiązków określonych w art. 66b, a zatem w sytuacji wprowadzania do użytkowania typów produktów, rodzajów usług i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka lub w sytuacji niewycofania z użytkowania przedmiotowych produktów, usług bądź procesów ICT dostarczanych przez dostawcę wysokiego ryzyka w terminie do 7 lat od ogłoszenia lub udostępnienia informacji o decyzji. Obydwie kary będą wynosiły do 3% całkowitego rocznego światowego obrotu danego podmiotu z poprzedniego roku obrotowego. W przypadku podmiotów publicznych kara będzie wynosić do 100 000 zł.

Ponadto, niezależnie od kary pieniężnej w przypadku podmiotu publicznego, który nie wyznaczył osób, o których mowa w art. 21 ustawy, minister właściwy do spraw informatyzacji zyskuje uprawnienie do nałożenia w drodze decyzji na kierującego podmiotem publicznym, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek. Podobne rozwiązanie przyjęto przy niewypełnianiu przez podmiot obowiązków informacyjnych o których mowa w art. 66c, przy czym w tym wypadku kara pieniężna nałożona na kierującego podmiotem może wynosić do 300% jego miesięcznego wynagrodzenia. Sankcję tą może w drodze decyzji nałożyć organ uprawniony do żądania informacji zgodnie z właściwością, która została określona w art. 66c ust. 2. Jak zostało powyżej podniesione, jest to uprawnienie ministra do spraw informatyzacji bądź innego właściwego organu (art. 66 ust. 2), a zatem odpowiedzialność karnoadministracyjna w tym przypadku jest fakultatywna.

Odnosząc się do fakultatywnej odpowiedzialności karnoadministracyjnej, należy wskazać, że art. 73 ust. 2d wprowadza możliwość nałożenia kary pieniężnej wyłącznie, gdy przemawia za tym charakter lub zakres naruszenia. Takie określenie jest niezbędne, aby zapewnić proporcjonalność w rozumieniu konieczności i adekwatności nakładanej kary do zakresu naruszenia. Może się również okazać, że działanie bądź zaniechanie podmiotu przejawia znikomą szkodliwość społeczną wobec czego niecelowe byłoby obligatoryjne karanie kierującego podmiotem. Wyjaśnienia wymagają jednak pojęcia „zakres naruszenia" oraz „charakter naruszenia".

Zakres naruszenia można zdefiniować jako rozmiar naruszenia oraz częstotliwość naruszeń. Zakres naruszenia jest niezbędny do określenia stopnia szkodliwości społecznej czynu sprawcy, a więc pozwala na

określenie rzeczywistych oraz potencjalnych skutków naruszenia prawa. Ze względu na to, że jest to pojęcie o charakterze stopniowalnym, dokonując oceny organ nakładający karę administracyjną powinien brać pod uwagę w szczególności podstawowe cele ustawy oraz szkodliwość naruszenia tj. rodzaj naruszonych obowiązków i dóbr, intensywność naruszenia, następstwa oraz wysokość wyrządzonej szkody[63)].

Charakter naruszenia należy rozumieć jako stopień zawinienia osoby podlegającej odpowiedzialności karnoadministracyjnej, tj. czy czyn został przez nią popełniony z winy umyślnej lub nieumyślnej[64]. Określając zatem charakter naruszenia organ obowiązany jest do ustalenia czy osoba podlegająca odpowiedzialności karnoadministracyjnej w tym przypadku popełniła ten czyn w zamiarze bezpośrednim, ewentualnym, poprzez lekkomyślność albo niedbalstwo. Od tego ustalenia zależeć będzie właśnie decyzja o odstąpieniu od nałożenia kary bądź o jej nałożeniu oraz wysokości.

W art. 74 wskazano organy właściwe do wymierzania administracyjnych kar pieniężnych, o których mowa w artykule poprzedzającym. Wprowadzono ogólną zasadę, że karę na przedsiębiorców komunikacji elektronicznej za niewycofanie sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nakłada Prezes UKE. Z kolei kary na operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej będą nakładać organy właściwe do spraw cyberbezpieczeństwa. W pozostałych przypadkach kary będzie nakładał minister właściwy do spraw informatyzacji.

W celu zagwarantowania prawidłowego przebiegu postępowania, a tym samym wymierzenia adekwatnej do popełnionego czynu kary pieniężnej, w stosunku do podmiotów obowiązanych do wycofania sprzętu bądź oprogramowania dostarczanego przez dostawcę wysokiego ryzyka (art. 66a ust. 1 pkt 1–4 wprowadzony zostaje art. 74a, który nakłada na te podmioty obowiązek dostarczenia danych organowi uprawnionemu do nakładania kary na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania. Jeżeli jednak dane nie zostały organowi doręczone bądź uniemożliwiają one ustalenie podstawy wymiaru kary pieniężnej, organ uprawniony do jej nałożenia ustala podstawę wymiaru kary w sposób szacunkowy biorąc pod uwagę wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu. Przyjęcie takiego rozwiązania ma przyczynić się do zapewnienia realizacji zasady szybkości postępowania oraz zasady proporcjonalności.

Mając na uwadze konieczność zapewnienia sprawnego przekazywania zgłoszeń incydentów z CSIRT sektorowego czy CSIRT INT do właściwego CSIRT poziomu krajowego wprowadza się karę za nie

---

63) M. Czyżak, *Fakultatywna odpowiedzialność karnoadministracyjna w świetle nowelizacji prawa telekomunikacyjnego z 10 maja 2018 r,* internetowy Kwartalnik Antymonopolowy i Regulacyjny, nr 3(8), 2019, s. 69-70.

64) Ibidem, s. 70.

wykonanie tego obowiązku. Kara będzie nakładana na kierownika CSIRT sektorowego i CSIRT INT w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku.

W związku z nałożeniem na przedsiębiorców komunikacji elektronicznej zadań i obowiązków, wprowadza się sankcje za niewykonywanie obowiązków wyszczególnionych w art. 76a–76c. Zgodnie z tymi przepisami, karze pieniężnej podlegać będzie przedsiębiorca komunikacji elektronicznej, który:

1) nie wypełnia obowiązku systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia, o którym mowa w art. 20 ust. 2;

2) nie podejmuje środków, o których mowa w art. 20a ust. 2 pkt 2;

3) nie dokumentuje czynności, o których mowa w art. 20a ust. 2 pkt 1 i 2;

4) nie przekazuje informacji, o których mowa w art. 20b ust. 2, w terminie wskazanym w żądaniu Prezesa UKE;

5) nie wykonuje obowiązku, o którym mowa w art. 20b ust. 4, w terminie wskazanym w decyzji Prezesa UKE;

6) nie obsługuje incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;

7) nie zgłasza poważnego incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;

8) nie współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco lub z właściwym CSIRT GOV, CSIRT MON, CSIRT NASK i tym samym nie wykonuje obowiązku, o którym mowa w art. 20d ust. 1 pkt 3 i 4;

9) nie usuwa, w wyznaczonym przez Prezesa UKE terminie, podatności, która doprowadziła lub mogła doprowadzić do incydentu telekomunikacyjnego lub krytycznego, o której mowa w art. 54a;

10) nie wykonuje zaleceń pokontrolnych Prezesa UKE, o których mowa w art. 59.

Ponadto, zgodnie z art. 76 ust. 2 sankcje przewiduje się za:

1) niewyznaczenie przez przedsiębiorcę komunikacji elektronicznej dwóch osób, o których mowa w art. 20a ust. 4;

2) niezapewnienie dostępu do informacji o rejestrowanych przez przedsiębiorcę komunikacji elektronicznej incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań;

3) niewykonywanie obowiązku, o którym mowa w art. 20f ust. 1 i 2;

4) niewykonywanie obowiązku, o którym mowa w art. 20h ust. 5.

Kary w powyżej przytoczonych sytuacjach będzie nakładał Prezes UKE. Należy jednak zwrócić uwagę na to, że art. 76a ust. 1 i ust. 2 dotyczy dwóch różnych odpowiedzialności karnoadministracyjnych. Pierwsza sytuacja to odpowiedzialność o charakterze obligatoryjnym, a zatem Prezes UKE będzie miał obowiązek nałożenia kary pieniężnej na przedsiębiorcę komunikacji elektronicznej, gdy zajdą przesłanki enumeratywnie wymienione w art. 76a ust. 1. W ust. 2 przewiduje się odpowiedzialność fakultatywną, wobec czego nadaje się uprawnienie Prezesowi UKE do nałożenia kary pieniężnej na przedsiębiorcę komunikacji elektronicznej, jeżeli przemawia za tym charakter lub zakres naruszenia. Przesłanki dotyczące charakteru i zakresu naruszenia należy rozumieć analogicznie względem uzasadnienia art. 73 ust. 2d. Wprowadza się również dopuszczalność nałożenia kary pieniężnej nawet w sytuacji zaprzestania naruszania prawa przez podmiot bądź naprawienia wyrządzonej przez niego szkody. Uprawniony będzie do tego Prezes UKE po uznaniu, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

Powyższe kary będą nakładane przez Prezesa UKE w drodze decyzji, której nie nadaje się rygoru natychmiastowej wykonalności. Górna granica nałożonej kary została ustalona na poziomie 3% przychodu ukaranego podmiotu osiągniętego w poprzednim roku kalendarzowym. Przepisy przewidują również sposób ustalania wysokości wymiaru kary, w przypadku, gdy podmiot nie osiągnął przychodu bądź nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary.

Wymierzanie kar pieniężnych co do zasady będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych tj. przy zastosowaniu przepisów działu 4A Kodeksu Postępowania Administracyjnego (z możliwością odwołania i drogi sądowej).

2.1.19 Strategiczna sieć bezpieczeństwa

Nowy art. 76c.

Celem tworzonej strategicznej sieci bezpieczeństwa jest zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w aspekcie telekomunikacyjnym, czyli związanym z nadawaniem, odbiorem lub transmisją informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Podmiotem zobowiązanym do jej uruchomienie oraz zarządzania będzie operator strategicznej sieci bezpieczeństwa (OSSB). Przepis ten precyzuje również, że strategiczna sieć bezpieczeństwa jest siecią telekomunikacyjną w rozumieniu Prawa komunikacji elektronicznej.

Stworzenie strategicznej sieci bezpieczeństwa jest niezbędne i konieczne, ponieważ usługi telekomunikacyjne związane z obronnością i bezpieczeństwem państwa powinien świadczyć podmiot kontrolowany w całości przez państwo, wolny od wpływów podmiotów trzecich.

w szczególności infrastruktura telekomunikacyjna służąca tego rodzaju usługom powinna być pod kontrolą państwa.

Istotne jest zapewnienie, aby dane na temat osób realizujących zadania z zakresu obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego podczas wypełniania obowiązków służbowych były w jak najmniejszym stopniu przetwarzane przez podmioty niepubliczne. Utworzenie strategicznej sieci bezpieczeństwa jest przydatne do osiągnięcia tego celu bowiem sieć ta będzie odrębna od innych sieci telekomunikacyjnych i będzie zarządzana przez podmiot znajdujący się pod kontrolą państwa.

Utworzenie strategicznej sieci bezpieczeństwa jest konieczne do osiągnięcia ww. celu. Obecnie organy administracji korzystają, przy realizacji zadań z zakresu obronności czy bezpieczeństwa państwa z usług operatorów znajdujących się, ze względu na strukturę, pod wpływem podmiotów trzecich. Sytuacja ta może zagrażać bezpieczeństwu przekazywanych informacji, a co za tym idzie zagraża bezpieczeństwu państwa.

Utworzenie strategicznej sieci bezpieczeństwa oraz jej operatora jest zdaniem projektodawcy najmniej uciążliwym rozwiązaniem. Podkreślić należy, że nie chodzi tutaj o utworzenie operatora, który świadczyłby usługi telekomunikacyjne do wykonywania wszystkich zadań administracji. Operator ten będzie świadczył jedynie usługi telekomunikacyjne związane ze szczególnymi zadaniami – tymi związanymi z bezpieczeństwem państwa. W pozostałym zakresie organy administracji będą mogły w swobodnym zakresie korzystać z usług różnych przedsiębiorców telekomunikacyjnych. Strategiczna sieć bezpieczeństwa będzie zapewniała poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych niezbędny do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Operatora strategicznej sieci cyberbezpieczeństwa będzie wyznaczał Prezes Rady Ministrów. Wpierw będzie zasięgał opinii Kolegium do Spraw Cyberbezpieczeństwa w tej sprawie. Wskazanie, jako organu wyznaczającego Operatora strategicznej sieci bezpieczeństwa, Prezesa Rady Ministrów wynika ze szczególnej pozycji ustrojowej tego organu, który na mocy art. 148 Konstytucji Rzeczypospolitej Polskiej nie tylko reprezentuje Radę Ministrów i kieruje jej pracami, ale także zapewnia wykonywanie polityki Rady Ministrów. Polski system prawa sytuuje władzę wykonawczą jako odpowiedzialną za zapewnienie obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, przypisując zadania w tych obszarach poszczególnym organom administracji rządowej, w szczególności ministrom kierującym działami administracji rządowej. Tworzona strategiczna sieć bezpieczeństwa ma zapewnić bezpieczną komunikację na potrzeby realizacji tych zadań, jej Operator ma świadczyć usługi w ramach tej sieci podmiotom realizującym zadania z zakresu bezpieczeństwa państwa. Ponadto, Prezes Rady Ministrów jest przewodniczącym zarówno Kolegium do Spraw Służb Specjalnych, Rządowego Zespołu Zarządzania Kryzysowego, jak i Kolegium do Spraw Cyberbezpieczeństwa. A zatem wskazanie Prezesa Rady Ministrów jako organu wyznaczającego operatora strategicznej sieci bezpieczeństwa jest w pełni uzasadnione.

Przez pojęcie zarządzania siecią, użyte w art. 76c ust. 2, należy rozumieć dokonywanie wszelkich czynności zarządczych związanych zarówno z bieżącym utrzymaniem tej sieci, zapewnieniem bezpieczeństwa, w tym bezpieczeństwa świadczonych w sieci usług, jak i modernizacją i rozwojem sieci, które są nierozerwalnie związane z podnoszeniem poziomu bezpieczeństwa oraz jakości świadczonych usług.

Wprowadza się fakultatywne upoważnienie ustawowe do wydania rozporządzenia przez Prezesa Rady Ministrów. Organ ten będzie mógł określić w rozporządzeniu minimalne wymagania techniczne jakie musi spełniać strategiczna sieć bezpieczeństwa oraz minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo–technicznej.

Nowy art. 76d.

Strategiczna sieć bezpieczeństwa będzie zarządzana przez OSSB wskazanego przez Prezesa Rady Ministrów. Wybór Prezesa Rady Ministrów jest ograniczony do kręgu podmiotów, które spełniają łącznie następujące warunki:

– będących jednoosobową spółką Skarbu Państwa,

– będących przedsiębiorcą telekomunikacyjnym,

– posiadających infrastrukturę telekomunikacyjną niezbędną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego,

– posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,

– posiadających świadectwo bezpieczeństwa przemysłowego pierwszego stopnia,

– dających rękojmię należytego wykonywania zadań operatora strategicznej sieci bezpieczeństwa.

Przyjęcie przez podmiot funkcji OSSB nastąpi po wyrażeniu przez niego zgody.

OSSB będzie przedsiębiorca telekomunikacyjny, który już dostarcza sieć telekomunikacyjną za wynagrodzeniem. Dlatego zasadne jest, aby działalność OSSB polegająca na zarządzaniu strategicznej sieci bezpieczeństwa była wyodrębniona m. in. pod kątem rachunkowości. Operator strategicznej sieci bezpieczeństwa ma świadczyć bezpieczne usługi dla szeregu kluczowych podmiotów administracji publicznej. Są to podmioty należące do różnych działów administracji rządowej. W związku z tym działalność OSSB będzie wpływać na realizację zadań administracji podlegającej różnym ministrom. Z tego względu jego wyznaczenie nie może zostać powierzone jednemu z ministrów, ale organowi, który posiada ogólne kierownictwo w kwestiach działań administracji publicznej.

Nowy art. 76e.

OSSB świadczy usługi telekomunikacyjne, a także może świadczyć inne usługi (np. w zakresie bezpieczeństwa, czy usługi związane z telekomunikacyjnym procesem inwestycyjnym) w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

OSSB oprócz możliwości korzystania, tak jak wszystkie inne podmioty cywilne, z częstotliwości przeznaczonych dla użytkowania cywilnego, będzie mógł także świadczyć swoje usługi telekomunikacyjne w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym. Zgodnie z obowiązującymi regulacjami częstotliwości rządowe lub użytkowane jako rządowe w użytkowaniu cywilno-rządowym, mogą być wykorzystywane wyłącznie przez określonych ustawą użytkowników, będących użytkownikami rządowymi.

Wykorzystanie częstotliwości rządowych przez OSSB będzie koordynowane przez Ministra Obrony Narodowej, jednakże koordynacja częstotliwości rządowych w zakresie 703–713 MHz oraz 758–768 MHz w drodze pewnego wyjątku zostaje powierzona Prezesowi Urzędu Komunikacji Elektronicznej (dalej jako „Prezes UKE"). Takie rozwiązanie jest konieczne ze względu na przewidzianą w niniejszej ustawie możliwość współużytkowania, w ramach jednej sieci telekomunikacyjnej, tych częstotliwości z częstotliwościami cywilnymi z zakresu 713–733 MHz oraz 768–788 MHz. W takim przypadku, organ regulacyjny odpowiedzialny za gospodarowanie widmem w Polsce musi mieć realne narzędzia, które umożliwią właściwe, a przede wszystkim niepowodujące szkodliwych zakłóceń, użytkowanie, współużytkowanych zakresów widma radiowego. Z tego także powodu wykorzystanie częstotliwości rządowych z zakresu 703–713 MHz oraz 758–768 MHz będzie wymagać uzyskania pozwolenia radiowego, które nie jest wymagane dla użytkowników rządowych.

Nowy art. 76f

W ust. 1. wskazano, że OSSB będzie świadczył na wniosek usługi telekomunikacyjne podmiotom najważniejszym z punktu widzenia bezpieczeństwa państwa, tj.: Kancelarii Prezydenta RP, Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezesa Rady Ministrów, Biuru Bezpieczeństwa Narodowego, urzędom obsługującym organy administracji rządowej, organy jednostek samorządu terytorialnego oraz instytucjom podległym tym organom lub przez nie nadzorowanym, wykonującym zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności państwa, ochrony granicy państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sprawiedliwości, w tym sądownictwa i prokuratury, Siłom Zbrojnym Rzeczypospolitej Polskiej oraz innym jednostkom organizacyjnym podległym lub nadzorowanym

przez Ministra Obrony Narodowej.

W zakresie art. 76f ust. 1 pkt 6 należy podkreślić, że usługi OSSB świadczone na rzecz urzędów obsługujących organy administracji rządowej będą wykorzystywane przede wszystkim przy realizacji zadań określonych w przepisach jako zadania organu. W praktyce zadania te wykonywane są przez pracowników urzędów obsługujących dany organ. W związku z tym nie istnieją przeszkody, które uniemożliwiałyby korzystanie z usług operatora przy wykonywaniu ustawowych zadań organów.

Jednocześnie OSSB będzie świadczył usługi telekomunikacyjne także instytucjom wykonującym na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa, również na wniosek tych podmiotów.

Projekt zakłada nałożenie na ww. podmioty obowiązku korzystania z usług telekomunikacyjnych świadczonych przez OSSB w ruchomej publicznej sieci telekomunikacyjnej w zakresie niezbędnym do zapewnienia w tych podmiotach realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Przyjęcie takiego rozwiązania ma zapewnić bezpieczeństwo informacji przekazywanych przy wykorzystaniu świadczonych przez OSSB usług. Jednocześnie, z uwagi na charakter działalności, obowiązek ten nie dotyczy służb specjalnych a także Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek podległych lub nadzorowanych przez Ministra Obrony Narodowej (projektowany art. 76f ust. 3). Jeżeli jednak służby specjalne albo Siły Zbrojne Rzeczypospolitej Polskiej podejmą decyzję o korzystaniu z usług telekomunikacyjnych świadczonych przez OSSB to na podstawie projektowanego art. 76f ust. 1 będą mogły wystąpić do OSSB o świadczenie takich usług.

Art. 76f ust. 4–6.

Przepis art. 76f ust. 4 przewiduje, że Prezes Rady Ministrów będzie mógł zobowiązać OSSB do świadczenia usług właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także przedsiębiorcom realizującym zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny. Wprowadzenie takiego uprawnienia dla Prezesa Rady Ministrów zwiększy elastyczność w reagowaniu na aktualne potrzeby w zakresie zapewnienia bezpiecznej wymiany informacji pomiędzy kluczowymi podmiotami odpowiedzialnymi za realizację zadań z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Prezes Rady Ministrów będzie mógł podejmować takie działania na wniosek odpowiednio ministra, we właściwości którego znajduje się określony system infrastruktury krytycznej lub Ministra Obrony Narodowej.

Z kolei przepis art. 76f ust. 5 ustawy wprowadza możliwość zlecenia OSSB świadczenia usługi wsparcia technicznego przy realizacji zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży

Granicznej, Państwowej Straży Pożarnej, Służby Ochrony Państwa oraz Policji. Usługi te są ściśle powiązane ze świadczonymi przez OSSB usługami telekomunikacyjnymi w związku z czym świadczenie ich przez inny podmiot byłoby co najmniej nieefektywne, a w wielu przypadkach niemożliwe.

Usługi wsparcia technicznego mogą polegać w szczególności na utrzymaniu, rozbudowie i modyfikacji sieci teleinformatycznych w zakresie sieci rozległych oraz zestawienia i utrzymania łączy dostępowych do takich sieci.

Świadczenie usług telekomunikacyjnych, usług wsparcia technicznego oraz innych usług, o których mowa w art. 76e ust. 1 i art. 76f ust. 1 i 2 wymaga zawarcia umowy pomiędzy stronami (art. 76f ust. 6), a umowa to musi odnosić się do jakości usług, co najmniej w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego (art. 76f ust. 7). Wskazano, że umowa określa również zasady odpłatności za świadczone usługi.

Rozwiązania zawarte w art. 76e oraz 76f zawierają rozwiązania niezbędna dla zapewnienia efektywności świadczenia usług przez OSSB. W szczególności usługi wsparcia technicznego oraz usługi badawczo-rozwojowe muszą być zapewniane w ramach bezpiecznej sieci telekomunikacyjnej. Rozdzielenie tych usług od usług telekomunikacyjnych byłyby nieefektywne, gdyż w efekcie dwa podmioty miałyby dostęp do sieci telekomunikacyjnej stosowanej przez OSSB. Prowadziłoby to potencjalnie do dodatkowych kosztów związanych z wpuszczeniem nowego podmiotu do tego systemu oraz wymagałoby to wprowadzenia dodatkowych środków bezpieczeństwa związanych z dostępem do informacji podmiotu zajmującego się świadczeniem usług wsparcia. Taka sytuacja jest nieakceptowalna z punktu widzenia wrażliwego charakteru danych jakie będą przesyłane za pośrednictwem strategicznej sieci bezpieczeństwa. Dopuszczenie dodatkowych osób do takich informacji zawsze zwiększa ryzyko wycieku danych w związku z czym inne środki nie są w stanie zapewnić realizację celów jakie służą utworzeniu strategicznej sieci bezpieczeństwa.

Nowy art. 76g.

Przepis przesądza, że przy zawieraniu umów dotyczących realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, z późn. zm.), gdyż umowy te są ściśle związane z ochroną istotnych interesów bezpieczeństwa państwa. Aby wyłączenie doszło do skutku muszą być więc spełnione dwie przesłanki – umowy muszą dotyczyć zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji oraz zachodzić konieczność ochrony istotnych interesów bezpieczeństwa państwa. Jest to rozwiązanie zgodne z art. 13 lit. a dyrektywy 2009/81/WE, zgodnie z którym nie stosuje się postanowień tejże dyrektywy do zamówień, w przypadku których stosowanie dyrektywy zobowiązałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje się za sprzeczne z jego podstawowymi interesami w zakresie bezpieczeństwa.

Wprowadzone wyłączenie jest niezbędne dla realizacji celu jaki stawia sobie niniejsza ustawa. Aby strategiczna sieć bezpieczeństwa realnie przyczyniła się do wzrostu poziomu bezpieczeństwa komunikacji kluczowych podmiotów niezbędne jest zapewnienie, aby wszystkie relewantne podmioty korzystały z tej sieci. Jeśli chociaż część z nich nie będzie z niej korzystała to przesyłanie do nich informacji wrażliwych będzie obarczone dodatkowym ryzykiem. Mamy tu do czynienia ze specyficznym efektem sieciowym, w którym korzyści z danego rozwiązania są tym większe im większa jest skala danego przedsięwzięcia. W związku z powyższym wszystkie podmioty, na rzecz których obowiązki powinien świadczyć, muszą mieć możliwość uzyskania jego usług tak szybko jak to możliwe. Z tego względu konieczne jest umożliwienie im jak najszybszego zawarcia umowy z OSSB.

Ponadto wyłączenie, o którym mowa w art. 76g ust. 1, mieści się w zakresie art. 12 ust. 1 lit. b ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych. Operatorem strategicznej sieci bezpieczeństwa będzie jednoosobowa spółka Skarbu Państwa, a więc istnieje zależność między państwem a OSSB. Państwo poprzez nadzór właścicielski (wykonywanie swoich uprawnień) będzie miało wpływ na działalność OSSB. Dzięki temu spełnione zostaną wymagania wskazane w art. 12 ust. 1 lit. a oraz c dyrektywy 2014/24/UE.

Wskazać przy tym należy, że OSSB będzie świadczył usługi w ramach strategicznej sieci bezpieczeństwa dla *stationes fisci* Skarbu Państwa. Dlatego projektodawca uważa wymaganie wskazane w art. 12 ust. 1 lit. b dyrektywy 2014/24/UE za spełnione.

Równocześnie jednak należy zwrócić uwagę, że w praktyce zastosowanie art. 12 PZP wiązałoby się z licznymi problemami praktycznymi, gdyż każdorazowo zamawiający musiałby dokonywać ocenę czy można zastosować to wyłączenie. Mogłoby to rodzić wątpliwości prawne oraz przedłużać proces zawierania umów z OSSB. Aby uniknąć wskazanych problemów i potencjalnych opóźnień zdecydowano się wprowadzić art. 76g ust. 1. Pozwoli to zapewnić sprawny proces zawierania umów z OSSB nie naruszając przy tym przepisów prawa europejskiego.

Należy też zauważyć, że stosowanie ustawy z dnia 11 września 2019 r. -Prawo zamówień publicznych do kluczowych usług telekomunikacyjnych mogłoby prowadzić do ujawnienia przez państwo polskie kluczowych informacji związanych z podstawowym interesem bezpieczeństwa państwa, o których mówi art. 346 Traktatu o funkcjonowaniu Unii Europejskiej. Kluczowe kwestie związane z technicznymi zabezpieczeniami komunikacji między najistotniejszymi organami państwa muszą pozostać tajemnicą tak aby nie ułatwiać w żaden sposób działań państw nieprzyjaznych, które mogłyby próbować przejąć taką komunikację. Każda informacja o stosowanych metodach zabezpieczania komunikacji mogłaby przyczynić się do wzrostu ryzyka tej komunikacji. Wraz z agresją Rosji na Ukrainę znacząco wzrosło zagrożenie działaniami w tym zakresie. Nie możemy ignorować tego faktu przy przygotowywaniu przepisów mających służyć bezpośrednio interesom bezpieczeństwa państwa.

Zgodnie z ust. 2 ceny usług świadczonych przez OSSB będą kształtowane zgodnie z przepisami ustawy,

tj. będą obejmowały koszty oraz rozsądną marżę. Rozwiązanie z rozsądną marżą występuje już w przepisach – por. art. 9mk ustawy z 28 marca 2003 r. o transporcie kolejowym. Mechanizm ten równoważy interesy zarówno OSSB jak i podmiotów zobowiązanych do zawarcia z nim umowy.

Nowy art. 76h

Prezes UKE będzie mógł przeprowadzić analizę cen usług telekomunikacyjnych stosowanych przez OSSB. Analiza ta będzie mogła być przeprowadzona na wniosek podmiotów korzystających z usług telekomunikacyjnych OSSB. Prezes UKE będzie miał 2 miesiące na przeprowadzenie analizy – od momentu złożenia wniosku. Jeżeli Prezes UKE stwierdzi, że ceny usług telekomunikacyjnych OSSB przekraczają koszty i rozsądną marżę to podmiot zobowiązany do zawarcia umowy z operatorem strategicznej sieci bezpieczeństwa będzie mógł rozpocząć procedurę zawarcia umowy o świadczenie usług telekomunikacyjnych z innym dostawcą usług. Po stronie OSSB powstanie również wtedy obowiązek przedstawienia usługobiorcy nowej oferty, która ponownie, na wniosek usługobiorcy, będzie podlegała analizie przez Prezesa UKE, tym razem w terminie 21 dni. Jeżeli ponownie Prezes UKE stwierdzi, że ceny usług świadczonych przez OSSB przekraczają koszty i rozsądną marżę, to będzie mógł wydać decyzję zmieniającą tą umowę. Operator strategicznej sieci bezpieczeństwa będzie również zobowiązany do udostępniania informacji na żądanie Prezesa UKE, tak aby zagwarantować, że organ będzie dysponował wszystkimi informacjami niezbędnymi do realizacji jego zadań.

Prezes UKE jako organ regulacyjny w dziedzinie rynku usług telekomunikacyjnych, jest jedynym podmiotem, który posiada kompetencję pozwalające mu ocenić czy cena zaproponowana przez OSSB odpowiada ponoszonym kosztom oraz rynkowym cenom podobnych usług. Należy podkreślić, że Prezes UKE w ramach swojej zwykłej działalności otrzymuje informacje o cenach usług oferowanych przez operatorów telekomunikacyjnych oraz jest z nimi w stałym kontakcie. Każdy inny organ musiałby osobno pozyskiwać informacje potrzebne do przeprowadzenia analiz.

Nowy art. 76i

Przepis ten reguluje obowiązki informacyjne OSSB wobec Prezesa UKE. OSSB będzie przekazywał Prezesowi UKE informacje o zawartej umowie na świadczenie usług za pośrednictwem strategicznej sieci bezpieczeństwa, w szczególności cenę oraz zakres świadczonych usług, w terminie 14 dni od dnia zawarcia umowy.

Nowy art. 76j

W art. 76j zapewniono operatorowi strategicznej sieci bezpieczeństwa możliwość uzyskania dostępu do infrastruktury technicznej, w tym współkorzystanie z niej, w celu realizacji zadań, o których mowa w art. 76c ust. 1. Wprowadzenie regulacji o charakterze szczególnym wobec przepisów art. 17-24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2023 r. poz. 733,) jest uzasadnione z uwagi na szczególny cel, któremu ma służyć wspomniany dostęp, tj. realizację zadań na rzecz obronności,

bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

Rozwiązania zawarte w art. 76j zostały opracowane na kanwie funkcjonującej obecnie regulacji - art. 17-24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, bądź wprost do nich odsyłają. Jednocześnie, z uwagi na specyfikę zadań realizowanych przez operatora strategicznej sieci bezpieczeństwa i szczególny charakter sytuacji, w jakich uzyskanie przez niego dostępu do infrastruktury technicznej będzie konieczne, zdecydowano się na wprowadzenie pewnych odstępstw od przepisów ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych.

W ust. 3 wprost wskazano, iż opłaty z tytułu dostępu do infrastruktury technicznej określa się w wysokości, która umożliwia zwrot części kosztów, które ponosi operator sieci w związku z utrzymaniem tej infrastruktury oraz z zapewnieniem dostępu.

Zdecydowano również, że podstawową formą zapewnienia Operatorowi strategicznej sieci bezpieczeństwa dostępu do infrastruktury technicznej przez operatora sieci będzie umowa. Decyzja Prezesa UKE może być wydana wyłącznie w przypadku odmowy udzielenia dostępu do infrastruktury technicznej przez operatora sieci lub niezawarcia umowy o dostępie do infrastruktury technicznej w terminie 2 miesięcy od dnia złożenia wniosku o taki dostęp. W związku z powyższym, wobec Operatora strategicznej sieci bezpieczeństwa nie znajdą zastosowania przepisy art. 18 ust. 2–10 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych. W celu przyspieszenia procedury wydania decyzji w sprawie dostępu do infrastruktury technicznej, zrezygnowano także z konieczności dokonywania uzgodnień z Prezesem URE i Prezesem UTK, o których mowa w art. 22 ust. 6 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych.

Nowy art. 76k.

W analogiczny sposób jak dostęp do infrastruktury technicznej, uregulowana została w art. 76k możliwość uzyskania przez operatora strategicznej sieci bezpieczeństwa dostępu do nieruchomości – co do zasady przepis ten bazuje na rozwiązaniach zawartych w ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych. Dostęp do nieruchomości, w tym do budynku, o którym mowa w przepisie, polega na umożliwieniu umieszczenia na tej nieruchomości infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości.

Podmiotami obowiązanymi do zapewnienia operatorowi strategicznej sieci bezpieczeństwa dostępu do nieruchomości są użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa jednostka samorządu terytorialnego oraz właściciel lub zarządca nieruchomości.

Co istotne, w odróżnieniu od dostępu, o którym mowa art. 30 ust. 1 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, dostęp do nieruchomości przez operatora

strategicznej sieci bezpieczeństwa nie ma na celu zapewnienia telekomunikacji w tym budynku, a realizację zadań, o których mowa w art. 76c ust. 1, czyli zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Ze względu na ten wyjątkowy charakter strategicznej sieci bezpieczeństwa i fakt, że jej celem jest realizacja zadań publicznych o szczególnym znaczeniu wprowadzono pewne odstępstwo od art. 30 ust. 3a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, zgodnie z którym dostęp do nieruchomości jest nieodpłatny. Zgodnie z ust. 4 pkt 2, jeżeli podmiotem zapewniającym dostęp jest jednostka samorządu terytorialnego, właściciel lub zarządca nieruchomości, operator strategicznej sieci bezpieczeństwa ponosi proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością, proporcjonalną część kosztów, które wystąpiły po stronie udostępniającego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu oraz koszty przywrócenia nieruchomości do stanu poprzedniego.

Nowy art. 76l

Od decyzji Prezesa UKE, o której mowa w ust. 76j ust. 5 oraz art. 76k ust. 5 w sprawie dostępu telekomunikacyjnego, jak również od decyzji w sprawie dostępu do nieruchomości użytkownika wieczystego lub zarządcy nieruchomości stanowiącej własność Skarbu Państwa lub jednostki samorządu terytorialnego, będzie przysługiwało odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

Nowy art. 76m.

Przepis zastrzega dla OSSB pierwszeństwo kupna sieci telekomunikacyjnych na wypadek, gdyby państwowa osoba prawna lub jednostka samorządu terytorialnego sprzedała je osobie trzeciej. Wprowadzono obowiązek poinformowania przez ww. podmioty OSSSB o zamiarze zbycia sieci telekomunikacyjnych. OSSB będzie miał nie krócej niż 2 tygodnia na skorzystanie z prawa pierwokupu. Do pierwokupu stosuje się przepisy rozdziału IV księgi III ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2022 r. poz. 1360, z późn. zm.).

Nowy art. 76n.

W sytuacjach nadzwyczajnych wzrasta potrzeba przekazywania sygnałów pomiędzy podmiotami realizującymi zadania z obszaru bezpieczeństwa państwa, porządku publicznego czy zarządzania kryzysowego. Czasowo może się okazać, że w takich sytuacjach, świadczący usługi tym podmiotom, OSSB nie dysponuje wystarczającymi zasobami częstotliwości, by zapewnić sprawną łączność wszystkim podmiotom zobowiązanym do działania w sytuacjach nadzwyczajnych na określonym obszarze. Dlatego uprawnia się Prezesa UKE do nałożenia w drodze decyzji administracyjnej na podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz udostępnienia zasobów częstotliwości z tego zakresu na rzecz OSSB. Uprawnienie to przysługuje, jeżeli wystąpi sytuacja szczególnego zagrożenia

oraz gdy OSSB wykorzysta możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758-768 MHz. Decyzja ta będzie wydawana na uzasadniony wniosek OSSB, który będzie zawierał opis sytuacji szczególnego zagrożenia, wskazanie przyczyn pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758–768 MHz i wskazanie obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia. Decyzja Prezesa UKE będzie wydana na czas określony, nie dłuższy niż czas trwania sytuacji szczególnego zagrożenia i nie dłużej niż 72 godziny. Będzie miała ona rygor natychmiastowej wykonalności.

Podmiot dysponujący tymi częstotliwościami będzie musiał niezwłocznie, nie później niż w ciągu 1 godziny, udostępnić Operatorowi strategicznej sieci bezpieczeństwa zasoby częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz. Wprowadza się tutaj wyjątek – nie będą mogły być w ten sposób udostępnione częstotliwości wcześniej udostępnione Siłom Zbrojnym RP.

OSSB będzie obowiązany udostępnić Siłom Zbrojnym RP udostępnione mu przez podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz zasoby częstotliwości z tego zakresu niezwłocznie, nie później niż w ciągu jednej godziny, na czas na jaki zostały mu udostępnione.

W przypadku udostępnienia częstotliwości operatorowi strategicznej sieci bezpieczeństwa, przedsiębiorca telekomunikacyjny nie uiszcza opłaty za prawo dysponowania częstotliwością, za okres udostępnienia częstotliwości

Wprowadza się także regulację odszkodowawczą - do roszczenia o odszkodowanie z tytułu strat poniesionych przez przedsiębiorcę telekomunikacyjnego wskutek wydania decyzji stosuje się odpowiednio przepisy ustawy z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela (Dz. U. poz. 1955).

Proponowane rozwiązanie dotyczy sytuacji nagłych, kryzysowych, niebezpiecznych, gdy OSSB nie ma wystarczających zasobów do realizacji zwiększonego zapotrzebowania na jego usługi. Obwarowane jest szczególnymi przesłankami. Udostępnienie częstotliwości jest ograniczone czasowo do okresu trwania sytuacji szczególnego zagrożenia – po tym czasie OSSB ma obowiązek zwolnić zasoby. Z tych powodów należy uznać to rozwiązanie za proporcjonalne.

Nowy art. 76o.

Reguluje obowiązek operatorów telekomunikacyjnych określenia kanału komunikacji z operatorem strategicznej sieci bezpieczeństwa. Gwarantuje to, że w przypadku wystąpienia sytuacji kryzysowej Operator będzie w stanie szybko skontaktować się z operatorami telekomunikacyjnymi i zareagować na kryzys.

Nowy art. 76p

Art. 76p określa, że w zakresie nieuregulowanym w niniejszej ustawie do operatora strategicznej sieci bezpieczeństwa stosuje się odpowiednio przepisy ustawy – Prawo komunikacji elektronicznej. Oznacza to, że

operator strategicznej sieci bezpieczeństwa posiada takie same prawa i obowiązki jak pozostali operatorzy telekomunikacyjni, z wyjątkiem kwestii uregulowanych w niniejszej ustawie.

Nowy art. 76q

Art. 76q zawiera kompetencję dla Prezesa Rady Ministrów, który może, w przypadku utraty przez OSSB co najmniej jednego z przymiotów niezbędnych do jego wyznaczenia, w drodze zarządzenia odwołać OSSB, oraz wyznaczyć nowego operatora strategicznej sieci bezpieczeństwa (art. 76q ust. 1), także z określeniem terminu skuteczności obu czynności (art. 76r ust. 2). Kompetencja ta ma charakter fakultatywny, aby zapewnić odpowiednią elastyczność, np. w sytuacji gdyby żaden podmiot w danym momencie nie spełniałby wymogów ustawowych lub w sytuacji gdy spółka wyznaczona jako OSSB przestałaby być w efekcie przekształceń spółką jednoosobową, a w ocenie Prezesa Rady Ministrów istniałaby nieproporcjonalne ryzyko związane ze zmianą OSSB w kontekście zapewnienia ciągłości świadczenia określonych usług w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Nowy art. 76r.

Nowy operator strategicznej sieci bezpieczeństwa, wyznaczony przez Prezesa Rady Ministrów, jest następcą prawnym dotychczasowego operatora strategicznej sieci bezpieczeństwa w zakresie realizacji jego zadań. Poprzez przepis szczególny przesądzony jest skutek niektórych stosunków prawnych – umowy o świadczenie usług, do których odnosi się, poprzez odesłanie, art. 76f ust. 4, 10 i 11 ustawy, wygasają z mocy prawa w terminie 3 miesięcy od dnia wydania zarządzenia.

2.1.20 Przyznanie częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz

11 marca 2013 r., na podstawie art. 4 ust. 2 Decyzji o spektrum radiowym[65)] Komisja Europejska udzieliła Europejskiej Konferencji Administracji Pocztowych i Telekomunikacyjnych (*European Conference of Postal and Telecommunications Administrations* - CEPT) zlecenia na opracowanie zharmonizowanych warunków technicznych dla pasma 700 MHz na potrzeby bezprzewodowych usług szerokopasmowej łączności elektronicznej w Unii oraz na potrzeby innych zastosowań, wspierających priorytety unijnej polityki widma radiowego. W ramach tego zlecenia, CEPT przedstawił sprawozdania nr 53[66)] (w 2014 r.) i 60[67)] (w 2016 r.), które stanowią podstawę technicznej harmonizacji pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w Europie. Komisja Europejska

---

65) Decyzja Nr 676/2002/WE Parlamentu Europejskiego i Rady Z dnia 7 marca 2002 r. w sprawie ram regulacyjnych dotyczących polityki spektrum radiowego we Wspólnocie Europejskiej.

66) *Report A from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 28 November 2014 by the ECC.*

67) *Report B from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 01 March 2016 by the ECC.*

w komunikacie pt. „Strategia jednolitego rynku cyfrowego dla Europy”[68] przedstawiła wizję powszechnego dostępu do łączności wysokiej jakości dla przedsiębiorstw i obywateli. Strategia ta zapowiadała konkretne wnioski ustawodawcze Komisji, dotyczące m.in. skoordynowanego zwalniania zakresu 694–790 MHz. Bazując na sprawozdaniach CEPT, oraz biorąc pod uwagę prace legislacyjne nad decyzją zmieniającą przeznaczenia pasma 700 MHz w Unii, 28 kwietnia 2016 r. Komisja Europejska wydała Decyzję harmonizacyjną odnośnie zakresu częstotliwości 694–790 MHz[69]. Tym samym zapewniono ujednolicone warunki techniczne, umożliwiające użytkowanie pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej i innych zastosowań zgodnie z priorytetami polityki widma radiowego na szczeblu unijnym i krajowym. 17 maja 2017 r. Parlament Europejski i Rada wydały Decyzję w sprawie wykorzystania zakresu częstotliwości 470–790 MHz w Unii Europejskiej[70] (dalej: Decyzja o zmianie przeznaczenia), na mocy której Państwa Członkowskie UE zostały zobowiązane do udostępnienia pasma 700 MHz na potrzeby usług szerokopasmowych do 30 czerwca 2020 r. lub w uzasadnionych przypadkach najpóźniej do 30 czerwca 2022 r.

Zgodnie z Krajowym Planem Działań zmiany przeznaczenia pasma 700 MHz w Polsce, którego przyjęcie wymagane było Decyzją o zmianie przeznaczenia, 28 grudnia 2018 r. na podstawie z art. 1. ust. 1. Decyzji Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii, Polska wystąpiła do Komisji Europejskiej z informacją o konieczności odsunięcia terminu udostępnienia pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej do 30 czerwca 2022 r. Wskazanym przez Polskę uzasadnionym powodem odroczenia dopuszczenia do korzystania z częstotliwości z pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewnienia usług bezprzewodowej szerokopasmowej łączności elektronicznej po dniu 30 czerwca 2020 r. (art. 1 ust. 1) były nierozwiązane problemy dotyczące koordynacji transgranicznej skutkujące szkodliwymi zakłóceniami. Brak informacji ze strony Federacji Rosyjskiej, Republiki Białorusi oraz Ukrainy o wyłączeniu do 30 czerwca 2020 r. naziemnej telewizji, działającej w paśmie 700 MHz na terenie tych krajów, uniemożliwiłby de facto w sposób niezakłócony uruchomienie pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej na terenie Polski w wymaganym terminie tj. do 30 czerwca 2020 r.

---

[68] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia jednolitego rynku cyfrowego dla Europy z dnia 6 maja 2015 r. (COM(2015) 192 final).

[69] Decyzja Wykonawcza Komisji (UE) 2016/687 z dnia 28 kwietnia 2016 r. w sprawie harmonizacji zakresu częstotliwości 694–790 MHz na potrzeby systemów naziemnych zapewniających bezprzewodowe szerokopasmowe usługi łączności elektronicznej oraz na potrzeby elastycznego użytkowania na poziomie krajowym w Unii (notyfikowana jako dokument nr C(2016) 2268).

[70] Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii.

Ramy krajowych działań wyznaczane są przez decyzje Unii Europejskiej oraz regulacje Międzynarodowego Związku Telekomunikacyjnego (International Telecommunications Union - ITU) stąd Krajowy Plan Działań zmiany przeznaczenia pasma 700 MHz w Polsce, stanowiący podstawę do dalszych decyzji ustawodawczych nie przesądza o kierunkach i sposobie wykorzystania tego zasobu. Z punktu widzenia realizacji Decyzji o zmianie przeznaczenia kluczowa jest więc zgodność podejmowanych działań na szczeblu krajowym z uwarunkowaniami Decyzji harmonizacyjnej. Zgodnie z tą Decyzją użytkowanie pasma 700 MHz do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej będzie opierało się o zharmonizowaną w skali europejskiej „podstawową aranżację" kanałów 2x30 MHz w zakresach 703- 733 MHz (FDD - Frequency Division Duplex łącze „w górę") oraz 758–788 MHz (FDD - Frequency Division Duplex łącze „w dół"). W myśl Decyzji harmonizacyjnej ww. zakresy pasma 700 MHz powinny być użytkowane do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w oparciu o zharmonizowaną aranżację kanałów (jako tzw. „aranżacja podstawowa") oraz powiązane wspólne najmniej restrykcyjne warunki techniczne, jeżeli państwa członkowskie wyznaczą je do użytkowania w zastosowaniach innych niż przez sieci radiodyfuzyjne o dużej mocy.

Niemniej jednak państwa członkowskie UE mają swobodę decyzji w zakresie użytkowania części pasma częstotliwości 700 MHz w celu zaspokojenia szczególnych potrzeb krajowych. Oprócz naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej powyższe obejmuje również użytkowanie zgodnie z priorytetami sektorowymi unijnej polityki widma radiowego, w szczególności na potrzeby Programme Making and Special Events (PMSE, bezprzewodowe urządzenia do transmisji sygnałów akustycznych), Public Protection and Disaster Relief (PPDR, łączność radiowa na potrzeby ochrony publicznej i pomocy w przypadku klęsk żywiołowych) i Internet of Things (IoT, Internet Rzeczy)) i w celu zapewnienia efektywnego użytkowania widma.

Nowy art. 76s

Przepis ustawy zobowiązuje Prezesa UKE do przydzielenia, w drodze decyzji administracyjnej, OSSB określonego zakresu częstotliwości, przeznaczonego do użytkowania rządowego. Do decyzji Prezesa UKE odpowiednio należy stosować przepisy ustawy Prawo komunikacji elektronicznej dotyczące rezerwacji częstotliwości, regulujące między innymi okres, na który jest ona wydawana oraz jej treść. Jednocześnie w decyzji tej Prezes UKE obligatoryjnie określi zobowiązania pokryciowe, czyli nałożone na OSSB wymogi w zakresie pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o te częstotliwości.

Decyzja harmonizacyjna w tym kontekście wyraźnie wskazuje, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa PPDR, należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji

podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.

Nowy art. 76t

Przepis reguluje kwestię zmiany podmiotu, któremu przydzielono częstotliwości rządowe z zakresu 703–713 MHz oraz 758–768 MHz w przypadku odwołania lub zmiany podmiotu będącego OSSB. W takim przypadku nowy OSSB wstępuje w prawa i obowiązki związane z przydziałem tego zakresu częstotliwości określone w ustawie oraz decyzji Prezesa UKE. Takie rozwiązanie zapewni dalsze niezakłócone funkcjonowanie sieci i prawidłową realizację usług strategicznych.

2.1.21 Finansowanie strategicznej sieci bezpieczeństwa

Nowy art. 76u.

Utworzenie, utrzymanie, rozwój i modernizacja infrastruktury strategicznej sieci bezpieczeństwa będą finansowane w formie dotacji celowej udzielanej operatorowi strategicznej sieci bezpieczeństwa przez ministra właściwego do spraw aktywów państwowych z części budżetu państwa, której jest dysponentem. Podstawą określenia wysokości dotacji będzie koszt realizacji poszczególnych zadań ustalony przez ministra właściwego do spraw aktywów państwowych. Łączna kwota dotacji zostanie oszacowana na podstawie przedstawionych przez operatora strategicznej sieci bezpieczeństwa danych dotyczących kosztu realizacji poszczególnych zadań z uwzględnieniem liczby zrealizowanych zadań. Szczegółowe warunki wypłaty środków, wysokość kwot przeznaczonych na realizację poszczególnych zadań, a także sposób i zasady rozliczeń będzie określała umowa zawarta pomiędzy tym ministrem a OSSB.

Jednocześnie ze środków tej dotacji Operator strategicznej sieci bezpieczeństwa nie będzie mógł finansować swojej działalności gospodarczej. Przepis ten zapewnia, że środki z dotacji zostaną wyłącznie spożytkowane na cele publiczne.

2.1.22 Zmiany w art. 93

Artykuł 93 ustawy o KSC zawiera maksymalny limit wydatków z budżetu państwa dla poszczególnych części budżetowych, będących skutkiem finansowym wejścia w życie ustawy o KSC. Przepis ust. 8 oraz ust. 23 zawierają limity dla części budżetowej dla Komisji Nadzoru Finansowego. Część ta już nie istnieje – Urząd Komisji Nadzoru Finansowego jest obecnie państwową osobą prawną, a zasady jego finansowania określa rozdział 3 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[71)]. Z tego powodu uchyla się przepisy art. 93 ust. 8 i 23 jako zbędne.

[71] Dz. U. z 2023 r. poz. 753 i 825

2.1.23 Zmiany w załącznikach do ustawy

W sektorze ochrona zdrowia obecnie za operatora usługi kluczowej może zostać uznana jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia. Zmiana załącznika polegałaby na zastąpieniu wyrażenia „Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia" na „Jednostka podległa ministrowi właściwemu do spraw zdrowia lub przez niego nadzorowana". Za operatora usługi kluczowej mogłaby być uznana każda jednostka podległa lub nadzorowana przez ministra właściwego do spraw zdrowia, która np. zarządza danymi epidemiologicznymi.

Ponadto w załączniku numer 1 w kolumnie „Rodzaj podmiotów" dotyczącej sektora „Ochrona zdrowia" usunięto:

- „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301 oraz z 2023 r. poz. 605 i 650)."
- „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne."

Podmioty lecznicze, w przedsiębiorstwie których funkcjonują dział farmacji szpitalnej lub apteka szpitalna są faktycznie tożsame z podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. Brak jest jakiegokolwiek uzasadnienia dla istnienia wyodrębnienia takich podmiotów, ponieważ podmioty posiadające dział farmacji lub aptekę szpitalną są podmiotami leczniczymi, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.

W tym samym załączniku nr 1 w kolumnie „Rodzaj podmiotów" odnoszącej się do sektora Infrastruktury cyfrowej dodano nowy podmiot, jakim jest operator strategicznej sieci bezpieczeństwa.

2.2 Zmiany w innych ustawach

Zgodnie z art. 10 w ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzaniu mieniem państwowym w art. 13 ust. 1 dodaje się pkt 31 w brzmieniu: „podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa". Ta zmiana jest konsekwencją wprowadzenia do polskiego porządku prawnego operatora strategicznej sieci bezpieczeństwa, który nie powinien zbywać akcji lub praw z akcji należących do Skarbu Państwa.

Wprowadza się również zmianę w art. 226 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych. Artykuł ten reguluje sytuacje, w którym zamawiający odrzuca ofertę złożoną w ramach postępowania o zamówienie publiczne. Kolejną przesłanką odrzucenia oferty będzie sytuacja, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i poz. …) oraz usługę ICT lub proces ICT, określone w tej decyzji.

2.3 Pozostałe przepisy przejściowe i dostosowujące

Art. 4

Celem art. 4 jest uregulowanie kwestii rozstrzygnięcia postępowań wszczętych o udzielenie zamówienia publicznego. Przepis przejściowy wprost rozstrzyga o stosowaniu do tych postępowań ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych w brzmieniu nadanym niniejszą ustawą, jeżeli zostały one wszczęte przed dniem wejścia w życie niniejszej ustawy, a jednocześnie nie zakończyły się wyborem wykonawcy albo unieważnieniem postępowania przed dniem opublikowania informacji o wydaniu decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, przy czym relewantną datą jest data publikacji w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 5

Artykuł ten reguluje funkcjonowanie niektórych umów w związku ze zmianami jakie zostały wprowadzone do art. 33 ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto wskazuje, że dotychczasowe porozumienia dot. korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ustawy o ksc zachowują ważność.

Art. 6

Art. 6 reguluje kwestię utrzymania w mocy aktów wykonawczych do ustawy o krajowym systemie cyberbezpieczeństwa. Jest to niezbędne dla zapewnienia ciągłości działania w ramach krajowego systemu cyberbezpieczeństwa.

Utrzymane w mocy zostaną następujące rozporządzenia:

- Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w *sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej*[72)] - do czasu wydania rozporządzenia z art. 10 ust. 5 znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy;

[72)] Dz. U. z 2018 r. poz. 2080.

- Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w *sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa*[73)] - do czasu wydania rozporządzenia z art. 66 ust. 9 znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 7

Zgodnie z tym artykułem operator usługi kluczowej wyznaczy 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 14 dni od dnia wejścia w życie ustawy. Ponadto wskazuje się, że do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Po dniu wydania komunikatu operator usługi kluczowej będzie zgłaszał incydenty do CSIRT sektorowego.

Art. 8

Zgodnie z tym przepisem z dniem wejścia w życie ustawy:

1) dotychczas powołane w ramach operatora usługi kluczowej wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo stają się SOC wewnętrznymi;

2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC zewnętrzne.

Art. 9

Przepis ten stanowi, że przedsiębiorca komunikacji elektronicznej zgłasza incydenty telekomunikacyjne do CSIRT poziomu krajowego do czasu ogłoszenia komunikatu o osiągnięciu zdolności operacyjnej przez CSIRT Telco.

Art. 10

Przepis ten zobowiązuje CSIRT poziomu krajowego do dostosowania porozumień ws. przeniesienia właściwości CSIRT do zmian w art. 26.

Art. 11

Podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 3 miesięcy od dnia wejścia w życie ustawy.

[73)] Dz. U. z 2018 r. poz. 1952.

Art. 12

Zgodnie z tym przepisem Pełnomocnik Rządu do spraw Cyberbezpieczeństwa oraz Przewodniczący Kolegium będą mogli złożyć zlecić badanie sprzętu lub oprogramowania, o którym mowa w art. 33 nie wcześniej niż 3 miesiące od wejścia w życie ustawy.

Art. 13

CSIRT Telco nie będzie brał udziału w uzgodnieniach sposobu zgłaszania incydentów telekomunikacyjnych do czasu wydania komunikatu o zdolności operacyjnej.

Art. 14

Art. 14 reguluje moment zgłaszania incydentów przez jednostki podległe MSZ do CSIRT INT.

Art. 15

Przewidziano termin 18 miesięcy od dnia wejścia w życie ustawy na powołanie przez organy właściwe do spraw cyberbezpieczeństwa CSIRT sektorowych.

Powyższy przepis przejściowy jest niezbędny na przeprowadzenie organizacji tych zespołów, w tym na zapewnienie środków w nowej ustawie budżetowej, jak również przygotowanie niezbędnych składników materialnych i pozyskanie wysoko kwalifikowanej kadry ekspertów.

Gdy CSIRT sektorowy zostanie utworzony, organ właściwy do spraw cyberbezpieczeństwa ogłosi komunikat o osiągnięciu przez CSIRT zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 16

Artykuł ten reguluje kwestie dot. pierwszego sprawozdania organu właściwego do spraw cyberbezpieczeństwa z działalności CSIRT sektorowego.

Art. 17

Zgodnie z tym artykułem dotychczas powołany sektorowy zespół cyberbezpieczeństwa (CSIRT KNF) staje się CSIRT sektorowym.

Art. 18-19

Przepisy te zawierają analogiczne regulacje dostosowujące co do utworzenia CSIRT Telco jak przy CSIRT sektorowym

Art. 20

Zgodnie z przepisem art. 20 Prezes Rady Ministrów wyznaczy OSSB w terminie do 30 dni od wejścia w życie ustawy. Termin zawarty w tym przepisie ma charakter instrukcyjny. Ponadto wskazuje, że Prezes Rady Ministrów podaje do publicznej wiadomości informacje o osiągnięciu pełnej zdolności operacyjnej do

świadczenia usług przez Operatora strategicznej sieci bezpieczeństwa. Pozwoli to precyzyjnie ustalić moment od kiedy podmioty wskazane w art. 76g ust. 2 mają obowiązek zawarcia umowy z OSSB.

Art. 21

Przepis określa maksymalne limity wydatków dla poszczególnych części budżetu państwa w związku z wejściem w życie niniejszej ustawy.

Art. 22

Ustawa wejdzie w życie w terminie 6 miesięcy od dnia ogłoszenia. Ze względu na związki treściowe niniejsza ustawa powinna wejść w życie w tym samym dniu co ustawa – Prawo komunikacji elektronicznej.

3 Pozostałe informacje

Wpływ projektu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 4 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa[74)] projekt został zamieszczony w wykazie prac legislacyjnych.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa oraz uchwałą nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów[75)] projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Projektowana regulacja nie podlega notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych[76)], które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, zwanej dalej „dyrektywą 2015/1535". Wiele przepisów zawartych w tym projekcie stanowi implementację prawa Unii

---

[74)] Dz. U. z 2017 r. poz. 248.

[75)] Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów M.P. z 2022 r. poz. 348.

[76)] Dz. U. poz. 2039 oraz z 2004 r. poz. 597.

Europejskiej. Ponadto wskazać należy, że dyrektywa 2015/1535 w art. 1 ust. 3 wprost wskazuje, że nie ma zastosowania do zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych. Taki charakter mają przepisy rozdziału 4a dotyczące telekomunikacji, które stanowią implementację art. 40 i 41 Europejskiego Kodeksu Łączności Elektronicznej[77]. Projektowane przepisy art. 66a i art. 66b ustawy o krajowym systemie cyberbezpieczeństwa mają na celu wdrożenie postanowień Unijnego zestawu narzędzi cyberbezpieczeństwa sieci 5G tzw. Toolbox 5G[78]. W swoim komunikacie z dnia 15 czerwca 2023 r. C (2023) 4049[79] dotyczącym wdrożenia Toolbox 5G Komisja Europejska wskazała, że wdrożenie Toolbox 5G mieści się w ramach wdrożenia art. 40 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Zgodnie ze wspomnianym przepisem art. 40 EKŁE państwa członkowskie zapewniają, aby dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowali właściwe i proporcjonalne środki techniczne i organizacyjne, które to środki mają zapewniać poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Wycofanie sprzętu lub oprogramowania od dostawcy wysokiego ryzyka jest środkiem mitygującym ryzyko związane z wykorzystywaniem tego sprzętu lub oprogramowania przez przedsiębiorców telekomunikacyjnych. W konsekwencji należy uznać, że proponowane art. 66a i art. 66b wdrażają zarówno Toolbox 5G jak i art. 40 dyrektywy 2018/1972. Dzięki temu korzystają ze zwolnienia, o którym mowa w art. 1 ust. 3 dyrektywy 2015/1535.

Z kolei przepisy rozdziału 11a, tworzące krajowy system certyfikacji cyberbezpieczeństwa, służą wykonaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[80]. Przepisy te korzystają ze zwolnienia z obowiązku notyfikacji, o którym mowa w art. 7 ust. 1 lit. a dyrektywy 2015/1535.

[77] Dz. Urz. UE L 321/36 z 17.12.2018, str. 1.

[78] Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, Cooperation Group on Network and Information Security, https://digital-strategy.ec.europa.eu/en/library/cybersecurity- 5g-networks-eu-toolbox-risk-mitigating-measures.

[79] https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5gcybersecurity-toolbox.

[80] Dz. Urz. L 151/15 z 7.6.2019, str. 15.

Nazwa projektu

Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

Ministerstwo wiodące i ministerstwa współpracujące

Ministerstwo Cyfryzacji

Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu

Janusz Cieszyński, Minister Cyfryzacji

Kontakt do opiekuna merytorycznego projektu

Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa,

Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa,

e-mail: Sekretariat.DC@cyfra.gov.pl

Data sporządzenia

07.06.2023

Źródło: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15)

Nr w wykazie prac legislacyjnych i programowych Rady Ministrów

UD68

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Doświadczenia z funkcjonowania krajowego systemu cyberbezpieczeństwa

Lata doświadczeń na poziomie krajowym (od 2018 r. – wejście w życie ustawy o KSC) pozwoliły ocenić skuteczność wdrożonych rozwiązań prawno-organizacyjnych oraz zidentyfikować obszary wymagające zmian ustawowych, które usprawniają funkcjonowanie systemu cyberbezpieczeństwa, m.in. konieczność ujednolicenia na poziomie krajowym procedur zgłaszania incydentów, przyspieszenie tworzenia sektorowych zespołów cyberbezpieczeństwa, czy umożliwienie włączenia centrów wymiany informacji i analiz (ISAC) do krajowego systemu cyberbezpieczeństwa.

Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były powoływane. Dotychczas powstał tylko jeden sektorowy CSIRT - w sektorze finansowym – CSIRT-KNF.

Ponadto, wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo (a także podmioty świadczące usługi z zakresu cyberbezpieczeństwa) nie współpracują ze sobą, co skutkuje brakiem przepływu istotnych informacji między podmiotami systemu. Operatorzy usług kluczowych mają trudności ze spełnieniem wyśrubowanych wymogów technicznych dla wewnętrznych struktur cyberbezpieczeństwa.

Do tej pory powstały w Polsce tylko 4 centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa, m.in. ISAC-Kolej, które rozpoczęło działalność w październiku 2020 r. ISAC (Information Sharing and Analysis Center, centrum wymiany informacji i analiz) gromadzi informacje o podatnościach i cyberzagrożeniach. Taka formuła znacząco wpływa na poprawę cyberbezpieczeństwa. Wskazane jest, aby więcej takich organizacji powstało w Polsce.

Zauważono również, że uprawnienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa są niewystarczające w stosunku do zadań, które musi wypełniać. Brakuje mu skutecznych środków oddziaływania na podmioty krajowego systemu cyberbezpieczeństwa, w tym przede wszystkim możliwości wydawania ostrzeżeń w sytuacji prawdopodobnego wystąpienia incydentu krytycznego. Chodzi o podobny instrument jaki jest m.in. w Czechach, czyli ostrzeżenie szefa agencji NUKIB.

Brakuje również środka prawnego, który umożliwiałby wydawanie rekomendacji o charakterze technicznym (w tym zakresie - Narodowych Standardów Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa RP na lata 2019-2024) i jednocześnie obowiązku uwzględnienia tych rekomendacji przez podmioty krajowego systemu cyberbezpieczeństwa w trakcie procesu zarządzania ryzykiem.

Zmiany na poziomie UE

Ponadto, w tym samym okresie doszło do istotnych zmian w prawie europejskim. Jednym z priorytetów Komisji Europejskiej stało się zapewnienie cyberbezpieczeństwa sieciom telekomunikacyjnym. Weszła w życie nowa regulacja – dyrektywa Europejski Kodeks Łączności Elektronicznej (EKŁE), który umożliwia (w odróżnieniu od poprzedniej regulacji tzw. dyrektywy ramowej) uspójnienie procedury zgłaszania i reagowania na incydenty i incydenty telekomunikacyjne na poziomie krajowym. Obecnie przedsiębiorcy telekomunikacyjni nie są obowiązani zgłaszać incydenty do jednego z zespołów CSIRT poziomu krajowego.

EKŁE nie jest jedynym symbolem zmian w postrzeganiu przez Komisję Europejską bezpieczeństwa w sektorze telekomunikacyjnym. Komisja wielokrotnie m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanego jako 5G Toolbox[1)]. Zestaw obejmuje zarówno narzędzia o charakterze strategicznym i technicznym, jak i te o charakterze wspierającym. Cele są dwa: po pierwsze, bezpieczeństwo sieci 5G, a po drugie: uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox zawiera także definicje zestawu środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą kręgosłupem Jednolitego Rynku Cyfrowego UE. Wyróżnione są środki o charakterze:

- strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym ocena bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
- technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT GOV, CSIRT MON, CSIRT NASK – wynikające z art. 33 ustawy o KSC,
- wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa

Krajowy System Certyfikacji Cyberbezpieczeństwa

Projektowana ustawa pozwala dostosować polski porządek prawny do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013, zwanego dalej aktem o cyberbezpieczeństwie. Stanowi również realizację celu 2. Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Rola sieci i systemów teleinformatycznych wzrosła niepomiernie w ostatnich latach, sprawiając, że stały się one niezbędnym elementem współczesnej gospodarki. W związku z pandemią COVID-19 proces ten postępuje coraz szybciej. Jako że społeczeństwa coraz bardziej będą polegały na produktach i usługach funkcjonujących w cyberprzestrzeni, tym istotniejsze staje się zapewnienie bezpieczeństwa działań podejmowanych w tej płaszczyźnie. Wprowadzenie jednolitych zasad przyznawania certyfikatów cyberbezpieczeństwa i ich wzajemne uznawanie w państwach Unii Europejskiej zapewnią, że przedsiębiorstwa będą w stanie lepiej zabezpieczyć swoje interesy w cyberprzestrzeni. Ponadto, wzajemne uznawanie certyfikatów zapewni im lepszą pozycję w konkurencji na rynku europejskim. Działania te przyczynią się do ogólnego wzrostu bezpieczeństwa w cyberprzestrzeni. Posłużą też uporządkowaniu rynku w tym zakresie oraz objęciu procesów certyfikacji nadzorem. Wyraźne wsparcie państwa w zakresie certyfikacji powinno również przyczynić się do zwiększenia świadomości społecznej w kwestii cyberbezpieczeństwa.

Przyjęcie proponowanych przepisów może dać polskim przedsiębiorcom dużą szansę na pozyskanie zainteresowanych certyfikacją swoich produktów klientów z sąsiednich krajów. Będzie to więc szansą na znaczne poszerzenie bazy potencjalnych klientów.

Sama certyfikacja w zakresie cyberbezpieczeństwa jest procesem czasochłonnym i kosztownym, co ogranicza dostępność do certyfikatów. Wprowadzenie krajowego systemu certyfikacji powinno przyczynić się do zmiany tego stanu rzeczy.

Przyjęte w ustawie rozwiązania umożliwiają również tworzenie krajowych programów certyfikacyjnych. Dzięki temu możliwe będzie zwiększenie cyberbezpieczeństwa w obszarach uznanych za kluczowe.

Dzięki przepisom umożliwiającym tworzenie krajowych programów certyfikacji cyberbezpieczeństwa administracja publiczna uzyska skuteczne narzędzie pozwalające reagować na cyberzagrożenia związane z konkretnymi produktami, usługami czy procesami. Możliwe będzie opracowanie programu certyfikacji, który weźmie te zagrożenia pod uwagę bez konieczności oczekiwania na działania na forum Unii Europejskiej.

Rewolucja informatyczna i rozwój sieci komputerowych spowodowały istotne uzależnienie działania państwa od sprawnych, bezpiecznych systemów teleinformatycznych i sieci telekomunikacyjnych. Bezpieczne systemy łączności strategicznej, spajającej działania administracji publicznej w sferze związanej z obronnością, bezpieczeństwem państwa, czy bezpieczeństwem i porządkiem publicznym i zapewniające sprawne działanie ePaństwa są niezwykle ważnym elementem dobrze funkcjonującego

[1)] *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

państwa. Dlatego istnieje potrzeba utworzenia w Polsce takiej sieci, będącej bezpieczną i niezawodną siecią telekomunikacyjną wykorzystywaną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Oczekiwany efekt wprowadzenia ww. narzędzi interwencji:

- Przebudowany zostanie model współpracy w ramach krajowego systemu cyberbezpieczeństwa. Sektorowe zespoły cyberbezpieczeństwa i podmioty świadczące usługi z zakresu cyberbezpieczeństwa zostaną zastąpione odpowiednio przez CSIRT sektorowe i SOC zewnętrzne (operacyjne centra bezpieczeństwa) z nieco tylko zmienionymi zadaniami Wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo staną się SOC wewnętrznymi.
- Do krajowego systemu cyberbezpieczeństwa zostaną dodani przedsiębiorcy komunikacji elektronicznej.
- Do krajowego systemu cyberbezpieczeństwa zostaną włączone ISAC wpisane do wykazu prowadzonego przez ministra właściwego do spraw informatyzacji – będące centrami wymiany informacji m.in. o podatnościach i zagrożeniach, ułatwiającymi dostęp do takich informacji zainteresowanym podmiotom.
- Zostanie wzmocniona pozycja Pełnomocnika poprzez wyposażenie go w konkretne uprawnienia w zakresie wydawania ostrzeżeń o incydentach krytycznych wraz z zalecaniem określonych zachowań. Pełnomocnik będzie mógł również wydawać rekomendacje mające na celu wzmocnienie poziomu cyberbezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa.
- Dostawcy sprzętu i oprogramowania będą mogli zostać poddani procedurze sprawdzającej pod kątem zagrożenia jakie może wywołać wykorzystywanie oferowanego przez nich konkretnego sprzętu lub oprogramowanie w kluczowych podmiotach polskiej gospodarki. Podmioty obowiązane, które będą objęte zakresem przedmiotowym oceny, będą musiały wycofać z użytkowania dany sprzęt lub oprogramowanie w ciągu 7 lat od wydania decyzji administracyjnej przez ministra właściwego ds. informatyzacji.
- Powstanie Krajowy System Certyfikacji Cyberbezpieczeństwa, w ramach którego wydawane będą certyfikaty w zakresie cyberbezpieczeństwa.
- Minister właściwy do spraw informatyzacji będzie przygotowywać programy, na podstawie których będzie można przeprowadzać certyfikacje. Programy te będą ostatecznie przyjmowane w drodze rozporządzenia Rady Ministrów.
- Organ nadzorczy będzie przeprowadzał kontrolę w podmiotach należących do krajowego systemu certyfikacji cyberbezpieczeństwa. W zakresie certyfikatów odwołujących się do poziomu zaufania „wysoki" będzie również zatwierdzał każdy wydany certyfikat. Rozwiązanie to jest gwarantuje, że ocena zgodności na najwyższy poziom bezpieczeństwa będzie przeprowadzana zgodnie z najlepszymi standardami w tej dziedzinie.
- Określone zostaną procedury akredytacji jednostek oceniających zgodność oraz procedury wydawania certyfikatów.
- Określone zostaną obowiązki spoczywające na podmiotach krajowego systemu certyfikacji cyberbezpieczeństwa.
- Zostanie uruchomiona bezpieczna sieć telekomunikacyjna wykorzystywana na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego przez kluczowe urzędy i podmioty działające w Rzeczypospolitej Polskiej. W tym celu Prezes Rady Ministrów wyznaczy operatora strategicznej sieci bezpieczeństwa

  Operator ten będzie świadczył usługi telekomunikacyjne, jak również inne usługi dla wskazanych w ustawie podmiotów.

  Przyjęcie takiego rozwiązania zapewni sprawną i zoptymalizowaną kosztowo budowę infrastruktury telekomunikacyjnej, wykorzystywanej na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Ponadto, skupienie realizacji szczególnie istotnych projektów w jednym miejscu przyczyni się do optymalizacji nakładów ponoszonych na nie przez Skarb Państwa oraz skrócenia czasu realizacji poszczególnych projektów.

Projekt ustawy służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy Strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

Jednocześnie wprowadzenie w życie projektowanych zmian w ustawie o krajowym systemie cyberbezpieczeństwa zrealizuje kamień milowy reformy C3.1. Krajowego Planu Odbudowy i Zwiększania Odporności. Zgodnie z tym wymogiem wprowadzone zostaną ramy prawne umożliwiające tworzenie sektorowych sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), tworzenie Centrów Wymiany i Analizy Informacji (ISAC) oraz wzmocni mechanizmy współpracy administracji rządowej z jednostkami samorządu terytorialnego w zakresie reagowania na incydenty bezpieczeństwa.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Projektodawca przy projektowaniu przepisów prawa dotyczących uznania dostawców sprzętu lub oprogramowania za dostawców wysokiego ryzyka – czyli wdrożenia zaleceń z tzw. 5G Toolbox, dokonał analizy porównawczej rozwiązań prawno-organizacyjnych zaimplementowanych lub zaproponowanych mechanizmów. Wyniki analizy zostały zaprezentowane w załączniku do OSR *Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie*.

W większości państw Unii Europejskiej wprowadzone zostały przepisy umożliwiające wyłączenie z budowy sieci 5G dostawcy uznanego za potencjalne zagrożenie dla bezpieczeństwa narodowego. Obowiązujące regulacje przewidują dokonanie takiego wyłączenia w drodze władczego rozstrzygnięcia dokonywanego przez jeden z organów władzy wykonawczej np. w drodze decyzji administracyjnej. W wielu państwach w tego rodzaju postępowaniach istotną rolę odgrywa również organ doradczy składający się z przedstawicieli administracji, wojska oraz służb specjalnych.

Analiza w zakresie środków reagowania na incydenty krytyczne

Czechy

Czeska agencja ds. cyberbezpieczeństwa NUKIB na podstawie sekcji 12 (1) ustawy o cyberbezpieczeństwie[2)], może wydawać ostrzeżenia do podmiotów. Ostrzeżenia wydawane są w przypadku wysokiego prawdopodobieństwa wystąpienia sytuacji kryzysowej, która może mieć krytyczne znaczenie dla bezpieczeństwa państwa. Ostrzeżenie zawiera także listę rekomendowanych działań, które podmioty powinny wdrożyć celem ograniczenia ryzyk związanych z sytuacją kryzysową. Przykłady rekomendacji: zwrócenie uwagi na określony typ cyberataków np. spear-phishingów, potrzebie zablokowania dostępu do swojej infrastruktury IT, pilnej konieczności dokonania aktualizacji oprogramowania, czy też zwrócenie szczególnej uwagi na wskazane w ostrzeżeniu domeny. Przykładem takiego ostrzeżenia jest dokument wydany 16 kwietnia 2020 r. znak 2066/2020-NÚKIB-E/350, na podstawie analizy możliwych zagrożeń wydał ostrzeżenie dla całego państwa, ze szczególnym naciskiem na sektor ochrony zdrowia[3)]. Innym przykładem jest ostrzeżenie NUKIB z 25 lutego 2022 r. znak 2384/2022-NÚKIB-E/350 wskazujące na cyberzagrożenia o charakterze krytycznym, których wystąpienie w systemach czeskiej administracji publicznej czy innych organizacji strategicznych jest bardzo prawdopodobne[4)].

Niemcy

Niemiecki Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für. Sicherheit in der Informationstechnik – BSI) może, na podstawie § 7 BSI-Gesetz[5)] ogłaszać ostrzeżenia o

- podatnościach w produktach i usługach informatycznych,
- złośliwym oprogramowaniu,
- utracie lub nieautoryzowanym dostępie do danych

a także zalecać środki bezpieczeństwa.

Włochy

[2)] Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) https://www.zakonyprolidi.cz/cs/2014-181.

[3)] https://www.nukib.cz/download/publications_en/Warning-NUKIB-2020-04-16.pdf.

[4)] https://nukib.cz/download/aktuality/2021-01-17_varovani_v.1.7_EN.pdf.

[5)] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik https://www.gesetze-im-internet.de/bsig_2009/BJNR282110009.html.

We Włoszech dekret nr 105 z 21 września 2019 r.[6)] uprawnia Prezesa Rady Ministrów do nakazania całkowitego lub częściowego wycofania z eksploatacji jednego lub więcej urządzeń lub produktów, w sytuacji poważnego i bezpośredniego zagrożenia bezpieczeństwa narodowego związanego z podatnościami występującymi w sieciach, systemach i usługach. Środek ten może być stosowany, jeżeli zagrożenia nie można uniknąć w inny sposób i tylko przez czas ściśle niezbędny do wyeliminowania lub ograniczenia konkretnego ryzyka.

Certyfikacja cyberbezpieczeństwa

Projektodawca w kontekście zmian prawa w obszarze certyfikacji cyberbezpieczeństwa dokonał analizy rozwiązań przyjętych w następujących państwach:

Francja

W ramach Francuskiej Agencji Cyberbezpieczeństwa (The National Cybersecurity Agency of France, zwana dalej „ANSSI") kwestiami certyfikacji zajmuje się Narodowe Centrum Certyfikacji. Agencja ta zajmuje się również licencjonowaniem laboratoriów w tym zakresie. ANSSI zostało również wyznaczone jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z Aktem o cyberbezpieczeństwie

Sama certyfikacja czy licencjonowanie nie podlega opłatom. Osoby wnioskujące ponoszą koszty badań laboratoryjnych ich produktów. Wynoszą one zwykle 600-700 euro na dzień, a sama certyfikacja trwa ok. 25-35 dni. Podmioty obsługiwane są w kolejności złożenia wniosków co często powoduje, iż zainteresowani muszą czekać na otrzymanie usługi. Certyfikacji można dokonać również u autoryzowanych podmiotów działających na wolnym rynku.

System francuski zasadniczo różni się od przyjętego w niniejszej ustawie. Wynika to przede wszystkim z uwarunkowań instytucjonalnych.

Niemcy

Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) wykonuje zadania niezwykle zbliżone do tych wynikających z implentowanego rozporządzenia jak również posiada zadania wykonywane w Polsce przez Agencję Bezpieczeństwa Wewnętrznego. Został on również wyznaczony jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z aktem o cyberbezpieczeństwie. BSI przygotowuje również krajowe programy certyfikacyjne takie jak niemiecki szybki program certyfikacji.

Szwecja

Kwestiami certyfikacji w Szwecji zajmuje się jedna z agencji rządowych - Swedish Defence Materiel Administration. Pobierana są liczne opłaty. Sam wniosek o certyfikację podlega bezzwrotnej opłacie, w wysokości 20 000 koron. Agencja ta zajmuje się również zamówieniami dla szwedzkich sił zbrojnych oraz rozwojem technologii na potrzeby wojska.

To sprzężenie kwestii cyberbezpieczeństwa w wymiarze cywilnym i wojskowym stanowi zasadniczą różnicę między polskim a szwedzkim systemem w tym zakresie.

Włochy

Przyjęty we Włoszech model certyfikacji oparty jest na działaniach organów administracji publicznej. Certyfikaty wydawane są przez odpowiednią komórkę w Ministerstwie Rozwoju Gospodarczego. W związku z tym, ten rodzaj działalności organów administracji publicznej jest finansowany w całości z budżetu państwa. Równocześnie podmioty ubiegające się o certyfikat nie muszą wnosić opłat w związku z jego wydaniem.

Cypr

W celu wdrożenia Aktu o cyberbezpieczeństwie powołany został nowy organ, który ma pełnić rolę krajowego organu ds. certyfikacji cyberbezpieczeństwa.

[6)] Decreto-legge 21 settembre 2019, n. 105 Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica. https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg.

Analiza w zakresie operatora strategicznej sieci bezpieczeństwa

W analizowanych krajach (Austria, Belgia, Finlandia, Francja, Niemcy, Węgry) udział wyspecjalizowanych jednostek państwowych lub operatorów państwowych w zarządzaniu sieciami w warstwie bezpieczeństwa oraz w warstwie aplikacyjnej jest 100-procentowy. Podmioty te są nadzorowane albo przez ministrów bezpieczeństwa wewnętrznego (Belgia, Austria, Niemcy, Węgry) albo przez jednostki międzyresortowe podległe bezpośrednio premierowi (Finlandia, Francja).

Warstwa szkieletowa i dystrybucyjna sieci krytycznych może być bezpośrednio lub pośrednio własnością państwa (Finlandia, Węgry, częściowo Francja i Belgia) lub może być dzierżawiona w formie usług transmisji danych lub ciemnych włókien od kwalifikowanych operatorów komercyjnych (pozostałe analizowane kraje). Dostawcy ci są na ogół wybierani w postępowaniach zamkniętych, na podstawie specjalnych dekretów (ustaw) bądź w trybie negocjacji. Podobnie nabywane są usługi integracyjne i usługi wsparcia technicznego (maintenance sieci). Ustawy dające podstawę prawną dla pomięcia trybów konkurencyjnych powołują się artykuł 296 Traktatu UE, który zezwala krajom członkowskim na samodzielne kształtowanie polityki zakupowej w sprawach dotyczących obronności kraju.

Poniżej zostały opisane przykłady rozwiązań z zakresu zarządzania strategicznymi, z punktu widzenia państwa, sieciami teleinformatycznymi i zadaniami z zakresu telekomunikacji w trzech państwa Unii Europejskiej: Finlandii, Francji i na Węgrzech.

Finlandia

W maju 1998 r. w Finlandii uruchomiono pierwszą na świecie ogólnokrajową sieć bezpieczeństwa publicznego wykorzystującą standard TETRA. Jest ona obecnie częścią zintegrowanej sieci łączności kryzysowej VIRVE. Sieć jest w całości własnością państwa, właścicielem jest istniejąca od 1992 r. grupa państwowych spółek Suomen Erillisverkot Oy (Grupa Sieci Bezpieczeństwa Państwa).

Formalnie Suomen Erillisverkot podlega bezpośrednio Kancelarii Prezesa Rady Ministrów – obecnie na podstawie Rozporządzenia Rady Ministrów o polityce własności państwowej z 2011 r. oraz ustawy o bezpiecznych sieciach administracji państwowej nr 10/2015 20.

Ustawa 10/2015 zawiera bezpośrednie umocowanie Suomen Erillisverkot lub jej spółek zależnych jako dostawców infrastruktury i usług sieciowych bezpiecznych sieci administracji państwowej. Użytkownikami uprawnionymi do bezpłatnego korzystania z usług VIRVE są policja, straż pożarna, ratownictwo medyczne, siły zbrojne (dysponujące też własną infrastrukturą łączności). Należąca do grupy Suomen Erillisverkot spółka Suomen Turvallisuusverkko dostarcza usługi bezpiecznej transmisji danych dla całej administracji centralnej, a także usługi kolokacyjne oraz zarządzane usługi telekomunikacyjne.

Francja

We Francji jednym z głównych organów wykonawczych w zakresie ochrony infrastruktury krytycznej państwa (w szerszym kontekście obronności i bezpieczeństwa) jest Agencja Narodowa Bezpieczeństwa Systemów Informacji (fr. ANSSI – Agence nationale de la sécurité des systèmes d'information). ANSSI została powołana dekretem nr 2009-834 z 7 lipca 2009 r. Dekret ten definiuje zadania ANSSI w zakresie bezpieczeństwa informacji, zapewnienia bezpiecznej łączności pomiędzy ministerstwami (Artykuł 3, tiret drugi) oraz wsparcia dla wszystkich operatorów infrastruktury krytycznej państwa, a dekret z 11 lutego 2011 r. powierza ANSSI misję ochrony wszystkich krajowych sieci informatycznych.

Innym organem podległym premierowi (w kontekście informatycznej infrastruktury krytycznej) jest powołany dekretem z 30 października 2012 r. SGMAP (fr. Secrétariat général pour la modernisation de l'action publique), który jest między innymi właścicielem sieci RIE (fr. Le réseau interministériel de l'Etat), ekstranetu rządowego, której operatorem początkowo była komórka międzyministerialna DISIC, a następnie agencja DINSIC (fr. Direction interministérielle du numérique et du système d'information et de communication de l'État). Zadania DINSIC definiuje rozporządzenie premiera Francji z dnia 21 września 2015 r., które wskazuje między innymi zadanie operowania istniejącą już wówczas siecią RIE.

Jeśli chodzi o tryb zamawianych usług, to zgodnie z opublikowaną w 2013 r. Białą Księgą definiująca strategie bezpieczeństwa i obronności Francji, szczególnie istotne znaczenie mają kwestie bezpieczeństwa sieci komunikacji elektronicznej oraz tworzącego je sprzętu.

Efektem opublikowania Białej Księgi w 2013 r. było rozszerzenie katalogu usług, które mogą być nabywane z pominięciem trybu zamówień publicznych (ustawa NR. 2015- 899 z 23 lipca 2015r), która w art. 14, 16 definiuje explicite między innymi takie wyjątki:

- udostępnienie publicznych sieci telekomunikacyjnych (art. 14 pkt 15);
- usługi bezpiecznej poczty elektronicznej (art. 14 pkt 16 a)
- usługi, których realizacja wymaga zachowania poufności w interesie obronności kraju (art. 14 pkt 11).

Ponadto, ustawa ta przewiduje wyłączenia podmiotowe z prawa zamówień publicznych dla dostawców, którzy:

- są jednostkami budżetowymi, podlegającymi prawu zamówień publicznych (art. 14 pkt 1) lub

- są jednostkami podległymi, nad którymi zamawiający sprawuje kontrolę, pod warunkiem że jednostka podległa ponad 80% swej aktywności realizuje na rzecz jednostki nadrzędnej.

Z uprawnień tych korzysta między innymi ANSSI, której zadaniem jest realizacja polityki cyberbezpieczeństwa Francji poprzez operowanie rządową infrastrukturą telekomunikacyjną do łączności tajnej: ISIS. RIMBAUD i HORUS.

Ponadto, funkcjonuje we Francji Dekret nr 2004-16 z 7 stycznia 2004 r. Dekret ten ustanawia możliwość pominięcia trybów konkurencyjnych w przypadku pewnych typów zamówień związanych z obronnością. Na mocy zarządzenia ministra obrony określa się kryteria kwalifikowania usługodawców – przez odniesienie do norm lub w inny sposób. Dekret ten powołuje się na Art. 296 Traktatu UE, który daje krajom członkowskim swobodę decydowania w kwestii nabywania produktów i usług istotnych dla obronności kraju – o ile nie zaburza to konkurencji na szczeblu międzynarodowym (stosowano przepisy dekretu przy budowie sieci Rimbaud i przy projekcie ISIS).

Węgry

Na Węgrzech organem pełniącym szczególną rolę w powyższym systemie sieci jest NISz (węg. Nemzeti Infokommunikációs Szolgáltató Zrt.), państwowa spółka świadczącą usługi ICT dla administracji publicznej, należąca do skarbu państwa i podległa MSW. Finansowanie NISz zapewniane jest przez Ministerstwo Rozwoju Narodowego (węg. NFM – Nemzeti Fejlesztési Minisztérium). Korzystanie ze wszystkich omawianych sieci jest na Węgrzech bezpłatne dla uprawnionych służb (użytkowników końcowych). Organa właścicielskie lub zarządzające danymi służbami korzystają z usług sieci na podstawie umów z NISz i z tym organem rozliczają się za usługi, korzystając z własnych środków budżetowych. Szczegółowe regulacje dotyczące obecnej budowy, organizacji oraz działania infrastruktury łączności określono w rozporządzeniu RM 346/2010. (XII. 28.) o sieciach rządowej komunikacji elektronicznej (z późn. zm.).

NISz, na mocy ww. rozporządzenia, jest operatorem radiowego systemu EDR obsługującego policję, służby bezpieczeństwa wewnętrznego, służby celne i finansowe.

NISz razem z Ministerstwem Rozwoju Narodowego zarządza też siecią KözHáló, która ma dwa oddzielne segmenty Köznet (sieć dostępowa dla administracji i instytucji publicznych przeznaczona do ogólnych, niekrytycznych celów administracyjnych) oraz Sulinet (sieć dostępowa dla szkół).

NISz zarządza również, na podstawie ww. rozporządzenia, siecią szkieletową NTG, wykorzystywaną m. in. do transmisji danych i obsługi ruchu głosowego dla administracji publicznej.

Zadania NISz w dziedzinie teleinformatyki dla administracji centralnej wynikają z Rozporządzenia Rady Ministrów 309/2011. (XII. 23.) o centralnych usługach informatycznych i komunikacji elektronicznej. Zgodnie z załącznikiem nr 2 Rozporządzenia RM 309/2011 Rada Ministrów, Kancelaria Prezesa Rady Ministrów, MSW, Ministerstwo Zasobów Ludzkich, Ministerstwo Rolnictwa, Ministerstwo Sprawiedliwości, Ministerstwo Współpracy Gospodarczej z Zagranicą i Spraw Zagranicznych, Ministerstwo Gospodarki Narodowej, Ministerstwo Rozwoju Narodowego oraz podległa Ministerstwu Gospodarki Narodowej Naczelna Dyrekcja Zamówień Publicznych i Zaopatrzenia (KEF) obowiązane są korzystać z rozwiązań i usług teleinformatycznych opracowywanych i/lub dostarczanych przez NISz. NISz pełni też rolę urzędu certyfikującego dla usług zaufania i podpisu elektronicznego.

NISz jest również liderem lub członkiem konsorcjów realizujących programy operacyjne związane z tworzeniem i rozwojem usług elektronicznych dla administracji, przedsiębiorców i obywateli.

Konkluzja:

We wszystkich trzech omówionych wyżej krajach funkcjonują specjalne instytucje (we Francji agendy rządowe, w Finlandii i na Węgrzech - spółki), które zapewniają łączność przewodową i bezprzewodową oraz transmisję danych dla administracji publicznej. W każdym z omawianych krajów istnieją akty prawne, powierzające te zadania ww. instytucjom bądź wprost, bądź też przez szczególne wyłączenia ze stosowania przepisów dotyczących zamówień publicznych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	394	Wykaz OUK	Pozytywne. Operatorzy usług kluczowej, w wyniku utworzenia obowiązkowych już CSIRT sektorowych, otrzymają bezpośrednie

			wsparcie przy reagowaniu na incydenty. Będą zobowiązani do podłączenia się do systemu S46 od 1 stycznia 2024 r. Będą obowiązani do wycofania z użytkowania sprzętu lub oprogramowania, określonego w decyzji o uznaniu za dostawcę wysokiego ryzyka, w ciągu 7 lat od wydania tej decyzji. Obowiązek posiadania operacyjnego centrum bezpieczeństwa (SOC). Uproszczenie wymagań co do środków technicznych i organizacyjnych.
Dostawcy usług cyfrowych	53	Szacunki DC MC	Pozytywne. Będą obowiązani do wycofania z użytkowania sprzętu lub oprogramowania, określonego w decyzji o uznaniu za dostawcę wysokiego ryzyka, w ciągu 7 lat od wydania tej decyzji.
Podmioty publiczne	Ok. 4000	Szacunki własne	Pozytywne. Motywujące wszystkie podmioty publiczne – będą one musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Będą obowiązane do wycofania z użytkowania sprzętu lub oprogramowania, określonego w decyzji o uznaniu za dostawcę wysokiego ryzyka, w ciągu 7 lat od wydania tej decyzji.
Jednostki samorządu terytorialnego	16 województw 314 powiatów i 2 477 gmin	Dane MSWiA[7]	Pozytywne. Jednostki samorządu terytorialnego będą zobowiązane wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Jednostki samorządu terytorialnego będą obowiązane umożliwić operatorowi strategicznej sieci bezpieczeństwa umieszczenie na nieruchomości obiektów i urządzeń infrastruktury telekomunikacyjnej, w szczególności instalowanie urządzeń telekomunikacyjnych, przeprowadzanie linii kablowych pod nieruchomością, na niej lub nad nią, umieszczanie tabliczek informacyjnych o urządzeniach, a także ich eksploatację i konserwację, jeżeli nie uniemożliwi to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości.
Przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia	69	Dane UKE[8)]	Będą obowiązani do wycofania z użytkowania sprzętu lub oprogramowania, określonego w decyzji o uznaniu za dostawcę wysokiego ryzyka, w ciągu 5 lat od wydania tej decyzji.
Operatorzy infrastruktury krytycznej[9)]	128	OSR do projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw[10)]	Pozytywne. Operatorzy infrastruktury krytycznej będą odbiorcami wydawanych przez Pełnomocnika ostrzeżeń. Będą obowiązani do wycofania z użytkowania sprzętu lub oprogramowania, określonego w decyzji o uznaniu za dostawcę wysokiego ryzyka, w ciągu 7 lat od wydania tej decyzji.
Krajowe instytucje płatnicze	41	Rejestr krajowych instytucji płatniczych[11)]	Pozytywne. Krajowe instytucje płatnicze będą odbiorcami wydawanych przez Pełnomocnika ostrzeżeń.
Kwalifikowani dostawcy usług zaufania	5	Rejestr kwalifikowanych usług zaufania[12)]	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń.

[7)] https://www.gov.pl/web/mswia/baza-jst.

[8)] Sprawozdanie z działalności Prezesa UKE za 2021 r. str. 108. https://bip.uke.gov.pl/sprawozdania/sprawozdanie-prezesa-uke-za-2021-r-,21.html.

[9)] Dla czytelności przyjęto tą nazwę na określenie właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej. Jest to pojęcie powszechnie przyjęte w praktyce.

[10)] Sejm IX kadencji, druk nr 203 http://www.sejm.gov.pl/sejm9.nsf/druk.xsp?nr=203.

[11)] https://e-rup.knf.gov.pl/.

[12)] https://www.nccert.pl/uslugi.htm.

Niekwalifikowani dostawcy usług zaufania	10	Rejestr niekwalifikowanych dostawców usług zaufania[13)]	Pozytywne. Dostawcy będą stałymi odbiorcami wydawanych przez Pełnomocnika ostrzeżeń.
Przedsiębiorcy telekomunikacyjni	3953	Rejestr przedsiębiorców telekomunikacyjnych[14)]	Pozytywne. Motywujące. Wobec nich będzie mogło być skierowane ostrzeżenie Operator strategicznej sieci bezpieczeństwa będzie mógł się zwracać o zapewnienie odpłatnego dostępu do infrastruktury w celu świadczenia usług w strategicznej sieci bezpieczeństwa. Zostaną włączeni do krajowego systemu cyberbezpieczeństwa. Będą stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo sieci i usług komunikacji elektronicznej, obsługiwać incydenty telekomunikacyjne, zgłaszać poważne incydenty telekomunikacyjne do CSIRT Telco.
Podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów	Brak danych	-	Jako przedsiębiorcy komunikacji elektronicznej zostaną włączeni do krajowego systemu cyberbezpieczeństwa. Będą stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo sieci i usług komunikacji elektronicznej, obsługiwać incydenty telekomunikacyjne, zgłaszać poważne incydenty telekomunikacyjne do CSIRT Telco.
Narodowy Bank Polski	1	Informacja ogólnodostępna	Neutralne. Wobec Narodowego Banku Polskiego nie będzie miał zastosowania obowiązek: wycofania sprzętu lub oprogramowania od dostawcy wysokiego ryzyka.
Operator strategicznej sieci bezpieczeństwa - przedsiębiorca telekomunikacyjny, jednoosobowa spółka Skarbu Państwa	1	Wynika to z art. 76b projektu	Pozytywne. Operator będzie mógł świadczyć usługi telekomunikacyjne w ramach strategicznej sieci bezpieczeństwa.
Podmioty, którym operator strategicznej sieci bezpieczeństwa będzie mógł świadczyć usługi.	Podmioty wskazane w przypisie[15]	Wynika to z art. 76d projektu	Pozytywne. Podmioty te będą mogły korzystać ze strategicznej sieci bezpieczeństwa.
Państwowe Gospodarstwo Wodne Wody Polskie	1	Ustawa z dnia 20 lipca 2017 r. – Prawo wodne[16)]	Pozytywne. Motywujące. Włączone zostanie do krajowego systemu cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
instytucje rozwoju z wyjątkiem Banku Gospodarstwa Krajowego	5	Ustawa z dnia 4 lipca 2019 r. o systemie instytucji rozwoju[17)]	Pozytywny. Motywujący. Zostaną włączone do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.

[13)] https://www.nccert.pl/uslugiNK.htm.

[14)] https://bip.uke.gov.pl/rpt/ stan na dzień 31.10.2022 r.

[15)] Kancelaria Prezydenta RP, Kancelaria Sejmu, Kancelaria Senatu, Kancelaria Prezesa Rady Ministrów, Biuro Bezpieczeństwa Narodowego; urzędy obsługujące organy administracji rządowej, organy jednostek samorządu terytorialnego oraz podmioty podległe tym organom albo przez nie nadzorowane, wykonujące zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności państwa, ochrony granicy państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sprawiedliwości, w tym sądownictwa i prokuratury, Siły Zbrojne Rzeczypospolitej Polskiej oraz inne jednostki organizacyjne podległe lub nadzorowane przez Ministra Obrony Narodowej; instytucje wykonujące na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa

[16)] Dz. U. 2022 r. poz. 2625, z późn. zm.

[17)] Dz. U. 2023 r. poz. 1103

			Bank Gospodarstwa Krajowego, będący instytucją rozwoju, już jest podmiotem krajowego systemu cyberbezpieczeństwa zgodnie z art. 4 pkt 10 ustawy o KSC.
Samodzielne Publiczne Zakłady Opieki Zdrowotnej	1255	Sprawozdanie o stanie Krajowego Rejestru Sądowego za luty 2022 r.[18)]	Pozytywny. Motywujący. Włączone zostaną do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Centrum Łukasiewicz	1	Informacja ogólnodostępna	Pozytywny. Motywujący. Włączone zostanie do krajowego systemu cyberbezpieczeństwa. Będzie zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
instytuty działające w ramach Sieci Badawczej Łukasiewicz	33	Mapa Instytutów Łukasiewicza[19)]	Pozytywny. Motywujący. Włączone zostaną do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Międzynarodowe instytuty badawcze	2	Rejestr jednostek naukowych w bazie POL-on[20)]	Pozytywny. Motywujący. Włączone zostaną do krajowego systemu cyberbezpieczeństwa. Będą zobowiązane do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Polska Akademia Umiejętności	1	Informacja ogólnodostępna	Pozytywny. Motywujący. Włączona zostanie do krajowego systemu cyberbezpieczeństwa. Zobowiązana będzie do wyznaczenia osób do kontaktów oraz do obsługi i zgłaszania incydentów w podmiocie publicznym.
Polska Akademia Nauk	1	Informacja ogólnodostępna	Pozytywne. Jako podmiot publiczny będzie musiała wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Instytuty naukowe PAN	69	Rejestr jednostek naukowych w bazie POL-on[21)])	Pozytywne. Jako podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Uczelnie publiczne	131	RAD-on[22)]	Pozytywne. Jako podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Uczelnie niepubliczne	278	RAD-on	Pozytywne. Jako podmioty publiczne[23] będą musiały wyznaczyć 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.
Jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane	418	Wykaz jednostek organizacyjnych podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych[24)]	Jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane będą zgłaszały incydenty do CSIRT INT.
CSIRT sektorowe	7	Szacunki MC oparte o obecny wykaz	CSIRT sektorowe będą wspierać operatorów usług kluczowych w reagowaniu na incydenty.

[18)] *Sprawozdanie o stanie Rejestru Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji i Publicznych Zakładów Opieki Zdrowotnej* dostępne na: https://www.gov.pl/web/sprawiedliwosc/SprawozdaniaKRS.

[19)] https://lukasiewicz.gov.pl/images/Mapa-Instytutow-Lukasiewicza.pdf.

[20)] https://polon.nauka.gov.pl/opi/aa/rejestry/nauka?execution=e1s1.

[21)] https://bip.pan.pl/artykuly/152/rejestr-instytutow-naukowych.

[22)] https://radon.nauka.gov.pl/raporty/Uczelnie_2021.

[23)] W przypadku uczelni niepublicznych obowiązki dotyczą m. in. zgłaszania incydentów, które mają wpływ na realizowanie przez te podmioty zadań publicznych. Warto tutaj dodać, że również ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne zalicza uczelnie niepubliczne do katalogu podmiotów publicznych w zakresie, w jakim realizują zadania publiczne.

[24)] Obwieszczenie Ministra Spraw Zagranicznych z dnia 22 lutego 2023 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych (M.P. 2023 r. poz. 265).

		sektorów kluczowych (załącznik 1 ustawy o krajowym systemie cyberbezpieczeństwa)	Za pośrednictwem CSIRT sektorowych będzie przekazywany szereg istotnych informacji od operatorów usług kluczowych do CSIRT poziomu krajowego.
CSIRT KNF	1	Informacja ogólnodostępna	Z dniem wejścia w życie ustawy stanie się zespołem CSIRT sektorowym.
Potencjalne ISAC	Kilkanaście podmiotów	Szacunki MC	Pozytywne. Motywujące podmioty krajowego systemu cyberbezpieczeństwa do oddolnego wzmacniania współpracy w obszarze wymiany informacji m.in. o cyberzagrożeniach, podatnościach, czy dobrych praktykach poprzez tworzenie sformalizowanej struktury w oparciu o sprawdzoną koncepcję Centrum Wymiany Informacji i Analizy. Podmioty krajowego systemu cyberbezpieczeństwa ustalą zasady współpracy oraz zakres wymiany informacji. ISAC będą mogły zawrzeć z ministrem właściwym ds. informatyzacji porozumienie ws. dostępu systemu teleinformatycznego, o którym mowa w art. 46.
Organy właściwe do spraw cyberbezpieczeństwa	6	Informacja ogólnodostępna	Pozytywne. Motywujące organy właściwe ds. cyberbezpieczeństwa, nadzorujące kluczowe sektory gospodarki, do tworzenia CSIRT sektorowych, których zadaniem będzie bezpośrednie wsparcie operatorów usług kluczowych m.in. w reagowaniu na incydenty.
Prezes Urzędu Komunikacji Elektronicznej	1	Informacja ogólnodostępna	Prezes Urzędu Komunikacji Elektronicznej będzie nadzorował przedsiębiorców komunikacji elektronicznej w zakresie realizowania obowiązków zapewniania bezpieczeństwa sieci i usług komunikacji elektronicznej. Będzie mógł nakładać kary za niedostosowanie się do ww. obowiązków. Ponadto, będzie nakładał kary za niewycofanie sprzętu lub oprogramowania dostawcy wysokiego ryzyka przez przedsiębiorców telekomunikacyjnych.Będzie również przekazywał informacje do Komisji Europejskiej i Agencji Unii Europejskiej do spraw cyberbezpieczeństwa o poważnych incydentach telekomunikacyjnych. Będzie obowiązany do utworzenia CSIRT Telco działającego na rzecz przedsiębiorców komunikacji elektronicznej. Będzie mógł przeprowadzić analizę cen usług telekomunikacyjnych świadczonych przez Operatora strategicznej sieci bezpieczeństwa.
Kolegium do spraw Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Pozytywne. Kolegium otrzyma nowe kompetencje w postaci wydawania opinii o dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa.
Szef Agencji Wywiadu	1	Informacja ogólnodostępna	Pozytywne. Szef Agencji Wywiadu będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego. Szef Agencji Wywiadu będzie odpowiedzialny za utworzenie CSIRT INT, którego zadaniem będzie wsparcie w obsłudze incydentów polskich placówek zagranicznych.
Szef Centralnego Biura Antykorupcyjnego	1	Informacja ogólnodostępna	Pozytywne. Szef Centralnego Biura Antykorupcyjnego będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa, a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Szef Służby Wywiadu Wojskowego	1	Informacja ogólnodostępna	Pozytywne. Szef Służby Wywiadu Wojskowego będzie mógł uczestniczyć w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa a tym samym współtworzyć opinie Kolegium, dzięki czemu będą uwzględnione wszystkie aspekty cyberbezpieczeństwa i bezpieczeństwa narodowego.
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa	1	Informacja ogólnodostępna	Pozytywne. Motywujące Pełnomocnika do podejmowania aktywnych działań wynikających z otrzymania nowych kompetencji do wydawania ostrzeżeń w sytuacji podejrzenia ryzyka wystąpienia incydentu

			krytycznego. Ponadto, wzmocniona została współpraca Pełnomocnika z zespołami CSIRT poziomu krajowego. Wiele informacji dotyczących cyberbezpieczeństwa będzie publikowane w Biuletynie Informacji Publicznej Pełnomocnika.
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Pozytywne. Minister właściwy ds. informatyzacji będzie prowadził wykazy ISAC oraz SOC, dzięki temu podmioty wpisane do wykazu, po zawarciu oddzielnego porozumienia z ministrem właściwym ds. informatyzacji, będą mogły przyłączyć się do z systemu teleinformatycznego S46. Ponadto, wykazy zmobilizują ministra właściwego ds. informatyzacji do działań promujących korzystanie z systemu teleinformatycznego S46. Ponadto, minister będzie prowadził postępowania w sprawie uznania za dostawcę wysokiego ryzyka (po zasięgnięciu opinii Kolegium). Minister uzyska również uprawnienia kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie też prowadził postępowania administracyjne w sprawach związanych z certyfikacją, np. będzie zatwierdzał certyfikaty odnoszące się do poziomu zaufania „wysoki”. Będzie informował Prezesa Narodowego Banku Polskiego o wydanych decyzjach o uznaniu dostawcy za dostawcę wysokiego ryzyka.
Prezes Rady Ministrów	1	Informacja ogólnodostępna	Będzie mógł wyznaczyć operatora strategicznej sieci bezpieczeństwa, spośród jednoosobowych spółek Skarbu Państwa będących przedsiębiorcami telekomunikacyjnymi. Otrzyma możliwość wydania decyzji, w której będzie mógł przekazać realizowanie zadań, o których mowa w art. 26 ustawy o KSC, Ministrowi Obrony Narodowej. Decyzja będzie mogła być wydana na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa.
Minister Obrony Narodowej	1	Informacja ogólnodostępna	W przypadku wydania decyzji, o której mowa w art. 67e, będzie wykonywał część zadań określonych w art. 26 ustawy o KSC.
Zespoły CSIRT poziomu krajowego – CSIRT GOV, CSIRT MON, CSIRT NASK	3	Informacja ogólnodostępna	Pozytywne. Motywujące do podejmowania działań wzmacniających odporność systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa m.in. CSIRT-y poziomu krajowego otrzymają nowe kompetencje, w tym możliwość wykonywania (w porozumieniu z właściwym podmiotem ksc) testów bezpieczeństwa. Ponadto, wzmocniona zostanie współpraca zespołów CSIRT poziomu krajowego z Pełnomocnikiem.
Polskie Centrum Akredytacji	1	Informacja ogólnodostępna	Pozytywne. Polskie Centrum Akredytacji uzyska uprawnienia do prowadzenia akredytacji w nowym obszarze tematycznym.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W dniach 30.06-8.07.2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej. Zostały również przeprowadzone konsultacje wewnątrz Ministerstwa Cyfryzacji.

W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium. Powtórzono również konsultacje wewnętrzne.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów na 14 dni. Jednakże, w z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni – łącznie na uwagi było 28 dni.

Zaproszenie w ramach konsultacji publicznych skierowano do następujących podmiotów:

Polska Izba Informatyki i Telekomunikacji; Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji; Polska Izba Komunikacji Elektronicznej; Krajowa Izba Gospodarcza; Krajowa Izba Komunikacji Ethernetowej; Krajowa Izba Gospodarki Cyfrowej; Polska Izba Radiodyfuzji Cyfrowej; Fundacja Bezpieczna Cyberprzestrzeń; Polska Izba Handlu; Polskie Towarzystwo Informatyczne; Stowarzyszenie Inżynierów Telekomunikacji; Związek Rzemiosła Polskiego; Związek Pracodawców Mediów Publicznych; Związek Pracodawców Branży Internetowej IAB Polska; Polska Rada Biznesu; Naczelna Organizacja Techniczna; Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom; Izba Gospodarki Elektronicznej; Fundacja ePaństwo; Fundacja Nowoczesna Polska; Fundacja Projekt Polska; Fundacja Panoptykon; Internet Society Poland; Związek Telewizji Kablowych w Polsce Izba Gospodarcza; Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV

i IT – ZIPSEE „Cyfrowa Polska"; Polskie Centrum Badań i Certyfikacji S.A.; Polska Organizacja Handlu i Dystrybucji; Naczelna Rada Zrzeszeń Handlu i Usług; Polska Izba Producentów Urządzeń i Usług na rzecz Kolei; Polskie Stowarzyszenie Marketingu SMB; Amerykańska Izba Handlowa; Federacja Konsumentów; Polski Związek Przemysłu Motoryzacyjnego; Ogólnopolskie Porozumienie Organizacji Radioamatorskich; Polski Związek Krótkofalowców; Business Centre Club; Konfederacja Lewiatan; Rada Dialogu Społecznego; Krajowa Izba Gospodarki Morskiej; Krajowa Izba Rozliczeniowa; Polska Wytwórnia Papierów Wartościowych; Towarzystwo Gospodarcze Polskie Elektrownie; Fundacja im. Stefana Batorego; Fundacja Instytut Mikromakro; Fundacja My Pacjenci; Fundacja Przedsiębiorców Polskich Archiwizjoner; Fundacja Pułaskiego; Stowarzyszenie Inżynierów Telekomunikacji; Sektorowa Rada ds. Kompetencji - Telekomunikacja i Cyberbezpieczeństwo; Internet Society Poland Chapter

W ramach opiniowania zaproszenie skierowano do następujących podmiotów:

Prezes Urzędu Komunikacji Elektronicznej; Prezes Urzędu Ochrony Konkurencji i Konsumentów; Prezes Urzędu Ochrony Danych Osobowych; Prezes Głównego Urzędu Statystycznego; Rzecznik Małych i Średnich Przedsiębiorców; Wojskowe Biuro Zarządzania Częstotliwościami; Komisja Nadzoru Finansowego; Rzecznik Praw Obywatelskich; Krajowa Rada Radiofonii i Telewizji; Polski Komitet Normalizacyjny; Urząd Zamówień Publicznych; Najwyższa Izba Kontroli; Agencja Bezpieczeństwa Wewnętrznego; Agencja Wywiadu; Biuro Bezpieczeństwa Narodowego; Centralne Biuro Antykorupcyjne; Służba Kontrwywiadu Wojskowego; Służba Wywiadu Wojskowego; Rządowe Centrum Bezpieczeństwa; Służba Ochrony Państwa.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, pod warunkiem zgłoszenia tego faktu opiekunowi merytorycznemu.

Do projektu ustawy w ramach konsultacji publicznych uwagi zgłosiły następujące podmioty:

Związek Banków Polskich, Santander, Narodowy Instytut Cyberbezpieczeństwa, Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, Bank Handlowy, Q-PRO Jakub Stoparek, RFCell Technologies Sp. z.o.o., KGHM/Związek Pracodawców Polska Miedź, Stowarzyszenie Libertariańskie, SayF, Transition Software, Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze, Izba Przemysłowo-Handlowa Polska-Azja, Huawei Polska, Business Centre Club, Digital Poland, Excogitate, Fundacja Bezpieczna Cyberprzestrzeń, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT, Narodowy Bank Polski, Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych, Polskie Centrum Badań i Certyfikacji, Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile, Federacja Przedsiębiorców Polskich, 1Innosystems, Polska Izba Komunikacji Elektronicznej, Fabryka E-Biznesu, Krajowa Izba Gospodarki Cyfrowej DigiCom, Home.pl, Install Tech, Polska Izba Handlu, ISACA Warsaw Chapter, Krajowy Sekretariat Łączności NSZZ Solidarność, MJC Sp. z.o.o., IAB Polska, Federacja Konsumentów, Stowarzyszenie „Miasta w Internecie", Stowarzyszenie Inżynierów Telekomunikacji, Uniwersytet Jagielloński Collegium Medicum, PKP Energetyka, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne, ISSA Polska, Związek Przedsiębiorców i Pracodawców, Krajowy Depozyt Papierów Wartościowych, Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL, S4IT Michał Podgórski, Orange Polska, Polsko-Chińska Główna Izba Gospodarcza SinoCham, Aberit, Młodzieżowy Delegat RP przy NATO, ERSTAR, ETOB-RES, Fundacja Alatum, GBX Soft, Instytut Lema, Mobile Logic, Mobilne Miasto, Nanocoder, NeuroGames Lab, SmartWeb Media, TELDATA, TEP Doradztwo Biznesowe, TILT, Związek Cyfrowa Polska, Signum Edward Kuś Marcin Kuś, PKN Orlen, Skandynawsko-Polska Izba Gospodarcza, Liquid Systems, Instytut Staszica, Akademia Sztuki Wojennej, Krajowa Izba Komunikacji Ethernetowej, Qualitel Service, JARTEL, Izba Gospodarki Elektronicznej, Konfederacja Lewiatan, Porozumienie Zielonogórskie. Federacja Związków Pracodawców Ochrony Zdrowia.

Ponadto, w trybie opiniowania opinie przedstawiły następujące podmioty:

Biuro Bezpieczeństwa Narodowego, Rzecznik Małych i Średnich Przedsiębiorców, Prezes Urzędu Komunikacji Elektronicznej, Agencja Wywiadu, Prezes Urzędu Ochrony Danych Osobowych, Komisja Nadzoru Finansowego, Najwyższa Izba Kontroli, Urząd Zamówień Publicznych, Prezes Urzędu Ochrony Konkurencji i Konsumentów, Polski Komitet Normalizacyjny, NASK-PIB.

W procedurze opiniowania i konsultacji publicznych projektu ustawy wszystkim podmiotom umożliwiono zajęcie stanowiska w sprawie projektu, a także poddano analizie przedłożone przez te podmioty uwagi.

W ramach konsultacji publicznych i opiniowania zgłoszono szereg uwag do projektu ustawy: w ramach konsultacji: 548 uwag, a w ramach opiniowania: 53 uwagi.

Ponadto, tabele zawierające stanowisko wnioskodawcy do zgłoszonych uwag udostępniono na stronie RCL, w zakładce „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach procesu konsultacji i opiniowania znaczna liczba podmiotów zwracała szczególną uwagę na kwestie dotyczące

uregulowania w przepisach prawa oceny dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa pod kątem uznania tych dostawców za dostawców wysokiego ryzyka. Wskazano na potrzebę zapewnienia transportowości procesu oceny (najlepiej w oparciu o przepisy Kodeksu postępowania administracyjnego) oraz o zapewnieniu skutecznej drogi odwoławczej od ewentualnej negatywnej decyzji.

Ponadto, zwracano uwagę o doprecyzowanie stosowania nowego instrumentu w krajowym systemie cyberbezpieczeństwa tj.: ostrzeżenia.

Wiele uwag dotyczyło także kwestii włączenia do ustawy o krajowym systemie cyberbezpieczeństwa, przepisów prawa wdrażających Europejski Kodeks Łączności Elektronicznej. Podmioty wskazywały, że kwestie wymagań bezpieczeństwa oraz zgłaszania incydentów bezpieczeństwa powinny pozostać w regulacji sektorowej, jaką ma być równolegle procedowany projekt ustawy - Prawo komunikacji elektronicznej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2023 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	305,967	848,623	1 556,250	640,545	652,671	673,633	736,760	764,988	769,213	827,236	941,261	8 717,147
budżet państwa	305,967	848,623	1 556,250	640,545	652,671	673,633	736,760	764,988	769,213	827,236	941,261	8 717,147
JST	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	-305,967	-848,623	-1 556,250	-640,545	-652,671	-673,633	-736,760	-764,988	-769,213	-827,236	-941,261	-8 717,147
budżet państwa	-305,967	-848,623	-1 556,250	-640,545	-652,671	-673,633	-736,760	-764,988	-769,213	-827,236	-941,261	-8 717,147
JST	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wejście w życie projektowanej regulacji będzie stanowić od 2024 r. podstawę do ubiegania się o dodatkowe środki na ten cel z budżetu państwa w częściach: • 21 – gospodarka morska, • 22 – gospodarka wodna, • 27 –informatyzacja, • 39 – transport, • 46 - zdrowie

<table>
<tr><td></td><td>

47 – energia,
55 – aktywa państwowe,
57 – Agencja Bezpieczeństwa Wewnętrznego,
59 – Agencja Wywiadu
76 – Urząd Komunikacji Elektronicznej.

Koszty zakupu sprzętu i oprogramowania dla CSIRT sektorowych i CSIRT Telco zostaną poniesione z innych źródeł – w tym ze środków europejskich przewidzianych na realizację inwestycji „C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo” z części grantowej (bezzwrotnej) Krajowego Planu Odbudowy i Zwiększania Odporności. W przypadku braku możliwości pozyskania finansowania ze środków unijnych wydatki zostaną sfinansowane z budżetu państwa.
</td></tr>
<tr><td>Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń</td><td>
W tabeli powyżej jako rok „0” przyjęto 2024 r.
Wzrost kwoty dotacji podmiotowej dla Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego.
Rosnąca liczba zgłoszeń oraz potwierdzonych incydentów zgłaszanych do CSIRT NASK (60% r/r według przekazanych raportów) wymaga rozwijania kadry CSIRT NASK zarówno w obszarze nowych i obecnych kompetencji jak i w zakresie zwiększenia liczebności zasobów specjalistycznych.
Wskazać należy, że w tej chwili liczba podmiotów ustawowo zobligowana do raportowania incydentów i zgłaszania osób kontaktowych do CSIRT NASK kształtuje się na poziomie ponad 60 tysięcy. Rosnąca świadomość tych podmiotów wymaga zwiększonych nakładów na utrzymywanie relacji i sprawne procedowanie spraw wynikających z ustawy.
Nie bez znaczenia jest fakt, iż ostatni rok wykazuje się szczególne dużą presją płacową kadry specjalistycznej, szczególnie w obszarze cyberbezpieczeństwa.
Dlatego przewiduje się wzrost kwoty dotacji podmiotowej dla Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego wynikającej z art. 26 ust. 9 ustawy o krajowym systemie cyberbezpieczeństwa.
Zgodnie z OSR z 2018 r. wysokość dotacji przewidziano na 8,5 mln zł – ta dotacja mieści się w ramach reguły wydatkowej obecnie obowiązującej ustawy o krajowym systemie cyberbezpieczeństwa. W ustawie nowelizującej zawarta jest nowa reguła wydatkowa, w której mieścić się będzie wzrost dotacji podmiotowej dla NASK-PIB. Docelowo od 2024 r. zakłada się, że łączny koszt dotacji podmiotowej (w ramach obydwu reguł wydatkowych) wyniesie 51 mln zł rocznie. Koszty te zostaną poniesione w ramach cz. 27 – informatyzacja.
<table>
<tr><th colspan="11">Koszty wzrostu dotacji podmiotowej dla NASK-PIB w podziale na lata w mln zł</th></tr>
<tr><td>2024</td><td>2025</td><td>2026</td><td>2027</td><td>2028</td><td>2029</td><td>2030</td><td>2031</td><td>2032</td><td>2033</td><td>2034</td></tr>
<tr><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td><td>42,5</td></tr>
</table>
Planuje się także udzielenie dotacji celowej dla NASK-PIB na zakup sprzętu i oprogramowania dla CSIRT NASK.
<table>
<tr><th colspan="11">Koszty dotacji celowej dla NASK-PIB na zakup sprzętu i oprogramowania dla CSIRT NASK. w podziale na lata w mln zł</th></tr>
<tr><td>2024</td><td>2025</td><td>2026</td><td>2027</td><td>2028</td><td>2029</td><td>2030</td><td>2031</td><td>2032</td><td>2033</td><td>2034</td></tr>
<tr><td>6,36</td><td>6,72</td><td>7,2</td><td>7,44</td><td>7,68</td><td>7,92</td><td>8,4</td><td>8,64</td><td>8,88</td><td>8,88</td><td>8,88</td></tr>
</table>
Wsparcie osobowe urzędu obsługującego ministra do spraw informatyzacji.
W związku z nowymi zadaniami ministra właściwego do spraw informatyzacji w zakresie:
</td></tr>
</table>

- prowadzenia postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka;
- nadzoru i kontroli nad krajowym systemem certyfikacji cyberbezpieczeństwa,

konieczne jest wzmocnienie urzędu obsługującego ministra właściwego do spraw informatyzacji.

Koszty te zostaną poniesione w ramach budżetu państwa z cz. 27 - informatyzacja.

Prowadzenie postępowań w sprawie uznania za dostawcę wysokiego ryzyka.

Aby zapewnić efektywność postępowań administracyjnych w sprawie uznania za dostawcę wysokiego ryzyka oraz postępowań w sprawach nałożenia administracyjnych kar pieniężnych za nie wycofanie produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy wysokiego ryzyka przewiduje się wzmocnienie urzędu obsługującego ministra do spraw informatyzacji o 1 etat.

Koszty wynagrodzenia wyniosą:

- w 2024 r. - 0,127 mln zł, w tym:
  - pochodne[25] w wysokości 0,023 mln zł;
- od 2025 r. – 0,138 mln zł, w tym:
  - pochodne w wysokości 0,025 mln zł,
  - dodatkowe wynagrodzenie roczne w wysokości 9 tys. zł.

Koszty wynagrodzenia 1 stanowiska w mln zł										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
0,127	0,138	0,138	0,138	0,138	0,138	0,138	0,138	0,138	0,138	0,138

Utworzenie wydziału krajowego systemu certyfikacji cyberbezpieczeństwa.

W ramach przyjęcia nowych zadań w zakresie certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji konieczne jest wzmocnienie urzędu obsługującego ten organ. W celu sprawnego wykonywania nowych zadań konieczne będzie utworzenie nowego wydziału i zatrudnienie pracowników. Pracownicy tworzonego wydziału będą zajmować się przede wszystkim prowadzeniem postępowań administracyjnych, analizą rynku i współpracą międzynarodową. Konieczne jest wyasygnowanie środków na stanowiska naczelnika wydziału oraz 2 głównych specjalistów.

Koszty wynagrodzeń wyniosą:

- w 2024 r. - 0,412 mln zł, w tym:
  - pochodne w wysokości 0,074 mln zł;
- od 2025 r. – 0,446 mln zł w tym:
  - pochodne w wysokości 0,073 mln zł,
  - dodatkowe wynagrodzenie roczne w wysokości 29 tys. zł.

Przy wyliczeniach przyjęto mnożnik kwoty bazowej w wysokości:

- 3,2 dla głównych specjalistów,
- 4,0 dla naczelnika wydziału.

[25] Pod pojęciem *pochodne* rozumie się:
- składki na ubezpieczenie emerytalne, ubezpieczenie rentowe, ubezpieczenie wypadkowe, Fundusz Pracy, Fundusz Solidarnościowy;
- a także wpłatę na Pracownicze Plany Kapitałowe.

Koszty wynagrodzeń 3 stanowisk w mln zł										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
0,412	0,446	0,446	0,446	0,446	0,446	0,446	0,446	0,446	0,446	0,446

Koszty organizacji stanowisk pracy.

Koszty organizacji stanowisk pracy dla wskazanych wyżej 4 osób wyniosą w 2024 r. łącznie 36 tys. zł. Koszty te zostaną poniesione w ramach budżetu państwa z cz. 27 - Informatyzacja.

Tworzenie krajowych programów certyfikacji cyberbezpieczeństwa.

Od 2024 r. podjęte zostaną prace nad tworzeniem krajowych programów certyfikacji cyberbezpieczeństwa. W ich ramach konieczne będzie wypracowanie standardów technicznych oraz wymagań na kilka poziomów uzasadnienia zaufania, co w praktyce oznacza konieczność przygotowania kilku szczegółowych dokumentów technicznych w ramach jednego krajowego programu certyfikacji cyberbezpieczeństwa. Zadania te będą zlecane na rynek w formie zamówienia publicznego. Ponadto krajowe programy certyfikacji cyberbezpieczeństwa będą stanowiły nowy rodzaj dokumentów technicznych, co potencjalnie wpływa na wzrost ceny. Wypracowane rozwiązania muszą też uwzględniać stan wiedzy technicznej i najlepsze praktyki w dziedzinie cyberbezpieczeństwa. Koszt obejmuje również przeniesienie majątkowych praw autorskich do wypracowanych dokumentów. Biorąc pod uwagę, że dotychczas podobne usługi związane ze wsparciem ekspertów kosztowały ok. 100 000 zł, mając równocześnie dużo mniejszy zakres czynności, przyjęto, że koszty wykonania tego zadania wyniosą 300 000 zł w 2024 r., a w kolejnych latach kwota będzie zwiększać się o 5%. Łącznie w latach 2024-2034 koszty wyniosą ok 4,481 mln zł. Koszty te zostaną poniesione w ramach cz. 27 – informatyzacja.

Koszty umów zlecenia bądź umów o dzieło z ekspertami tworzącymi propozycje krajowych programów certyfikacji cyberbezpieczeństwa w mln zł										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
0,315	0,331	0,348	0,365	0,383	0,403	0,423	0,444	0,466	0,489	0,514

Przygotowanie opinii na potrzeby realizacji zadań krajowego organu ds. certyfikacji cyberbezpieczeństwa

W celu wsparcia ministra właściwego do spraw informatyzacji w zakresie nadzoru nad krajowym systemem certyfikacji cyberbezpieczeństwa planuje się zlecanie przygotowania opinii zewnętrznych. Koszty opinii wyniosą 30 tys. zł rocznie. Koszty te zostaną poniesione w ramach cz. 27 – informatyzacja.

Wzrost kwoty na dotację celową na utrzymanie i rozwój systemu teleinformatycznego S46

W związku z obowiązkiem korzystania przez:

- Pełnomocnika,
- zespoły CSIRT poziomu krajowego,
- Prezesa Urzędu Komunikacji Elektronicznej,
- zespoły CSIRT sektorowe,
- CSIRT Telco

z systemu, o którym mowa w art. 46 ustawy o KSC przewidziano wzrost kwoty na dotację celową na utrzymanie i rozwój tego systemu[26].

Koszty wzrostu dotacji celowej zostaną poniesione z cz. 27 – informatyzacja.

Koszty wzrostu dotacji celowej na utrzymanie i rozwój S46 w podziale na lata w mln zł										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
14,459	12,714	8,844	7,882	11,750	15,452	25,079	25,046	17,009	17,009	17,009

Urządzenia dla Systemów Brzegowych Uczestnika (SBU) są finansowane ze środków budżetowych. SBU są w istocie elementami S46 i muszą pozostawać pod kontrolą utrzymującego system. Po stronie Uczestnika pozostaną koszty związane z utrzymywaniem łączy telekomunikacyjnych do Centrów Operacyjnych S46.

Uczestnicy/Partnerzy (operatorzy usług kluczowych, dostawcy usług cyfrowych lub podmioty publiczne, którzy są zdefiniowani w ustawie o krajowym systemie cyberbezpieczeństwa) w związku z podłączeniem się do S46 będą musieli dedykować odpowiednie zasoby ludzkie do obsługi systemu. W przypadku konieczności dodatkowego finansowania zakupu SBU, Uczestnicy mogą zrezygnować z podłączenia się do S46.

Centralne finansowanie SBU zapewnia interoperacyjność sprzętu, umożliwia lepsze serwisowanie, zmniejsza koszt zakupu jednostkowego sprzętu wraz z niezbędnymi licencjami, usprawnia instalację logistycznie (SBU programuje i administruje nim operator S46).

Koszty transmisji pomiędzy Centrami Operacyjnymi będą finansowane ze środków budżetowych.

Komunikacja pomiędzy Centrami Operacyjnymi jest niezbędnym elementem, mającym na celu zapewnienie wysokiej dostępności S46. Organy właściwe do spraw cyberbezpieczeństwa, uprawnione do korzystania z S46, są podmiotami z sektora administracji publicznej. Zakłada się podłączanie interesariuszy ze środków przeznaczonych na utrzymanie i rozwój S46. Po stronie organu właściwego znajdzie się koszt utrzymywania łącza telekomunikacyjnego do Centrum Operacyjnego.

Powstanie zespół na potrzeby całościowej analizy obrazu sytuacyjnego i analizy ryzyka na poziomie kraju.

Jednym z celów wytworzenia S46 jest uzyskanie całościowego obrazu sytuacyjnego i szacowania ryzyka na poziomie kraju. Przetwarzanie i analizowane informacji na tym poziomie przez poszczególne CSIRT wiązałoby się z budowaniem kompetencji w modelu wyspowym. Co więcej doświadczenie pokazuje, że poszczególne sektory niechętnie dzielą się informacjami z własnego *constituency*. Wskazuje to na potrzebę zorganizowania centralnego zespołu analityków, którzy zajmowaliby się analizą danych, ich korelacją, normalizowaniem itp. - w S46, na poziomie całego Państwa.

Pożądanym byłoby, aby analitycy byli zlokalizowani w podmiocie odpowiedzialnym za utrzymanie i rozwój S46.

Liczba dołączanych SBU w ciągu roku.

Liczba dołączanych SBU wpływa na odwzorowanie sieci powiązań pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa, a zatem na odwzorowanie rzeczywistego poziomu cyberbezpieczeństwa w Polsce. Założono harmonogram podłączeń, w ramach którego do maksymalnie 2023 roku będą dołączone wszystkie podmioty KSC, a następnie będą podłączane jedynie instytucje nowe lub realizujące nowe lub zmodyfikowane przedsięwzięcia, gdy zmiana powoduje, że spełniają one kryteria podłączenia do systemu teleinformatycznego S46.

[26] System ten dalej będzie zwanym: S46.

Szczegółowe wyliczenia wzrostu kwoty na dotację celową na utrzymanie i rozwój S46 zawiera załącznik nr 2 do OSR.

Budowa CSIRT sektorowych oraz CSIRT Telco

Budowa 6 zespołów CSIRT sektorowych będzie kosztownym przedsięwzięciem, które pozwoli jednak zapełnić lukę w reagowaniu na incydenty w najbardziej narażonych sektorach gospodarki, w których incydenty mogą mieć katastrofalne skutki. W skład usług oferowanych przez CSIRT sektorowy wchodzić będą usługi analityczne oraz reagowania na incydenty.

Ponadto utworzony zostanie CSIRT Telco wspierający przedsiębiorców komunikacji elektronicznej w obsłudze incydentów telekomunikacyjnych.

W zależności od wielkości sektora utworzone zostaną 3 rodzaje CSIRT sektorowych:

Rodzaj CSIRT	Sektor/podsektor	Organ właściwy do spraw cyberbezpieczeństwa	Część budżetowa
Mały CSIRT sektorowy	Infrastruktura cyfrowa	minister właściwy do spraw informatyzacji[27)]	27 - Informatyzacja
	Zaopatrzenie w wodę i jej dystrybucja	minister właściwy do spraw gospodarki wodnej	22 - Gospodarka wodna
Średni CSIRT sektorowy	Transport wodny	minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej	21 - Gospodarka morska
	Transport lądowy i powietrzny	minister właściwy do spraw transportu[28)]	39 - Transport
Duży CSIRT sektorowy	Energia	minister właściwy do spraw energii[29)]	47 - Energia
	Ochrona zdrowia	minister właściwy do spraw zdrowia[30)]	46 - Zdrowie

CSIRT Telco będzie utworzony przez Prezesa Urzędu Komunikacji Elektronicznej, który jest dysponentem części budżetowej 76 – Urząd Komunikacji Elektronicznej.

Wydatki na utworzenie i funkcjonowanie CSIRT sektorowych zostaną poniesione z budżetu państwa, z poszczególnych części budżetowych organów właściwych do spraw cyberbezpieczeństwa.

[27)] Obecnie (kwiecień 2023 r.) jest nim Minister Cyfryzacji zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 792.)

[28)] Obecnie (kwiecień 2023 r.) działami administracji rządowej gospodarka morska, gospodarka wodna, transport oraz żegluga śródlądowa kieruje Minister Infrastruktury, zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 18 listopada 2019 r. w sprawie szczegółowego zakresu działania Ministra Infrastruktury (Dz. U. z 2021 r. poz. 937).

[29)] Obecnie (kwiecień 2023 r.) jest nim Minister Klimatu i Środowiska, zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 27 października 2021 r. w sprawie szczegółowego zakresu działania Ministra Klimatu i Środowiska (Dz. U. z 2021 r. poz. 1949).

[30)] Obecnie (kwiecień 2023 r.) jest nim Minister Zdrowia, zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 27 sierpnia 2020 r. w sprawie szczegółowego zakresu działania Ministra Zdrowia (Dz. U. 2021 r. poz. 932).

Wydatki na CSIRT sektorowy dla sektora „ochrona zdrowia” zostaną poniesione w ramach limitów wskazanych w art. 131c ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych[31)].

Z uwagi na to, że obecny jedyny sektorowy zespół cyberbezpieczeństwa – CSIRT KNF – już funkcjonuje w ramach Urzędu Komisji Nadzoru Finansowego to nie przewiduje się dodatkowych środków na jego funkcjonowanie. Finansowanie tego zespołu odbywa się na zasadach określonych w rozdziale 3 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[32)].

Dla celów obliczeń w OSR przyjęto następujące rodzaje pracowników

- operator 1 linii SOC – odpowiedzialny za przyjmowanie zgłoszeń incydentów, monitorowane incydentów, triaż, przekazywanie informacji dalej. 1 linia działa w trybie 24/7 – przewiduje się pracę 3 zmianową.
- analityk 2 linii – obsługa zgłoszeń przekazanych z pierwszej linii.
- ekspert 3 linii – zaawansowany specjalista od najtrudniejszych zdarzeń.
- pozostali specjaliści – specjaliści m. in. od Cyber Threat Intelligence, analiz podatności, informatyki śledczej, testów bezpieczeństwa, szkoleń. Liczba zależna od wielkości CSIRT – od 4 do 6 w zależności od wielkości CSIRT.
- kierownik CSIRT sektorowego – osoba zarządzająca CSIRT.

Przyjęto następujące kalkulacje wynagrodzeń:

dla dużego CSIRT sektorowego:

- 1 linia SOC - 15 etatów - wynagrodzenie miesięczne 8000 zł:
  - w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 1 440 000 zł oraz pochodne w wysokości 304 000 zł;
  - od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 1 440 000 zł, dodatkowe wynagrodzenie roczne w wysokości 123 000 zł, pochodne w wysokości 330 000 zł;
- 2 linia SOC - 3 etaty - wynagrodzenie miesięczne 9000 zł:
  - w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł oraz pochodne w wysokości 69 000 zł;
  - od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł, dodatkowe wynagrodzenie roczne w wysokości 28 000 zł, pochodne w wysokości 75 000 zł;
- 3 linia SOC - 2 etaty - wynagrodzenie miesięczne 11 000 zł:
  - w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 264 000 zł oraz pochodne w wysokości 56 000 zł;
  - od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 264 000 zł, dodatkowe wynagrodzenie roczne w wysokości 23 000 zł, pochodne w wysokości 61 000 zł;
- pozostali specjaliści - 6 etatów - wynagrodzenie miesięczne 10 000 zł:
  - w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 720 000 zł oraz pochodne w wysokości 152 000 zł;
  - od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 720 000 zł, dodatkowe wynagrodzenie roczne w wysokości 62 000 zł, pochodne w wysokości 166 000 zł;
- Kierownik CSIRT - 1 etat - wynagrodzenie miesięczne 12 000 zł:
  - w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł oraz pochodne w wysokości 31 000 zł;
  - od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł, dodatkowe wynagrodzenie roczne w wysokości 13 000 zł, pochodne w wysokości 34 000 zł.

[31)] Dz. U. z 2022 r. poz. 2561 z późn. zm

[32)] Dz. U. z 2023 r. poz. 753 i 825.

	Dla średniego CSIRT sektorowego: • 1 linia SOC - 12 etatów - wynagrodzenie miesięczne 8000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 1 152 000 zł oraz pochodne w wysokości 244 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 1 152 000 zł, dodatkowe wynagrodzenie roczne w wysokości 98 000 zł, pochodne w wysokości 264 000 zł; • 2 linia SOC - 3 etaty - wynagrodzenie miesięczne 9000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł oraz pochodne w wysokości 69 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł, dodatkowe wynagrodzenie roczne w wysokości 28 000 zł, pochodne w wysokości 75 000 zł; • 3 linia SOC - 2 etaty - wynagrodzenie miesięczne 11 000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 264 000 zł oraz pochodne w wysokości 56 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 264 000 zł, dodatkowe wynagrodzenie roczne w wysokości 23 000 zł, pochodne w wysokości 61 000 zł; • pozostali specjaliści - 5 etatów - wynagrodzenie miesięczne 10 000 zł; ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 600 000 zł oraz pochodne w wysokości 127 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 600 000 zł, dodatkowe wynagrodzenie roczne w wysokości 51 000 zł, pochodne w wysokości 138 000 zł; • Kierownik CSIRT - 1 etat - wynagrodzenie miesięczne 12 000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł oraz pochodne w wysokości 31 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł, dodatkowe wynagrodzenie roczne w wysokości 13 000 zł, pochodne w wysokości 34 000 zł. Dla małego CSIRT sektorowego: • 1 linia SOC - 9 etatów - wynagrodzenie miesięczne 8000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 864 000 zł oraz pochodne w wysokości 183 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 864 000 zł, dodatkowe wynagrodzenie roczne w wysokości 74 000 zł, pochodne w wysokości 198 000 zł; • 2 linia SOC - 3 etaty - wynagrodzenie miesięczne 9000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł oraz pochodne w wysokości 69 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 324 000 zł, dodatkowe wynagrodzenie roczne w wysokości 28 000 zł, pochodne w wysokości 75 000 zł; • 3 linia SOC - 2 etaty - wynagrodzenie miesięczne 11 000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 264 000 zł oraz pochodne w wysokości 56 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 264 000, dodatkowe wynagrodzenie roczne w wysokości 23 000 zł, pochodne w wysokości 61 000 zł; • Pozostali specjaliści - 4 etaty - wynagrodzenie miesięczne 10 000 zł: ○ w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 480 000 oraz pochodne w wysokości 102 000 zł; ○ od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 480 000, dodatkowe wynagrodzenie roczne w wysokości 41 000 zł, pochodne w wysokości 110 000 zł; • Kierownik CSIRT - 1 etat - wynagrodzenie miesięczne 12 000 zł:

- w 2024 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł oraz pochodne w wysokości 31 000 zł;
- od 2025 r. łączne roczne koszty wynagrodzenia wyniosą 144 000 zł, dodatkowe wynagrodzenie roczne w wysokości 13 000 zł, pochodne w wysokości 34 000 zł.

Oprócz kosztów wynagrodzeń konieczne będzie sfinansowanie:

- kosztów zakupu sprzętu i licencji na oprogramowanie, a także aktualizacji i wymiany sprzętu w latach 2024–2034 w wysokości ok. 84 mln zł.

  Planuje się, że w pierwszym roku funkcjonowania CSIRT sektorowych oraz CSIRT Telco każdy z nich otrzyma po 3 000 000 zł na sprzęt i oprogramowanie. W kolejnych latach poniosą one koszty amortyzacji w wysokości 900 000 zł na CSIRT.

  Koszty te zostaną poniesione z innych źródeł – w tym ze środków europejskich przewidzianych na realizację inwestycji „C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo" z części grantowej (bezzwrotnej) Krajowego Planu Odbudowy i Zwiększania Odporności. W przypadku niemożliwości uzyskania środków z innych źródeł wydatki te zostaną poniesione z budżetu państwa.
- kosztów podłączenia do systemu S46 w latach 2024–2032 w wys. 3,304 mln zł.

  Zespoły CSIRT sektorowe oraz CSIRT Telco będą podłączone do S46. Podłączenie 1 zespołu szacuje się na 43 000 zł. Natomiast utrzymanie łączy rocznie wraz z kosztem energii elektrycznej szacuje się na 39 000 zł.

Wszystkie koszty dla CSIRT sektorowych i CSIRT Telco przedstawiono jako koszty stałe.

Koszty budowy i funkcjonowania CSIRT sektorowych według rodzaju w mln zł											
Rodzaj /rok	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
Duży CSIRT	6,586	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746
Średni CSIRT	6,093	4,208	4,208	4,208	4,208	4,208	4,208	4,208	4,208	4,208	4,208
Mały CSIRT	5,599	3,672	3,672	3,672	3,672	3,672	3,672	3,672	3,672	3,672	3,672

Koszty budowy i funkcjonowania CSIRT sektorowych i CSIRT Telco w podziale na lata w mln zł.										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
43,142	29,998	29,998	29,998	29,998	29,998	29,998	29,998	29,998	29,998	29,998

Przepisy nie określają formy prawnej podmiotu realizującego zadania CSIRT sektorowego, pozostawiając organowi właściwemu decyzję co do wyboru podmiotu, który stanie się takim CSIRT. Podobnie jest w przypadku CSIRT Telco, który powołuje Prezes UKE. Mogą to być zarówno jednostki budżetowe, jak i np. instytuty badawcze.

Dla CSIRT Telco przyjęto założenia jak dla dużego CSIRT.

CSIRT INT

Ustawa przewiduje powstanie CSIRT INT prowadzonego przez Szefa Agencji Wywiadu. Będzie to CSIRT dedykowany dla jednostek organizacyjnych podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych.

Koszty jego budowy i funkcjonowania zostaną sfinansowane z cz. 59 budżetu państwa – Agencja Wywiadu.

Koszty budowy i funkcjonowania CSIRT INT w podziale na lata w mln zł.										
2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034
6,586	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746	4,746

Koszty badań z art. 33

Ustawa przewiduje możliwość zlecania, przez Pełnomocnika lub Przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa, badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

W oparciu o dane przedstawione przez Ministra Koordynatora Służb Specjalnych szacuje się, że roczne koszty tych badań wyniosą ok. 3 mln zł.

Powstanie strategicznej sieci bezpieczeństwa i wyznaczenie jej operatora.

Utrzymanie, rozwój i modernizacja strategicznej sieci bezpieczeństwa będą finansowane, w formie dotacji celowej dla Operatora strategicznej sieci bezpieczeństwa, ze środków budżetu państwa – cz. 55 - aktywa państwowe. W 2024 r. wysokość kosztów związanych z realizacją tych zdań wyniesie 189 mln zł.

Niemierzalnym skutkiem dla budżetu państwa jest zapewnienie takiego funkcjonowania bezpiecznego ekosystemu sieci telekomunikacyjnej dla najważniejszych osób, urzędów i służb w państwie, który do minimum ograniczy incydenty bezpieczeństwa i konieczność reagowania na nie.

Koszty związane z wdrożeniem i utrzymaniem sieci strategicznej (w podziale na kategorie) w latach 2024 – 2034 prezentują się następująco:

Kategoria kosztów	Koszty w latach 2024-2034 (w mln zł)											Suma kosztów
	2024	**2025**	**2026**	**2027**	**2028**	**2029**	**2030**	**2031**	**2032**	**2033**	**2034**	
Zapewnienie infrastruktury pasywnej	24	190	458	248	248	248	248	248	248	248	248	2 656
Zapewnienie infrastruktury aktywnej	127	398	831	161	167	175	183	191	227	287	387	3 134
Zatrudnienie i wynagrodzenia	32	54	58	62	66	71	76	81	87	93	100	780
Pozostałe koszty infrastrukturalne i software'owe	6	106	112	73	71	75	115	130	100	92	99	979
Suma kosztów	189	748	1 459	544	552	569	622	650	662	720	834	**7 549**

Wydatki te obejmują:

- zapewnienie infrastruktury pasywnej

Ta kategoria kosztów obejmuje przede wszystkim dzierżawę masztów telekomunikacyjnych oraz innych lokalizacji, na których możliwe jest umiejscowienie infrastruktury aktywnej (np. dachy budynków, wieże). Dodatkowo, w okresie od 2024 do 2026 planowane jest zbudowanie od podstaw ok. 330 stacji tak, aby zapewnić pokrycie zasięgiem 5G miejsc trudno dostępnych. W ramach budowy sieci planowane jest zarządzenia łącznie 10 000 stacjami. Do wyceny kosztów dzierżawy lokalizacji przyjęto średnią cen rynkowych dostępnych ofert operatorów mobilnych.

W przypadku budowy infrastruktury od podstaw przyjęto rynkowy koszt budowy pomnożony przez współczynnik 2-3. Wynika to głównie z budowy wzmocnionych konstrukcji, doprowadzenia przyłącza energetycznego, doprowadzenia łącza światłowodowego lub kilku przęsłowych radiolinii oraz kosztów robocizny w niestandardowym terenie.

- zapewnienie infrastruktury aktywnej

Kategoria ta obejmuje zakup urządzeń do komunikacji i wdrożenia Radio Access Network (RAN), ich instalację, utrzymanie, a także koszt energii elektrycznej na potrzeby RAN. Zakup urządzeń odbywać się będzie u dostawców zagranicznych, stąd też powyższe wydatki zależne są od kursu PLN. Dla celów analizy przyjęto ostrożnie, że kurs wyniesie przeciętnie 4,7 USD/PLN.

- zatrudnienie i wynagrodzenia

Szacuje się, że zarządzanie siecią strategiczną wymagać będzie około 120 FTE (Full-Time equivalent), w tym około 100 inżynierów i 20 osób z obszaru administracji.

- pozostałe koszty infrastrukturalne i software'owe

Pozostałe koszty obejmują m.in. zapewnienie punktów agregujących ruch sieciowy z infrastruktury aktywnej, sieci backhaul, sieci core oraz systemów wsparcia obsługi procesów operacyjnych i biznesowych OSSB.

Wpływ projektu ustawy na jednostki samorządu terytorialnego.

Jednostki samorządu terytorialnego są zobowiązane na podstawie § 20 rozporządzenia o Krajowych Ramach Interoperacyjności[33)] do przeprowadzania zarządzania ryzykiem. Wobec tego będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Natomiast decyzja o uwzględnieniu tych środków będzie należała wyłącznie do nich.

Jednostki samorządu terytorialnego będą obowiązane umożliwić operatorowi strategicznej sieci bezpieczeństwa umieszczenie na nieruchomości obiektów i urządzeń infrastruktury telekomunikacyjnej, w szczególności instalowanie urządzeń telekomunikacyjnych, przeprowadzanie linii kablowych pod nieruchomością, na niej lub nad nią, umieszczanie tabliczek informacyjnych o urządzeniach, a także ich eksploatację i konserwację, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia wartości nieruchomości. Jednostce samorządu terytorialnego zostanie zwrócona część kosztów związanych z zapewnieniem dostępu.

Wpływ finansowy projektu ustawy na jednostki samorządu terytorialnego jest niemożliwy do oszacowania.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
	duże przedsiębiorstwa	-32,308	-15,366	-15,366	-15,366	-15,366	-15,366	-185,968

[33)] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

W ujęciu pieniężnym (w mln zł, ceny stałe z 2023 r.)	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa	Zmiany w ustawie o krajowym systemie cyberbezpieczeństwa spowodują konieczność wypracowania przez operatorów usług kluczowych procedur kontaktu z zespołami CSIRT sektorowymi. Operatorzy usług kluczowych będą zobowiązani korzystać z systemu S46 od 1 stycznia 2024 r. co spowoduje konieczność poniesienia kosztów jednorazowych (zakup sprzętu, oprogramowania i łączy) oraz stałe koszty abonamentu łączy i energii. Koszty te zostały uwzględnione w tabeli powyżej. W ramach Krajowego Planu Odbudowy i Zwiększania Odporności oraz funduszu REACT-EU planowane jest sfinansowanie podłączenia niektórych podmiotów, w tym operatorów usług kluczowych, do systemu S46. Dotychczasowe podmioty świadczące usługi z zakresu cyberbezpieczeństwa staną się SOC zewnętrznymi działającymi na rzecz operatorów usług kluczowych. Zmieni się zakres obowiązków SOC w stosunku do poprzednich przepisów ustawowych. Z chwilą wejścia w życie nowelizacji SOC zewnętrzne będą wdrażały zabezpieczenia na podstawie przeprowadzonego szacowania ryzyka. Przedsiębiorcy komunikacji elektronicznej zostaną włączeni do krajowego systemu cyberbezpieczeństwa. Będą stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo sieci i usług komunikacji elektronicznej, obsługiwać incydenty telekomunikacyjne, zgłaszać poważne incydenty telekomunikacyjne do CSIRT Telco. Będą musieli wypracować wewnętrzne procedury w zakresie stosowania ww. środków technicznych i organizacyjnych, obsługi incydentów telekomunikacyjnych. Ponadto będą musieli wypracować kanały komunikacji z CSIRT Telco oraz z właściwym CSIRT poziomu krajowego. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorstwami) będą musiały wycofać dany sprzęt lub oprogramowanie określony w decyzji o uznaniu za dostawcę wysokiego ryzyka z użycia w ciągu 7 lat. Podkreślenia wymaga, że wycofaniu będą podlegały produkty, usługi, procesy określone w decyzji – a więc nie wszystkie produkty (usługi, procesy) oferowane przez dostawcę wysokiego ryzyka. Natomiast przedsiębiorcy telekomunikacyjni, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku. Podmioty zobowiązane do wycofania produktów, usług i procesów pochodzących od dostawcy wysokiego ryzyka nie będą mogły ich zamawiać poprzez Prawo zamówień publicznych, jeżeli do nich stosuje się ta ustawa. .						

		Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Nowelizacja wprowadza kary za niedostosowanie się do obowiązku wycofania produktów ICT, usług ICT i procesów ICT dostawcy wysokiego ryzyka. Kary te wyniosą do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Oczywiście znajdą tutaj zastosowanie przepisy dotyczące administracyjnych kar pieniężnych z Kodeksu postępowania administracyjnego. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów.
	sektor mikro-, małych i średnich przedsiębiorstw	W wyniku planowanych zmian SOC wewnętrzne oraz SOC zewnętrzne, na podstawie przeprowadzonego szacowania ryzyka, mają prowadzić działania zapewniające cyberbezpieczeństwo, w szczególności wprowadzać zabezpieczenia zapewniające poufność integralność, dostępność i autentyczność przetwarzanych danych. Charakter zabezpieczeń będzie więc zależny od wielkości podmiotu, posiadanej infrastruktury, charakteru świadczonych usług oraz ryzyk z jakimi mierzy się dany podmiot. Tym samym jest to proporcjonalne rozwiązanie także wobec SOC będących przedsiębiorcami MŚP. Z kolei obowiązki z nowego rozdziału 4a nakładane na przedsiębiorców komunikacji elektronicznej są ewolucją obecnych przepisów Działu VIIA. Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych Prawa telekomunikacyjnego[34)]. Wszyscy przedsiębiorcy telekomunikacyjni obecnie są już obowiązani stosować środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. W proponowanym przepisie art. 20a ust. 2 pkt 2 wskazano, że przedsiębiorca komunikacji elektronicznej podejmuje środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka. Uwzględnia to sytuację mikro-, małych i średnich przedsiębiorców, którzy będą mierzyć się z innymi ryzykami w swojej działalności niż np. duzi operatorzy sieci mobilnych. Przedsiębiorcy ci będą obsługiwać incydenty telekomunikacyjne oraz zgłaszać poważne incydenty telekomunikacyjne do CSIRT Telco. Będą musieli wypracować wewnętrzne procedury w zakresie stosowania ww. środków technicznych i organizacyjnych, obsługi incydentów telekomunikacyjnych. Ponadto, będą musieli wypracować kanały komunikacji z CSIRT Telco oraz z właściwym CSIRT poziomu krajowego. Warto też dodać, że wprowadzając wymóg wyznaczenia 2 osób do kontaktu wyłączono z tego obowiązku sytuację mikro-, małych i średnich przedsiębiorców komunikacji elektronicznej (art. 20a ust. 4). Projektowane zmiany w nowelizacji polegają m.in. na powołaniu nowych zespołów CSIRT sektorowych oraz zespołu CSIRT Telco, których zadaniem będzie wspieranie przedsiębiorców w kluczowych sektorach gospodarki. Będzie to konkretna pomoc dla tych podmiotów – nie będzie ona ograniczała się wyłącznie do wsparcia w reagowaniu na incydenty, ale na bieżącej wymianie informacji o podatnościach, cyberzagrożeniach, prowadzeniu szkoleń, czy wspieraniu operatorów usług kluczowych w wykonywaniu obowiązków z ustawy o krajowym systemie cyberbezpieczeństwa. Innymi słowy nowelizacja nakłada bardzo wiele obowiązków na państwo celem wsparcia przedsiębiorców. Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy, operatorzy infrastruktury krytycznej czy przedsiębiorcy telekomunikacyjni (będący dużymi przedsiębiorstwami) będą musiały wycofać dany sprzęt lub oprogramowanie określony

[34)] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, z późn. zm.).

		w decyzji o uznaniu za dostawcę wysokiego ryzyka z użycia w ciągu 7 lat. Podkreślenia wymaga, że wycofaniu będą podlegały produkty, usługi, procesy określone w decyzji – a więc nie wszystkie produkty (usługi, procesy) oferowane przez dostawcę wysokiego ryzyka. Obowiązek wycofania produktów, usług i procesów dostawcy wysokiego ryzyka będzie dotyczył tych mikro-, małych i średnich przedsiębiorców telekomunikacyjnych, którzy sporządzają plany działań w sytuacji szczególnego zagrożenia. Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. W związku z działalnością operatora strategicznej sieci bezpieczeństwa przedsiębiorcy telekomunikacyjni udostępniają swoją infrastrukturę na zasadach odpłatności.
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.
Niemierzalne	Koszty związane z wycofaniem sprzętu lub oprogramowania od dostawców wysokiego ryzyka	Nowelizacja przewiduje kompetencję dla ministra właściwego do spraw informatyzacji do wydania decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni oraz operatorzy infrastruktury krytycznej w związku z wycofaniem produktów, usług i procesów pochodzących od dostawców wysokiego ryzyka, ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu. Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 5-7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu (operator usług kluczowych, dostawca usług cyfrowych, SOC, przedsiębiorców telekomunikacyjnych) i sektora. Nie jest możliwe oszacowanie kosztów dostosowania się przedsiębiorców do wymogów określonych w nowelizacji. Wynika to z faktu, że konkretne środki techniczne i organizacyjne stosowane przez przedsiębiorców będą zależne od przeprowadzonego szacowania ryzyka. Innego rodzaju środki będą stosować operatorzy zarządzający własną infrastrukturą telekomunikacyjną a inne dostawcy usług komunikacji elektronicznej, którzy swoją działalność opierają o infrastrukturę innego operatora. Ponadto nie są znane konkretne środki już teraz stosowane przez przedsiębiorców – często, z powodów bezpieczeństwa, informacja o tych środkach stanowi tajemnicę przedsiębiorstwa. Projekt nakłada jedynie konieczne i niezbędne obowiązki, aby osiągnąć cele ustawy. Projekt nie wprowadza regulacji dot. zakazu wykonywania określonej działalności gospodarczej. Z tych powodów uznaje się, że projekt jest zgodny z ustawą z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☒ tak ☐ nie ☐ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Ustawa spowoduje zmniejszenie w niektórych obszarach (SOC zewnętrzne/wewnętrzne) obciążeń regulacyjnych, za to wprowadzi nowe – dla ISAC, oraz dostawców sprzętu lub oprogramowania, przedsiębiorców telekomunikacyjnych, podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów.

Zmiany regulacyjne dla operatorów usług kluczowych:

- będą obowiązani regularnie przeprowadzać aktualizacje oprogramowania zgodnie z zaleceniami producenta z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji.
- będą obowiązani wyznaczyć dwie osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa, a nie jedną, jak do tej pory.
- rozszerzono obowiązki z zakresu nadzoru nad dokumentacją bezpieczeństwa systemu informacyjnego.
- zgłoszenia incydentów poważnych będą przekazywane do zespołu CSIRT sektorowego za pomocą systemu S46.
- uproszczono obowiązki SOC wewnętrznych lub SOC zewnętrznych działających na rzecz OUK. Będą wdrażać zabezpieczenia na podstawie szacowania ryzyka, zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji. Obecnie wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa muszą spełniać szczegółowe minimalne warunki techniczno-organizacyjne określone w rozporządzeniu.
- będą obowiązani do korzystania z systemu S46 od 1 stycznia 2024 r.
- Infrastruktura SOC będzie musiała znajdować się na terytorium kraju.
- Personel SOC będzie obowiązany posiadać poświadczenie bezpieczeństwa do poziomu „poufne”.

Przedsiębiorcy komunikacji elektronicznej zostaną włączeni do krajowego systemu cyberbezpieczeństwa. Będą stosować środki techniczne i organizacyjne zapewniające bezpieczeństwo sieci i usług komunikacji elektronicznej, obsługiwać incydenty telekomunikacyjne, zgłaszać poważne incydenty telekomunikacyjne do CSIRT Telco. Będą musieli wypracować wewnętrzne procedury w zakresie stosowania ww. środków technicznych i organizacyjnych, obsługi incydentów telekomunikacyjnych. Ponadto będą musieli wypracować kanały komunikacji z CSIRT Telco oraz z właściwym CSIRT poziomu krajowego.

Wpływ w tym obszarze będzie zróżnicowany. Przedsiębiorcy telekomunikacyjni już na podstawie dotychczas obowiązujących przepisów Działu VIIA Prawa telekomunikacyjnego byli obowiązani stosować środki techniczne i organizacyjne celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Ponadto byli obowiązani poinformować Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach. Prezes UKE jednak nie posiadał kompetencji reagowania na te naruszenia.

Podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów do tej pory w ogóle nie były prawnie obowiązane stosować środki bezpieczeństwa związane z usługami komunikacji interpersonalnej (pomijając kwestie związane z ochroną danych osobowych). Dlatego też nowością będzie dla nich obowiązek zgłaszania incydentów telekomunikacyjnych do CSIRT Telco, czy też obowiązek wprowadzenia środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa sieci lub usług. Obowiązek ten wynika wprost z dyrektywy EKŁE.

Podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić w ramach procesu zarządzania ryzykiem rekomendacje Pełnomocnika określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu cyberbezpieczeństwa systemów informacyjnych. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa.

Podmioty krajowego systemu cyberbezpieczeństwa, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych będą musiały wycofać sprzęt lub oprogramowanie, dostarczane przez dostawcę wysokiego ryzyka, z użycia w ciągu 5-7 lat.

Dobrowolny charakter certyfikacji sprawia, że nie dojdzie do zmiany obciążeń regulacyjnych spoczywających na przedsiębiorcach. Uczestnicy krajowego systemu certyfikacji cyberbezpieczeństwa będą musieli stosować przepisy niniejszej ustawy związane z kontrolą zarówno ze strony Polskiego Centrum Akredytacji, jak i ministra właściwego do spraw informatyzacji. Udział w tym systemie jest jednak całkowicie dobrowolny.

Zmiany dot. strategicznej sieci bezpieczeństwa

- Operator strategicznej sieci bezpieczeństwa będzie zarządzał strategiczną siecią bezpieczeństwa. Cena za usługi świadczone przez operatora strategicznej sieci bezpieczeństwa uwzględni koszt usługi powiększony o rozsądną marżę. OSSB przekaże Prezesowi UKE informacje o zawartej umowie na świadczenie usług za pośrednictwem strategicznej sieci bezpieczeństwa w terminie 14 dni od dnia zawarcia umowy.
- Prezes UKE będzie mógł przeprowadzić dokonywać analizę cen usług telekomunikacyjnych stosowanych przez operatora strategicznej sieci bezpieczeństwa
- Operator sieci zapewnia operatorowi strategicznej sieci bezpieczeństwa dostęp do infrastruktury technicznej w celu realizacji zadań związanych ze strategiczną siecią bezpieczeństwa.
- Użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa, jednostka samorządu terytorialnego, oraz właściciel lub zarządca nieruchomości zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do nieruchomości, w tym do budynku, polegający na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej

- OSSB przysługuje prawo pierwokupu sieci telekomunikacyjnych będących własnością
  - Skarbu Państwa lub innych państwowych osób prawnych;
  - jednostek samorządu terytorialnego.
- W sytuacji szczególnego zagrożenia, w przypadku pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703 –713 MHz i 758–768 MHz, Prezes UKE będzie mógł nakazać podmiotowi dysponującemu rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz udostępnienie zasobów częstotliwości z tego zakresu Operatorowi strategicznej sieci bezpieczeństwa.

9. Wpływ na rynek pracy

Jednym z najatrakcyjniejszy rynków rozwoju dla polskich firm technologicznych jest sektor cyberbezpieczeństwa. Związane jest to w szczególności z wydarzeniami takimi jak wybuch pandemii Covid-19 czy wojna w Ukrainie, co z kolei przekłada się na zwiększoną liczbę przeprowadzonych cyberataków. Wzrasta wobec tego zapotrzebowanie na zabezpieczenie urządzeń oraz wprowadzenie rozwiązań mających na celu m.in. ochronę danych. W 2021 roku odnotowano dwukrotny wzrost globalnych inwestycji dbających o bezpieczeństwo w sieci. Skala i stopień skomplikowania zagrożeń rosną lawinowo, w efekcie czego zwiększył się popyt na specjalistów IT zajmujących się cyberbezpieczeństwem – zarówno w ramach przedsiębiorstwa jak i outsourcingu. Proces cyfryzacji, a także dynamiczny rozwój ataków w cyberprzestrzeni skutkuje jednak niedoborem wykwalifikowanych pracowników w sektorze cyberbezpieczeństwa.

Projekt wywiera wpływ na rynek pracy poprzez wygenerowanie konieczności zatrudnienia wysoko wykwalifikowanych specjalistów zajmujących się cyberbezpieczeństwem. Pojawi się ponadto okazja do rekwalifikacji kadr, a także systemowego podnoszenia kompetencji i wiedzy osób zatrudnionych w podmiotach krajowego systemu cyberbezpieczeństwa. Szkolenia i certyfikacje są bowiem kluczowymi sposobami na rozwiązanie problemów z lukami w umiejętnościach. Co więcej, działania szkoleniowe mogą stanowić odpowiedź na braki kadrowe. Ustawa umożliwi ponadto rozwój przedsiębiorstw zajmujących się ochroną systemów informacyjnych. Działania w postaci zatrudnienia oraz rekwalifikacji i podnoszenia kompetencji mają szczególne znaczenie z racji tego, że dysponowanie wysoko wykwalifikowaną kadrą jest niezbędne z punktu widzenia zapewnienia bezpieczeństwa państwa. Sektor cyberbezpieczeństwa stanowi jeden z najatrakcyjniejszych rynków rozwoju dla polskich firm technologicznych. W 2021 roku odnotowano ponad dwukrotny wzrost globalnych inwestycji w tym startupy dbające o bezpieczeństwo w sieci. Cyberprzestępstwa wskazywane są jako jedne z pięciu najistotniejszych zagrożeń dla firm obok m.in. katastrof naturalnych. Na tak szybko zmieniającym się rynku certyfikaty w zakresie cyberbezpieczeństwa będą cenną pomocą, co do wyboru określonych produktów ICT. Przyczyni się to do większego wykorzystania bezpiecznych rozwiązań w sektorze przedsiębiorstw.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☒ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☒ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Ustawa zwiększy poziom bezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, w tym spółek Skarbu Państwa i jednostek samorządu terytorialnego. Projekt spełnia wymagania interoperacyjności, czyli zdolności systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach. Projekt spełnia również wymogi neutralności technologicznej, wykorzystania danych z rejestrów publicznych oraz ochrony danych osobowych. Ustawa wprowadza administracyjne kary za niedostosowanie się do obowiązków wynikających z przepisów nowelizujących ustawę o krajowym systemie cyberbezpieczeństwie. Skargi na decyzje administracyjne o nałożeniu kary będą rozpatrywane przez sądy administracyjne. Trudno jest oszacować, ile może być nałożonych kar, a co za tym idzie, nie jest możliwe oszacowanie liczby postępowań sądowo-administracyjnych wszczętych na podstawie skarg na te decyzje. W zakresie skarg na działalność jednostek certyfikacyjnych należy wskazać, że będą to pojedyncze sprawy. Należy zauważyć, że wciąż nie został przyjęty ani jeden z europejskich programów certyfikacji cyberbezpieczeństwa. Przewiduje się, że od przyjęcia programu na poziomie Unii Europejskiej do osiągnięcia zdolności jednostek certyfikacyjnych do przeprowadzania certyfikacji upłynie około 6 miesięcy. Pierwszy z Europejskich Programów certyfikacji cyberbezpieczeństwa – European Union Common Criteria przewiduje certyfikację systemów na zgodność z normami określonymi w systemie common criteria. Tego typu certyfikacja trwa zwykle ok. 12 miesięcy. Z tego względu pierwszych spraw z tego zakresu możemy spodziewać się dopiero w 2024 roku. Równocześnie odnosząc się do zbliżonych procesów certyfikacji prowadzonych obecnie należy zauważyć, że w krajach porównywalnych do Polski takich jak Hiszpania, Szwecja czy Włochy prowadzonych jest około 20 takich certyfikacji rocznie. Przyjmując, że w 5% z nich dojdzie do sporu, który będzie rozwiązywany na drodze sądowej to w skali roku będzie to 1 sprawa sądowa. Z tego względu wskazaliśmy, że przewiduje się potencjalne, pojedyncze sprawy wynikające z tych przepisów.

11. Planowane wykonanie przepisów aktu prawnego

Ustawa wejdzie w życie po upływie 6 miesięcy od dnia ogłoszenia. Ze względu na związki treściowe niniejsza ustawa powinna wejść w życie w tym samym dniu co ustawa - Prawo komunikacji elektronicznej.

Z chwilą wejścia w życie ustawy:

1) wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej staną się SOC wewnętrznymi;
2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę staną się SOC zewnętrznymi;
3) sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym stanie się CSIRT sektorowym;
4) podmioty publiczne wyznaczą osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy;
5) organy właściwe do spraw cyberbezpieczeństwa będą miały 18 miesięcy na ustanowienie CSIRT sektorowego;

6) operatorzy usług kluczowych będą zobowiązani do korzystania z systemu S46;
7) Podjęte zostaną działania w celu wyznaczenia operatora strategicznej sieci bezpieczeństwa.

W zakresie utworzenia CSIRT sektorowych oraz CSIRT Telco pierwszym krokiem będzie zaplanowanie budowy takiej instytucji – wybranie podmiotu, który będzie realizował to zadanie, zaplanowanie budżetu, określenie liczby etatów, zaplanowanie struktury zespołu. Następnie konieczne będzie zapewnienie lokalizacji, sprzętu, oprogramowania, rekrutacja kadr. Po uzyskaniu zdolności operacyjnej nastąpi ogłoszenie tej informacji w Dzienniku Urzędowym Rzeczypospolitej Polskiej „ Monitor Polski" – od tego momentu operatorzy usług kluczowych będą zgłaszać incydenty do danego CSIRT sektorowego. Niezależnie od tego powinna być przeprowadzona akcja informacyjna w ramach sektora – spotkania, konferencje mające przybliżyć zespół CSIRT a także budować zaufanie między operatorami a zespołem.

Ostrzeżenie oraz postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będą stosowane w razie zaistnienia potrzeby.

W zakresie certyfikacji pierwszym krokiem jest stworzenie jednolitych procedur akredytacji i certyfikacji na potrzeby cyberbezpieczeństwa. Równocześnie utworzony zostanie organ nadzoru, który będzie monitorował rozwój rynku certyfikacji. Odpowiednie działania zostaną podjęte w Ministerstwie Cyfryzacji. Zatrudnione zostaną dodatkowe osoby, które będą prowadziły postępowania administracyjne oraz przeprowadzały kontrole zgodnie z niniejszą ustawą.

Przyznanie uprawnień akredytacyjnych, w tym zakresie, Polskiemu Centrum Akredytacji pozwoli w możliwie krótkim horyzoncie czasowym rozpocząć akredytację jednostek certyfikacyjnym i jednostek oceniających zgodność.

Organ nadzoru będzie również w stanie określić, czy istnieje potrzeba wprowadzenia krajowych programów certyfikacyjnych. Początkowo certyfikacja odbywać się będzie w ramach europejskich programów certyfikacji.

Szef Agencji Wywiadu będzie zobowiązany utworzyć CSIRT INT po wejściu w życie ustawy.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane będą następujące mierniki:

1) liczba powstałych CSIRT sektorowych;
2) liczba wydanych ostrzeżeń;
3) liczba akredytowanych jednostek oceniających zgodność;
4) liczba wydanych certyfikatów i wystawionych deklaracji zgodności.

Dzięki obowiązkowi sprawozdawania się przez CSIRT sektorowe oraz CSIRT Telco Pełnomocnik Rządu do spraw Cyberbezpieczeństwa będzie w stanie dokonać oceny ich funkcjonowania, w ramach jego kompetencji do oceny funkcjonowania krajowego systemu cyberbezpieczeństwa. W szczególności wzięte pod uwagę zostaną takie kwestie jak liczba zgłoszonych incydentów do danego CSIRT w tym liczba zgłoszonych incydentów poważnych/poważnych incydentów telekomunikacyjnych, czas reagowania na incydenty a także pozostała działalność CSIRT sektorowego/CSIRT Telco – liczba przeprowadzonych działań edukacyjnych wśród operatorów usług kluczowych oraz przedsiębiorców komunikacji elektronicznej.

Monitorowana będzie liczba poważnych incydentów telekomunikacyjnych, a także przyczyny ich wystąpienia.

Ewaluacja nastąpi w dwa lata po wejściu ustawy w życie, a następnie będzie prowadzona cyklicznie, co dwa lata.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

1. Analiza - Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie
2. Wyliczenia wzrostu kwoty na dotację celową na utrzymanie i rozwój systemu teleinformatycznego S46.

Zał. nr 1 do OSR

Dostawca wysokiego ryzyka (high risk vendor) i bezpieczeństwo sieci 5G w Europie

Austria 2
Belgia 3
Bułgaria 4
Chorwacja 4
Cypr 4
Czechy 4
Dania 5
Estonia 6
Finlandia 8
Francja 8
Grecja 9
Hiszpania 9
Irlandia 10
Litwa 11
Luksemburg 12
Łotwa 12
Malta 13
Niderlandy 13
Niemcy 14
Portugalia 17
Rumunia 17
Słowacja 18
Słowenia 19
Szwecja 20
Wielka Brytania 20
Węgry 21
Włochy 21

Austria

W zakresie bezpieczeństwa sieci 5G kluczowym aktem prawnym jest austriackie rozporządzenie w sprawie bezpieczeństwa sieci[1)] z 2020 roku. Zgodnie z nim na operatorów telekomunikacyjnych, posiadających ponad 100 000 abonentów, nałożono liczne obowiązki informacyjne, w tym obowiązek przedstawiania na uzasadnione żądanie organu regulacyjnego wykazu funkcji i producentów urządzeń wykorzystywanych do obsługi sieci 5G oraz, w stosownych przypadkach, innych komponentów przez nich wykorzystywanych. Ponadto, muszą oni:

1. prowadzić Sieciowe Centra Operacyjne (NOC), jak również Centra Operacyjne Bezpieczeństwa (SOC) we własnych obiektach na terenie Unii Europejskiej;
2. skutecznie monitorować przez NOC/SOC wszystkie krytyczne elementy sieci 5G, w celu wykrywania anomalii oraz identyfikacji i zapobiegania zagrożeniom;
3. zarządzać ruchem sieciowym lub usługami komunikacyjnymi, w celu zapobiegania nieuprawnionym nieautoryzowanym zmianom w komponentach sieci lub usług;
4. zapewniać ochronę fizyczną krytycznych komponentów sieci i sieci 5G z zastosowaniem podejścia opartego na analizie ryzyka w przypadku wielodostępowych komputerów brzegowych (MEC) i stacji bazowych;
5. zapewnić, aby dostęp do sieci miał wyłącznie wykwalifikowany personel, który przeszedł kontrolę bezpieczeństwa, a dostęp osób trzecich był ograniczony i monitorowany;
6. stosować odpowiednie narzędzia i procesy w celu zapewnienia integralności oprogramowania, w szczególności aktualizować oprogramowanie oraz likwidować wykryte podatności;
7. posiadać strategię wielu dostawców uwzględniającą ograniczenia techniczne i wymogi interoperacyjności różnych części sieci 5G.

W załączniku do tego rozporządzenia została określona lista funkcji komponentów sieci 5G[2)].

[1)] https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Text-BGBLA_2020_II_301.pdf .
[2)] https://www.rtr.at/TKP/aktuelles/veroeffentlichungen/veroeffentlichungen/Verordnungen/TKNSiV-Anhang2.pdf .

Federalny Minister Rolnictwa, Regionów i Turystyki może ze względów bezpieczeństwa narodowego zakwalifikować, w drodze decyzji, producentów elementów sieci łączności elektronicznej lub dostawców usług dla takich sieci, w każdym przypadku, z wyjątkiem sieci nadawczych w rozumieniu federalnej ustawy o radiofonii i telewizji (BVG-Rundfunk), jako dostawców wysokiego ryzyka.

Taki dostawca jest wykluczony

- z dostaw składników istotnych dla bezpieczeństwa lub składników sieciowych dla sieci oraz
- ze świadczenia usług związanych z bezpieczeństwem sieci.

Tego typu decyzja może obowiązywać maksymalnie 2 lata.

Prawo austriackie w zakresie czynników wpływających na uznanie za dostawcę wysokiego ryzyka nie odnosi się wprost do kwestii wpływu państw trzecich na dostawcę.

Belgia

Nie posiada konkretnych regulacji dotyczących dostawców wysokiego ryzyka.

Najwięksi operatorzy telekomunikacyjni w tym kraju – Orange i Proximus – zawarli umowę z Nokią na rozwój sieci 5G[3)].

Istnieje projekt zmian w systemie prawnym przewidujący procedurę autoryzacji dla sprzętu wykorzystywanego w sieci 5G. Wnioski w tym zakresie będzie trzeba zgłaszać do ministra, który będzie wydawał decyzje przy autoryzacji.

Będą przy tym brane pod uwagę czynniki związane z dostawcą takie jak:

- powiązania z rządami państw trzecich;
- prawo lub sytuacja w kraju dostawcy, w szczególności w przypadku braku nadzoru demokratycznego lub legislacyjnego;
- funkcjonowanie konwencji o ochronie danych lub bezpieczeństwa między Unią Europejską a danym państwem;
- zdolność danego państwa do wywierania jakiejkolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
- zdolność dostawcy do zabezpieczenia dostaw;

[3)] https://www.telko.in/le-soir-belgijskie-orange-i-proximus-wybrali-europejskich-partnerow-w-5g.

- ogólna jakość produktów lub usług oraz praktyki bezpieczeństwa dostawcy, w tym stopień kontroli nad jego własnym łańcuchem dostaw oraz czy praktyki bezpieczeństwa są odpowiednio traktowane priorytetowo.

Bułgaria

Obecne przepisy prawa komunikacji elektronicznej w Bułgarii nakładają jedynie ogólny obowiązek zapewniania bezpieczeństwa sieci telekomunikacyjnych oraz szacowania ryzyka[4)]. Kwestie dostawcy wysokiego ryzyka są na razie na etapie opracowywania przepisów w ramach planowanych zmian w prawie komunikacji elektronicznej. Proponowane zasady nie zostały jeszcze opublikowane.

Chorwacja

Na razie nie wprowadziła żadnych regulacji w zakresie HRV. Nie ujawniono też informacji o planowanej legislacji.

Cypr

Funkcjonuje tam regulacja dotycząca oceny ryzyka dostawców. Podstawą dla niej jest decyzja cypryjskiego organu ds. cyberbezpieczeństwa, która reguluje szczegóły związane z oceną ryzyka dostawców – przypomina ona rozporządzenie z naszego porządku prawnego[5)]. W ramach cypryjskiej ustawy o bezpieczeństwie sieci i systemów informacyjnych[6)] implementowano przepisy Europejskiego Kodeksu Łączności Elektronicznej dotyczące bezpieczeństwa sieci.

W ramach kryteriów branych pod uwagę przy ocenie dostawców są również czynniki strategiczne.

Czechy

Czechy regulują kwestię bezpieczeństwa sieci 5G i szerzej bezpieczeństwa łańcuchów dostaw w ramach ustawy o cyberbezpieczeństwie i zmianie ustaw powiązanych[7)]. Ustawa ta nakłada na operatorów telekomunikacyjnych oraz operatorów innych kluczowych usług ogólny obowiązek uwzględniania wymagań wynikających ze środków bezpieczeństwa przy wyborze

[4)] https://www.lex.bg/laws/ldoc/2135553187.
[5)] https://dsa.cy/images/pdf-upload/Decision-408-2020.pdf.
[6)] https://dsa.cy/images/pdf-upload/DSA-Law-89-I-2020.pdf.
[7)] https://nukib.cz/download/publications_en/legislation/EN_Decree-82-2018_v1.3_final.pdf.

dostawców dla ich systemów informacyjnych lub komunikacyjnych oraz do uwzględnienia tych wymagań w umowie, którą zawierają z dostawcą. Uwzględnianie wymogów wynikających ze środków bezpieczeństwa zgodnie ze zdaniem pierwszym w zakresie niezbędnym do spełnienia wymogów zgodnie z niniejszą ustawą nie jest uznawane za niezgodne z prawem ograniczenie konkurencji lub nieuzasadnioną barierę dla konkurencji.
W lutym 2022 roku czeski CSIRT wystosował rekomendacje dotyczące oceny wiarygodności dostawców technologii dla sieci 5G w Republice Czeskiej[8)]. Nie są one wiążące, ale podmioty, na które nałożone są ogólne obowiązki zapewniania cyberbezpieczeństwa powinny brać je pod uwagę.
W tym dokumencie wskazane zostało, że na wiarygodność dostawców wpływają następujące czynniki:

- rezydowanie lub podleganie prawu w demokratycznym państwie;
- naruszanie prawa międzynarodowego, w szczególności jeśli zostały przeciwko nim skierowane rezolucje Rady Bezpieczeństwa Organizacji Narodów Zjednoczonych lub restrykcyjne środki wspólnej polityki zagranicznej i bezpieczeństwa Unii Europejskiej;
- prowadzenie działań sprzecznych z podstawowymi interesami Republiki Czeskiej lub jej państw sprzymierzonych;
- nieznajdowanie się pod niewłaściwym wpływem obcego rządu lub organu administracji państwowej i możliwość zapewnienia dostępności, integralności i wiarygodności danych w dostarczanych rozwiązaniach technologicznych z odpowiednim stopniem autonomii;
- spełnianie norm bezpieczeństwa, które są powszechne na rynku w momencie dostawy i jest skłonny zobowiązać się do ich spełniania w przyszłości;
- prowadzenie działalności gospodarczej zgodnie z międzynarodowymi praktykami handlowymi oraz to, że nie czerpie nieproporcjonalnych korzyści od państwa, w którym zamieszkuje lub pod którego wpływy podlega.

Dania

Kwestie dostawcy wysokiego ryzyka zostały uregulowane w Ustawie o bezpieczeństwie dostawców w krytycznej infrastrukturze telekomunikacyjnej[9)]. Zgodnie z nią Centrum

[8)] https://nukib.cz/download/aktuality/5G-Recommendation_EN.pdf.
[9)] https://www.retsinformation.dk/api/pdf/223450.

Cyberbezpieczeństwa może zakazać dostawcy publicznych usług telekomunikacyjnych zawarcia umowy lub nakazać odstąpienie od umowy, która stwarza zagrożenie dla bezpieczeństwa narodowego.

Przy ocenie czy umowa stwarza takie zagrożenie, Centrum bierze pod uwagę cechy kontrahenta takie, jak:

- wpływ jego poddostawców i podmiotów mogących wywierać kontrolę na danego przedsiębiorcę;
- pochodzenie z kraju, który nie ma zawartej umowy związanej z bezpieczeństwem z Danią, bądź nie gwarantuje współpracy w obszarze bezpieczeństwa;
- bycie kontrolowanym, pośrednio lub bezpośrednio, przez obcy rząd;
- historia zaangażowania w działania w Danii lub innych krajach, które spowodowały zagrożenie dla bezpieczeństwa narodowego, bezpieczeństwa informacji lub porządku publicznego.

Centrum może nakazać ww. środki tylko, gdy bezpieczeństwa narodowego nie da się zapewnić w inny sposób. Decyzja Centrum może prowadzić do wywłaszczenia własności prywatnej za odszkodowaniem.

Taka decyzja może być zaskarżona do sądu. W ramach procesu sądowego powoływany jest specjalny adwokat, który ma mieć dostęp do dokumentów będących podstawą ww. decyzji. Te dokumenty nie są ujawniane bezpośrednio stronie. Jednakże minister obrony może wskazać, że niektóre dokumenty nie będą przedstawione temu specjalnemu przedstawicielowi.

Estonia

Estonia wprowadziła kwestie bezpieczeństwa sieci 5G do swojego porządku prawnego w ramach wdrażania Europejskiego Kodeksu Łączności Elektronicznej[10)]. Akt ten zobowiązuje operatorów telekomunikacyjnych do stosowania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa swoim sieciom oraz do szacowania ryzyka w tym obszarze. Zgodnie z dodawanym art. 87^3 sprzęt lub oprogramowanie używane w sieci telekomunikacyjnej nie może powodować zagrożenie dla bezpieczeństwa

[10)] https://www.riigiteataja.ee/en/eli/501042015003/consolide.

narodowego[11)]. Przy ocenie sprzętu lub oprogramowania wysokiego ryzyka bierze się pod uwagę m.in. informacje o tym czy:

1) lokalizacja lub siedziba znajduje się w państwie (dalej: państwo lokalizacji), które nie jest członkiem Unii Europejskiej, Organizacji Traktatu Północnoatlantyckiego (dalej: NATO) lub państwem członkowskim Organizacji Współpracy Gospodarczej i Rozwoju (dalej: OECD);

2) w państwie pochodzenia nie są przestrzegane zasady demokratycznego państwa prawa lub nie są przestrzegane prawa człowieka;

3) w państwie przyjmującym nie jest chroniona własność intelektualna, dane osobowe lub tajemnice handlowe osób z innego państwa;

4) państwo pochodzenia zachowuje się agresywnie w cyberprzestrzeni;

5) państwa członkowskie Unii Europejskiej, NATO lub OECD przypisały cyberataki państwu pochodzenia;

6) podlega władzy rządowej lub państwowej państwa pochodzenia lub innego obcego państwa bez niezależnej kontroli sądowej;

7) państwo pochodzenia lub inne obce państwo może zobowiązać go do działania w sposób zagrażający bezpieczeństwu państwa estońskiego;

8) działalność gospodarcza nie jest oparta na konkurencji rynkowej lub w kraju pochodzenia nie stworzono do tego celu wystarczających warunków;

9) struktura własności, struktura organizacyjna lub struktura zarządzania nie jest przejrzysta;

10) finansowanie nie jest przejrzyste;

11) produkty lub usługi zawierają słabe punkty bezpieczeństwa i nie wdrożono odpowiednich środków bezpieczeństwa w celu ich wyeliminowania;

12) nie jest konsekwentnie w stanie zapewnić dostaw produktów lub usług, z wyjątkiem przypadków spowodowanych siłą wyższą.

Sprzęt, który zostanie uznany za stanowiący zagrożenie będzie mógł być wykorzystywany tylko po uzyskaniu zgody odpowiedniego organu. W przypadku obecnie wykorzystywanych urządzeń wprowadzono kilka kategorii sprzętu w zależności od jego funkcji. Danym kategoriom wyznaczono terminy w jakich mogą być użytkowane bez potrzeby uzyskania pozwolenia.

Przepisy te wejdą w życie 3 września 2022 r.

[11)] riigiteataja.ee/akt/ESS.

Finlandia

Kluczowymi fińskimi aktami prawnymi w tym obszarze są Prawo Komunikacji Elektronicznej[12)] oraz Rozporządzenie Agencji Transportu i Komunikacji w sprawie krytycznych części sieci łączności[13]. Rozporządzenie to zawiera listę funkcji krytycznych w sieci 5G. Z kolei Prawo Komunikacji Elektronicznej przewiduje, że urządzenie sieci komunikacyjnej nie może być używane w krytycznych częściach publicznej sieci komunikacyjnej, jeżeli istnieją poważne podstawy do podejrzeń, że użycie urządzenia zagrażałoby bezpieczeństwu narodowemu lub obronie narodowej w taki sposób, że użycie to umożliwiłoby działania obcego wywiadu lub działania, które zakłóciłyby, sparaliżowały lub w inny sposób negatywnie wpłynęły na ważne interesy Finlandii, podstawowe funkcje społeczeństwa lub demokratyczny porządek społeczny. Agencja Transportu i Łączności może zobowiązać właściciela lub innego posiadacza sieci łączności do usunięcia urządzenia sieci łączności z krytycznych części jego sieci.

Powołana została również Rada doradcza ds. bezpieczeństwa sieci, w której zasiadają zarówno przedstawiciele administracji publicznej, jak i biznesu, która będzie prezentować rekomendacje organom rządowym.

Francja

1. W celu zagwarantowania bezpieczeństwa i obrony narodowej w ustawie „LOI n° 2019-810" wprowadza się przepis o wcześniejszej kontroli wszelkiej działalności polegającej na eksploatacji niektórych urządzeń radioelektrycznych w sieciach 5G. Operatorzy będą musieli składać wniosek o zezwolenie do premiera. Premier udzieli odpowiedzi w terminie dwóch miesięcy od dnia otrzymania pełnej dokumentacji wniosku.

Ustali, czy istnieje poważne ryzyko naruszenia interesów w obszarze obrony i bezpieczeństwa narodowego na podstawie kryteriów określonych w ustawie, a zwłaszcza w świetle gwarancji, jakie dają urządzenia co do integralności, bezpieczeństwa, dostępności sieci lub poufności przekazywanych wiadomości i informacji powiązanych z komunikacją.

W razie niespełniania jednego z tych kryteriów wniosek o zezwolenie może zostać odrzucony przez premiera. Aby ocenić ryzyko, uwzględnia się zasady budowy i eksploatacji wprowadzone przez operatora, poziom bezpieczeństwa urządzenia i fakt, czy operator lub

[12)] https://www.finlex.fi/fi/laki/ajantasa/2014/20140917#O9L29P244a.
[13)] https://finlex.fi/data/normit/47015/Regulation_on_critical_parts_of_a_communications_network.pdf.

jego usługodawcy, w tym podwykonawcy, podlegają lub nie podlegają kontroli lub ingerencji państwa niebędącego członkiem Unii Europejskiej.

2. Budowa sieci 5G zwiększa ryzyko w obszarze cyberbezpieczeństwa związane z urządzeniami sieci ze względu na:

(1) szczególny charakter techniczny sieci 5G (dynamiczne zarządzanie siecią dostępu, wprowadzenie jednostek przetwarzania informacji na końcówkach sieci – edge computing), oraz

(2) przypadki używania sieci 5G w dziedzinach przemysłowych, w niektórych gałęziach o znaczeniu krytycznym (np. pojazd podłączony / pojazd autonomiczny, przemysł przyszłości, sieć elektroenergetyczna itp.).

To zwiększone ryzyko wpływa na nowe wymogi w obszarze bezpieczeństwa w odniesieniu do urządzeń, które będą wspierać przyszłe sieci 5G, dotyczące zarówno ich cech technicznych, jak i zobowiązań prawnych, które mogą zmuszać dostawców do współpracy z obcymi organami w gromadzeniu informacji.

Mając na uwadze te nowe obawy dotyczące bezpieczeństwa i najnowsze zmiany w planach budowy sieci 5G niektórych francuskich operatorów telekomunikacyjnych, które mogą zagrażać bezpieczeństwu narodowemu Francji, przyjęto ustawę o bezpieczeństwie sieci. Celem jest ustanowienie wcześniejszego systemu zezwoleń na urządzenia sieci radioelektrycznych.

Przepisy francuskie wpisują się również w skoordynowane działania na szczeblu Unii Europejskiej zainicjowane przez Komisję Europejską.

Ustawa ta zapewnia ochronę ruchomych sieci radiowych przed zagrożeniami szpiegostwa, piractwa i sabotażu.

Grecja

Obecnie prowadzone są prace nad ustawą w tym zakresie. Wciąż nie zostały określone szczegóły związane z HRV.

Hiszpania

Prace nad regulacją dotyczącą dostawcy wysokiego ryzyka wciąż trwają. Obecnie procedowany jest projekt Ustawy o wymogach zapewnienia bezpieczeństwa sieci i usług[14)].

[14)] https://avancedigital.mineco.gob.es/es-es/Participacion/Documents/5G_audiencia/Texto_APL_ciberseguridad_5G.pdf?csf=1&e=48JHOH.

Ma on nałożyć na operatorów telekomunikacyjnych m.in. obowiązek szacowania i zarządzania ryzykiem w obszarze 5G oraz stosowania odpowiednich środków technicznych i organizacyjnych w celu zabezpieczenia sieci. Ustawa przewiduje, że rząd będzie mógł dokonywać oceny dostawców. Przy dokonywaniu takiej oceny mają być brane pod uwagę następujące czynniki:

a) powiązania dostawców i ich łańcucha dostaw z rządami państw trzecich;

b) skład kapitału zakładowego i struktura organów dostawcy;

c) uprawnienie państwa trzeciego do wywierania nacisku na wyniki lub lokalizację przedsiębiorstwa;

d) cechy reżimu politycznego państwa pochodzenia dostawcy i jego polityki w zakresie cyberbezpieczeństwa, takie jak:

- charakterystyka reżimu politycznego państwa trzeciego i jego polityki cyberbezpieczeństwa;
- umowy o współpracy w dziedzinie bezpieczeństwa, umowy o współpracy w zakresie cyberbezpieczeństwa, cyberprzestępczości lub ochrony danych podpisane z danym państwem trzecim, jak również traktaty międzynarodowe dotyczące tych dziedzin, których stroną jest to państwo;
- stopień zgodności jego przepisów o ochronie danych osobowych z przepisami unijnymi w tym zakresie.

Ustawa przewiduje trzy poziomy ryzyka jakie można przypisać dostawcy. Szczegółowe obowiązki mają być nakładane na operatorów telekomunikacyjnych w drodze aktów wykonawczych (schematów bezpieczeństwa sieci i usług 5G), które szczegółowo będą określały środki techniczne i organizacyjne jakie będą musieli przyjąć. W takim schemacie może być nałożony obowiązek zmiany dostawcy oraz inne obowiązki związane z bezpieczeństwem łańcucha dostaw.

Irlandia

Trwają prace nad przepisami implementującymi Toolbox 5G – obecnie Irlandczycy analizują wyniki przeprowadzonych konsultacji publicznych[15)]. Ocena ryzyka dostawcy ma być jednym z obowiązków jakie zostaną nałożone na operatorów telekomunikacyjnych obok analizy

[15)] https://www.gov.ie/pdf/?file=https://assets.gov.ie/205231/36cba263-8a62-4777-a314-74d4685741d5.pdf#page=null .

swojego łańcucha dostaw i unikania podatności. Ze środków nietechnicznych operatorzy, przy dokonywaniu oceny, mają brać pod uwagę:

- praktyki biznesowe dostawcy;
- związki pomiędzy dostawcą a państwem spoza UE;
- ramy prawne i regulacyjne w kraju, w którym dostawca ma główną siedzibę;
- zdolność dostawcy do zapewnienia ciągłości dostaw;
- poprzednią historię bezpieczeństwa i przejrzystości dostawcy.

Litwa

Rząd lub upoważniony przez niego organ określa kryteria, zgodnie z którymi uznaje się, że przedsiębiorstwo świadczy usługi mobilne piątej generacji (5G) lub zarządza infrastrukturą niezbędną do świadczenia takich usług.

Na Litwie zobowiązanie do wyeliminowania niezaufanych dostawców oprogramowania i sprzętu z sieci 5G zostało ujęte jako jeden ze strategicznych celów nowego programu rządowego, zatwierdzonego w marcu 2021 r. 25 maja 2021 r. litewski parlament jasno zadeklarował, że Litwa nie chce należeć do technosfery kontrolowanej przez Chiny i wprowadził zmiany do istniejących ram prawnych, które umożliwiają rządowi uniemożliwienie udziału nierzetelnych dostawców w rynku komunikacji elektronicznej. Jednym z głównych kryteriów przy definiowaniu zaufanego producenta jest to, czy jest on (lub jego beneficjent) zarejestrowany w kraju NATO, Unii Europejskiej lub EOG i/lub Organizacji Współpracy Gospodarczej i Rozwoju (OECD). Kryterium to dotyczy firmy telekomunikacyjnej, dostawcy sprzętu oraz dostawcy usług utrzymania sprzętu, co oznacza, że na rynku komunikacji elektronicznej nie mogą uczestniczyć tzw. firmy z krajów trzecich. Litewskie Narodowe Centrum Cyberbezpieczeństwa[16)] (NCSC) będzie odgrywać główną rolę w procesie weryfikacji zaufania do urządzeń, gdzie jedną z funkcji NCSC jest zapewnienie oceny bezpieczeństwa cybernetycznego konkretnych urządzeń i aplikacji w oparciu o potrzeby sektora prywatnego i publicznego. Między innymi na podstawie jego opinii litewski rząd będzie mógł wydać decyzję stwierdzającą, że inwestor stanowi potencjalne zagrożenie dla bezpieczeństwa narodowego. W przypadku wydania takiej decyzji inwestor nie może zawierać decyzji dotyczących obszarów, w których stanowi to zagrożenia do czasu

[16)] https://www.nksc.lt/en/.

aż ustanie powód, dla którego uznano go za zagrożenie. Decyzje w tej sprawie podejmuje Komisja Bezpieczeństwa Narodowego, w której skład wchodzą przedstawiciele administracji oraz służb specjalnych.

Ww. środki mogą być przedsięwzięte wobec producentów i dostawców sprzętu komputerowego, urządzeń lub oprogramowania wykorzystywanego w działalności związanej z łącznością elektroniczną i/lub dostawcy usług konserwacyjnych lub pomocniczych.

Luksemburg

Luksemburg nie zdefiniował w swoim prawie pojęcia dostawcy wysokiego ryzyka. Wprowadzone jednak zostały regulacje związane z ochroną sieci 5G w ramach ustawy implementującej Europejski Kodeks Łączności Elektronicznej[17)]. Zgodnie z tą ustawą w przypadku poważnego zagrożenia dla bezpieczeństwa sieci i usług, wpływającego na bezpieczeństwo narodowe, które jest spowodowane wykorzystywanym sprzętem lub oprogramowaniem, na wniosek ministra właściwego do spraw komunikacji elektronicznej i poczty, rząd może wprowadzić środki odnoszące się do tych urządzeń lub programów, w tym zakaz ich stosowania. W ustawie wpisano wprost, że zastosowanie tych środków nie rodzi uprawnień do jakichkolwiek roszczeń odszkodowawczych od rządu.

Powołany został również narodowy komitet telekomunikacji składający się z 20 przedstawicieli ministerstw i innych organów państw, który ma doradzać rządowi w zakresie środków opisanych powyżej.

Łotwa

Funkcjonują zasady związane z zawieraniem umów dotyczących systemów wysokiego ryzyka. Umowy ich dotyczące mogą zawierać tylko:

1) osoby prawne:

- mające siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;
- których rzeczywisty właściciel jest obywatelem państwa członkowskiego NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub jest obywatelem Republiki Łotewskiej;

[17)] https://legilux.public.lu/eli/etat/leg/loi/2021/12/17/a927/jo.

- producentem oprogramowania lub sprzętu wykorzystywanego przez nich do świadczenia usługi jest osoba prawna mająca siedzibę w państwie członkowskim NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego lub osoba fizyczna będąca obywatelem Republiki Łotewskiej lub obywatelem państwa NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego;

2) osoby fizyczne będące obywatelami Republiki Łotewskiej lub obywatelami państwa należącego do NATO, Unii Europejskiej lub Europejskiego Obszaru Gospodarczego.
Pomiot, który nie spełnia tych wymagań musi uzyskać zgodę organu odpowiedzialnego za bezpieczeństwo narodowe.

Malta

Malta stoi na stanowisku, że ryzyka związane z dostawcą wysokiego ryzyka, a zwłaszcza powiązane ze środkiem strategicznym SM03, nie stanowią realnego zagrożenia dla ich systemu. Na Malcie została wydana decyzja w sprawie przyznania częstotliwości[18], zgodnie z którą operatorzy telekomunikacyjni muszą szacować ryzyko i stosować adekwatne środki. Nie ma tam jednak bezpośrednich odniesień do dostawcy wysokiego ryzyka.

Niderlandy

W Niderlandach funkcjonuje kategoria dostawcy wysokiego ryzyka[19)]. Minister Sprawiedliwości i Bezpieczeństwa, nałoży na dostawcę publicznej sieci lub usługi łączności elektronicznej obowiązek wyłącznego korzystania, w wyznaczonych częściach jego sieci lub urządzeń towarzyszących, z produktów lub usług podmiotów innych niż podmiot wyznaczony przez Ministra.
Dostawcą Wysokiego Ryzyka jest podmiot, który:
a) jest państwem, podmiotem lub osobą, o której wiadomo lub co do której istnieją podstawy do podejrzeń, że zamierza ona niewłaściwie korzystać z sieci łączności elektronicznej lub usług oferowanych w Niderlandach lub zakłócać ich działanie, lub

18)
https://www.mca.org.mt/sites/default/files/Assignment%20process%20for%20additional%20spectrum%20for%20wireless%20broadband%20electronic%20communications%20service.pdf .
19) https://wetten.overheid.nl/BWBR0042843/2020-03-01.

b) ma bliskie powiązania z państwem, podmiotem lub osobą, o których mowa w lit. a, lub jest podmiotem lub osobą, co do których istnieją podstawy do podejrzeń, że mają takie powiązania lub wpływ.

W przypadku, gdy produkty danego dostawcy są już wykorzystywane w funkcjonujących sieciach, minister wyznaczy termin na ich wymianę biorąc pod uwagę konieczność zapewnienia ciągłości świadczenia usług.

Niemcy

W Niemczech zaprezentowano aktualizację modelu dotyczącego cyberbezpieczeństwa z uwzględnieniem funkcjonowania sieci 5G. Podstawowe zasady funkcjonowania systemu zostały przedstawione w kwietniu 2020 r. w opracowaniu zatytułowanym **„Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)”[20].** Publikację przygotowały podmioty zajmujące się cyberbezpieczeństwem oraz rynkiem telekomunikacyjnym, w tym m.in. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahn.

Wśród uwzględnionych kwestii wskazano np.: katalog wymagań z zakresu cyberbezpieczeństwa, składniki infrastruktury telekomunikacyjnej dla 5G, komponenty systemu odpowiedzialne za realizację funkcji krytycznych, a także stworzono listę funkcji krytycznych odnoszących się m.in. do infrastruktury zapewniającej przekazywanie i przechwytywanie danych telekomunikacyjnych. Wiele uwagi poświęcono również procesowi certyfikacji gwarantującej, że dany komponent systemu spełnia określone wymagania z zakresu bezpieczeństwa, odwołując się w tym przypadku do obowiązujących już przepisów Unii Europejskiej oraz regulacji niemieckich. Ważnym aspektem jest ponadto wprowadzenie zasad odnoszących się bezpośrednio do dostawców, takich jak choćby ich różnorodność, wiarygodność, weryfikacja technologiczna czy zobowiązanie do wczesnego informowania o nowych produktach i usługach.

1. Nowe regulacje bezpieczeństwa zostały opublikowane przez niemiecki urząd Bundesnetzagentur (BNetzA), regulujący funkcjonowanie sektora

20) https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=6 .

telekomunikacyjnego. Według serwisu Tech Radar wprowadzają one dodatkowe wymagania wobec wszystkich firm, które będą chciały brać udział w budowie niemieckiej sieci łączności 5G. Według nowych przepisów producenci sprzętu zobowiązani są do certyfikowania krytycznych komponentów zgodnie z wymogami bezpieczeństwa ustalanymi przez niemieckie organy państwowe. Zobowiązani są również do zatrudniania w obszarach związanych z bezpieczeństwem jedynie kwalifikowanych pracowników, a także do ciągłego monitorowania procedur bezpieczeństwa. Niemiecka administracja wezwała również działające w kraju firmy telekomunikacyjne do dywersyfikacji dostawców sprzętu i "unikania monokultury".

2. Niemiecki rząd uchwalił projekt nowej ustawy dotyczącej bezpieczeństwa informatycznego. Ma ona umożliwić dokładne sprawdzenie wiarygodności dostawców komponentów dla systemów infrastrukturalnych o krytycznym znaczeniu, takich jak sieć 5G. Kwestia ta była przedmiotem ożywionych publicznych dyskusji w związku z ewentualnym uczestnictwem chińskich koncernów w budowaniu niemieckiej sieci 5G. W ustawie tej chodzi zdecydowanie o zagadnienia bezpieczeństwa informatycznego, a nie o poszczególnych producentów".

Zgodnie z brzmieniem ustawy producenci mają składać oświadczenia, w których będą musieli między innymi zadeklarować, czy i jak mogą zapewnić, by komponenty o krytycznym znaczeniu nie posiadały żadnych technicznych właściwości pozwalających na ich nadużywanie - „w szczególności na potrzeby sabotażu, szpiegowania lub terroryzmu poprzez wpływanie na bezpieczeństwo, integralność, dostępność lub zdolność funkcjonowania krytycznie ważnej infrastruktury". Minimalne wymogi bezpieczeństwa, jakie ma spełniać producent, określi federalne ministerstwo spraw wewnętrznych.

Gdyby okazał się on nie w pełni wiarygodny, na przykład nie zgłaszając użytkownikowi znanych sobie niedociągnięć systemu, będzie mu można wymówić współpracę. W razie utrzymującego się braku dowodów wiarygodności resortowi spraw wewnętrznych wolno będzie w porozumieniu z innymi zainteresowanymi ministerstwami zabronić dalszego użytkowania wszystkich pochodzących od tego producenta komponentów.

Projekt ustawy zawiera również nakaz zgłaszania przez zarządców krytycznej infrastruktury kierowanych przeciwko niej cyberataków. Wprowadza ponadto jednolitą formę wystawianych przez Federalny Urząd Bezpieczeństwa Techniki Informacyjnej (BSI)

certyfikatów bezpieczeństwa dla sprzętu - https://cyberdefence24.pl/polityka-i-prawo/niemcy-wzmacniaja-cyberbezpieczenstwo

3. W Niemczech Federalna Agencja ds. Sieci (Bundesnetzagentur – BnetzA) określiła bardzo konkretny katalog wymagań w zakresie bezpieczeństwa. Według zaostrzonych kryteriów, w szczególności pod lupę będą brane te elementy infrastruktury, które realizują tzw. funkcje krytyczne. Będą one musiały przejść przez proces certyfikacji, tj. po przeprowadzeniu odpowiedniej procedury technicznej zdobyć świadectwo, że dany komponent spełnia wymagania w zakresie bezpieczeństwa. - https://biznes.interia.pl/gospodarka/news-bezpieczenstwo-sieci-5g-kluczowe-dla-funkcjonowania-panstwa,nId,4732854#utm_source=paste&utm_medium=paste&utm_campaign=firefox.
4. 11 sierpnia 2020 r. Federalna Agencja ds. Sieci opublikowała aktualny projekt katalogu wymagań bezpieczeństwa dla obsługi systemów telekomunikacyjnych i przetwarzania danych oraz przetwarzania danych osobowych. Katalog został opracowany w porozumieniu z Federalnym Urzędem Bezpieczeństwa Informacji (BSI) oraz Federalnym Komisarzem ds. Ochrony Danych i Wolności Informacji (BfDI).

Katalog wymagań bezpieczeństwa dotyczy operatorów sieci telekomunikacyjnych i systemów przetwarzania danych oraz przetwarzania danych osobowych. Jest podstawą koncepcji bezpieczeństwa, uzgodnień technicznych i innych środków zwiększających bezpieczeństwo sieci i usług.

Katalog zawiera w szczególności krytyczne komponenty do certyfikacji:

a) deklaracje wiarygodności do uzyskania od producentów i dostawców systemów;
b) zapewnienie integralności produktu;
c) wprowadzenie monitoringu bezpieczeństwa;
d) zatrudnianie wyłącznie przeszkolonego i wykwalifikowanego personelu do pracy w obszarach związanych z bezpieczeństwem;
e) dostępność wystarczającej refundacji;
f) unikanie monokultur.

Katalog zawiera dodatkowe wymagania bezpieczeństwa dla publicznych sieci i usług telekomunikacyjnych o wysokim poziomie ryzyka. W związku z tym należy stworzyć listę

funkcji krytycznych dla infrastruktur o wysokim poziomie ryzyka. Te krytyczne funkcje zostaną wymienione w dokumencie sporządzonym wspólnie z BSI.

W przyszłości lista funkcji krytycznych ma być stale aktualizowana i poprawiana. Uwzględniono i są brane pod uwagę wyniki międzynarodowych analiz, np. Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) czy Organu Europejskich Regulatorów Łączności Elektronicznej (BEREC).

Następujące funkcje są uważane za krytyczne:

a) zarządzanie abonentami i mechanizmami kryptograficznymi (jeśli jest to element sieci);
b) interfejsy międzysieciowe;
c) zarządzane usługi sieciowe;
d) zarządzanie wirtualizacją funkcji sieciowych i orkiestracja sieci (MANO), a także wirtualizacja;
e) systemy zarządzania i inne systemy wsparcia;
f) kontrola transportu i przepływu informacji;

Portugalia

Obecnie wciąż trwają prace nad przepisami wprowadzającymi Toolbox 5G. Nie funkcjonują w związku z tym przepisy dotyczące HRV. Obecnie obowiązuje rozporządzenie nr 303/2019[21)], które zawiera ogólne obowiązki związane z zapewnieniem bezpieczeństwa. Ten akt prawny zwraca szczególną uwagę na kwestie przeprowadzenia oceny własnych zasobów i dostosowaniu do nich środków bezpieczeństwa. Jego sformułowania przypominają normę 27001.

W ramach warunków aukcji 5G wskazano, że posiadacze nabytych częstotliwości będą podlegali obowiązkom wynikającym z implementacji Europejskiego Kodeksu Łączności Elektronicznej oraz Toolboxa 5G.

Rumunia

W Rumunii funkcjonuje ustawa nr 163/2021 o przyjęciu środków dotyczących infrastruktur informacyjnych i komunikacyjnych o znaczeniu krajowym oraz warunków wdrażania sieci

[21)] https://www.anacom.pt/render.jsp?contentId=1474999 .

5G[22]. Zgodnie z nią producent sprzętu, który miałby być wykorzystany do budowy sieci 5G musi uzyskać autoryzację w formie decyzji Premiera, wydanej na podstawie zgody Najwyższej Rady Obrony Narodowej. W procesie oceny dostawcy brane pod uwagą są uwagę kwestie, takie jak:

a) kontrola obcego rządu nad producentem przy braku niezależnego systemu prawnego;

b) brak przejrzystej struktury akcjonariatu producenta;

c) brak historii etycznego postępowania korporacyjnego producenta;

d) funkcjonowanie producenta w systemie prawnym, który nie narzuca przejrzystych praktyk korporacyjnych.

W Najwyższej Radzie Obrony Narodowej zasiadają przedstawiciele rządu, wojska oraz służb specjalnych[23].

Słowacja

Słowacja nie posiada ściśle określonych zasad dotyczących bezpieczeństwa sieci 5G.

W niektórych ustawach pojawiają się ogólne obowiązki związane z zarządzaniem bezpieczeństwem w łańcuchu dostaw.

Ponadto, przewidywana jest procedura oceny ryzyka dostawcy produktów do działań bezpośrednio związanych z eksploatacją sieci i systemów informatycznych dla operatora usługi podstawowej (zwanego dalej "osobą trzecią") na rzecz cyberbezpieczeństwa Republiki Słowackiej.

W 2020 podpisane zostało przez Słowację i USA memorandum[24] dotyczące sieci 5G. podkreślają znaczenie zachęcania do udziału rzetelnych i godnych zaufania dostawców sprzętu sieciowego i oprogramowania na rynkach 5G, uwzględniania ocen profilu ryzyka oraz promowania ram, które skutecznie chronią sieci 5G przed nieautoryzowanym dostępem i zakłóceniami.

Wskazano, że w szczególności, oceny bezpieczeństwa powinny być staranne i kompletne oraz obejmować zwłaszcza następujące elementy:

- czy dostawcy sprzętu sieciowego i oprogramowania podlegają kontroli ze strony obcego rządu;

[22] https://lege5.ro/gratuit/haydomrygy2q/legea-nr-163-2021-privind-adoptarea-unor-masuri-referitoare-la-infrastructuri-informatice-si-de-comunicatii-de-interes-national-si-conditiile-implementarii-retelelor-5g .
[23] https://csat.presidency.ro/ro/prima-pagina/componenta-csat .
[24] https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html .

- czy dostawcy sprzętu sieciowego i oprogramowania mają przejrzyste struktury własności, partnerstwa i ładu korporacyjnego;
- czy dostawcy sprzętu sieciowego i oprogramowania są zaangażowani w działalność innowacyjną i poszanowanie praw własności intelektualnej;
- czy dostawcy sprzętu sieciowego i oprogramowania mają na koncie etyczne zachowania korporacyjne i podlegają systemowi prawnemu, który wymusza przejrzyste praktyki korporacyjne.

Na marginesie można dodać, że na Słowacji występuje świadczenie teleinformatyczne.

Słowenia

Przepisy dotyczące bezpieczeństwa sieci 5G nie zostały jeszcze wprowadzone. Zgodnie z projektem ustawy rząd będzie mógł zabronić stosowania urządzeń dostarczanych przez dostawcę wysokiego ryzyka w niektórych częściach sieci. Istniejące urządzenia HRV w tych częściach należy wymienić. Jego produkty będą mogły być również zakazane w niektórych innych obszarach takich jak infrastruktura krytyczna, systemy rządowe, obrona narodowa czy systemy ratownicze. Decyzja w sprawie HRV będzie miała charakter niejawny.

Rząd, na podstawie opinii Rady Bezpieczeństwa Narodowego, będzie określać dostawców wysokiego ryzyka w drodze decyzji.

Będą przy tym brane pod uwagę następujące kryteria, z których będą musiały wystąpić przynajmniej trzy:

- powiązanie dostawcy z rządem państwa trzeciego;
- ustawodawstwo państwa trzeciego, szczególnie w przypadku braku demokratycznej kontroli i trójpodziału władz, oraz zawarte umowy o bezpieczeństwie lub ochronie danych między UE a danym państwem trzecim;
- cechy własności korporacyjnej dostawcy;
- zdolność państwa trzeciego do wywierania jakiejkolwiek formy nacisku, w tym w odniesieniu do miejsca produkcji sprzętu;
- zdolność dostawcy do zapewnienia dostaw;
- ogólna jakość produktów i praktyk dostawcy w zakresie bezpieczeństwa cybernetycznego, w tym stopień kontroli nad własnym łańcuchem dostaw oraz to, czy praktykom w zakresie bezpieczeństwa nadano odpowiedni priorytet.

Nie rzadziej jednak niż raz na dwa lata będzie przeprowadzany przegląd wydanych decyzji.

Szwecja

Szwedzkie prawo komunikacji elektronicznej zawiera jedynie ogólne obowiązki będące implementacją Europejskiego Kodeksu Łączności Elektronicznej[25)]. Implementacja przepisów Toolboxa 5G nastąpiła poprzez określenie warunków aukcji sieci 5G.

W październiku 2020 r. szwedzki krajowy regulacyjny organ telekomunikacyjny (PTS) nałożył następujące warunki udziału w aukcji widma 5G:

- nowe instalacje i wdrożenie funkcji centralnych dla radia w pasmach częstotliwości nie mogą korzystać z produktów pochodzących od chińskich sprzedawców;

oraz

- wszelka istniejąca infrastruktura pochodząca od takich dostawców musi zostać wycofana najpóźniej do 1 stycznia 2025 r.

Wielka Brytania

Telecommunications (Security) Act 2021[26)] znowelizował *The Communications Act 2003*. Właściwy sekretarz stanu może wydać "*designated vendor directions*", jeśli uważa, że są one niezbędne ze względu na interes bezpieczeństwa narodowego i jeśli nałożone przez ten środek wymagania są proporcjonalne. Do tych aktów muszą stosować się przedsiębiorcy telekomunikacyjni.

Designated vendor direction zawierają zakazy lub ograniczenia dotyczące używania produktów, usług dostarczanych przez dostawcę.

Designated vendor directions mają być przeglądane, co jakiś czas. Sekretarz stanu może wymagać od dostawców usług telekomunikacyjnych przygotowania i przedstawienia planu wdrożenia wymagań określonych w *designated vendor directions*.

Dostawca zostaje określony w *designation notice*. Przy wydawaniu tego aktu sekretarz stanu bierze pod uwagę zarówno czynniki techniczne (jakość, niezawodność, bezpieczeństwo

[25)] https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482#K8 .

[26)] Telecommunications (Security) Act 2021 chapter 31 https://www.legislation.gov.uk/ukpga/2021/31/enacted .

produktów), jak i nietechniczne (związki między dostawcą a krajem pochodzenia, tożsamość osób uczestniczących w rozwoju lub produkcji produktów).

Węgry

Węgry nie wprowadziły przepisów związanych z dostawcą wysokiego ryzyka. Art. 156 ich Prawa telekomunikacyjnego[27)] nakłada na operatorów telekomunikacyjnych ogólne obowiązki związane z zapewnianiem bezpieczeństwa, nie odnosi się jednak do kwestii bezpieczeństwa łańcucha dostaw czy oceny wysokiego ryzyka.
W tym obszarze funkcjonuje jeszcze rozporządzenie 41/2015 Ministra Spraw Wewnętrznych, które wprowadza ogólne wymogi bezpieczeństwa informacji dla podmiotów węgierskiego systemu cyberbezpieczeństwa[28)].

Włochy

Włochy implementowały przepisy Toolboxa 5G w zakresie dostawcy wysokiego ryzyka poprzez zastosowanie do operatorów w tej sieci zasad zawartych w ustawie z 15 marca 2012 r. o specjalnych uprawnień dotyczących struktur korporacyjnych w sektorach obronności i bezpieczeństwa narodowego, a także dla działalności o znaczeniu strategicznym w sektorach energii, transportu i komunikacji[29)]. Środki z tej ustawy, takie jak możliwość zablokowania zawarcia umowy bądź nałożenia określonych obowiązków, będą miały zastosowanie do umów z podmiotami spoza UE dotyczących:

1) zakupu towarów i usług związanych z projektowaniem, wdrażaniem, utrzymaniem i obsługą sieci 5G; i/lub
2) nabycia powiązanych komponentów zaawansowanych technologicznie.

Ustawa nakłada obowiązek notyfikacji takich transakcji. Krajowy Urząd Oceny i Certyfikacji (Centro di valutazione e certificazione nazionale - CVCN) ocenia ewentualne czynniki podatności, które mogłyby zagrozić integralności i bezpieczeństwu sieci 5G i przesyłanych danych poprzez wstępne dochodzenie[30].

[27)] https://net.jogtar.hu/jogszabaly?docid=a0300100.tv .
[28)] https://njt.hu/jogszabaly/2015-41-20-0A .
[29)] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2012-03-15;21 .
[30)] https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105 .

Załącznik nr 2 do OSR

Lp.	rodzaj kosztów	2024	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	SUMA
1	koszty realizacji i utrzymania podłączeń do S46 (w tym zakup urządzeń końcowych)	8 212 000	5 941 000	2 823 000	2 605 000	2 678 000	5 592 000	10 392 000	8 367 000	5 513 000	5 513 000	5 513 000	57 636 000
2	koszty rozwoju S46 związanego z nowymi zadaniami	275 000	286 000	354 000	368 000	677 000	991 000	1 117 000	1 247 000	1 383 000	1 383 000	1 383 000	8 081 000
3	koszty zapewniania działania systemu	3 638 000	4 451 000	4 280 000	3 702 000	6 551 000	6 417 000	9 532 000	11 445 000	7 468 000	7 468 000	7 468 000	64 952 000
4	koszty pośrednie	2 334 000	2 036 000	1 387 000	1 207 000	1 844 000	2 452 000	4 038 000	3 987 000	2 645 000	2 645 000	2 645 000	24 575 000
	SUMA	14 459 000	12 714 000	8 844 000	7 882 000	11 750 000	15 452 000	25 079 000	25 046 000	17 009 000	17 009 000	17 009 000	155 244 000

Ad 1	Koszty realizacji i utrzymania podłączeń do S46 (w tym zakup urządzeń końcowych) związane są z koniecznością podłączenia ponad dwukrotnie większej od szacunków z 2018 r. liczby podmiotów krajowego systemu cyberbezpieczeństwa. W skład tych kosztów wchodzą koszty jednorazowe - zakup urządzeń, usług, koszty instalacji oraz koszty ciągłe - koszty łączności i serwisu urządzeń zakończenia sieci dla podłączanych podmiotów celem zmniejszenia bariery finansowej - szczególnie dla podmiotów publicznych (z odnowieniem parku maszynowego - sukcesywnym od 2028 roku)
Ad 2	Koszty rozwoju S46 związane z nowymi zadaniami wynikają ze zmian technologicznych oraz ciągłego dostosowywania S46 do potrzeb rozszerzonego grona jego użytkowników.
Ad 3	Koszty zapewnienie działania systemu zawierają koszty zapewnienia ciągłości działania rozbudowanego systemu S46, koszty odnowienia parku maszynowego (centra) - sukcesywne od 2028 roku, koszty uspójniania modelu cyberbezpieczeństwa w środowisku wielu CSIRT (analizy merytoryczne S46) oraz inne koszty (serwisy, kolokacje, prąd, łączność centrów, materiały, koszty stanowisk pracy, szkoleń, delegacji, transportu, nakłady związane ze zwiększaniem poziomu bezpieczeństwa systemu).
Ad 4	Koszty pośrednie są związane z zapewnieniem administracyjnej obsługi projektu, w tym: koszty dyrekcji (zarządu), obsługi kadrowej czy księgowości. Stanowią ryczałt, odpowiadający 20% sumy wszystkich innych kosztów z wyłączeniem usług.

RAPORT Z OPINIOWANIA I KONSULTACJI PUBLICZNYCH

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UD68).

Projekt ustawy został poddany opiniowaniu oraz konsultacjom publicznym.

Niniejszy raport został sporządzony na podstawie § 51 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin Pracy Rady Ministrów (M.P. z 2022 r. poz. 348). Zawiera on podsumowanie konsultacji publicznych oraz opiniowania ww. projektu ustawy.

1. Omówienie wyników przeprowadzonych konsultacji publicznych

Celem opiniowania i konsultacji publicznych było zapewnienie zainteresowanym podmiotom i organizacjom, możliwości wyrażenia opinii na temat rozwiązań prawnych zawartych w przedmiotowym projekcie.

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (pierwotny tytuł projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych) w dniu 8 września 2020 r. został skierowany do konsultacji publicznych i opiniowania. Projekt został udostępniony również w Biuletynie Informacji Publicznej Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, w celu zapoznania się z nim przez wszystkie zainteresowane podmioty. Ponadto, projekt został przesłany niżej wymienionym instytucjom w oddzielnej korespondencji mailowej.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów, z 14 – dniowym terminem na przedstawienie stanowiska. Jednakże, w z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni. Tym samym łączny termin na przedstawienie stanowiska wynosił 28 dni.

Zaproszenie w ramach konsultacji publicznych otrzymały:

1) Polska Izba Informatyki i Telekomunikacji;

2) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;

3) Polska Izba Komunikacji Elektronicznej;

4) Krajowa Izba Gospodarcza;

5) Krajowa Izba Komunikacji Ethernetowej;

6) Krajowa Izba Gospodarki Cyfrowej;

7) Polska Izba Radiodyfuzji Cyfrowej;

8) Fundacja Bezpieczna Cyberprzestrzeń;

9) Polska Izba Handlu;

10) Polskie Towarzystwo Informatyczne;

11) Stowarzyszenie Inżynierów Telekomunikacji;

12) Związek Rzemiosła Polskiego;

13) Związek Pracodawców Mediów Publicznych;

14) Związek Pracodawców Branży Internetowej IAB Polska;

15) Polska Rada Biznesu;

16)Naczelna Organizacja Techniczna;

17) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;

18)Izba Gospodarki Elektronicznej;

19) Fundacja ePaństwo;

20) Fundacja Nowoczesna Polska;

21) Fundacja Projekt Polska;

22) Fundacja Panoptykon;

23)Internet Society Poland;

24) Związek Telewizji Kablowych w Polsce Izba Gospodarcza;

25) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;

26) Polskie Centrum Badań i Certyfikacji S.A.;

27) Polska Organizacja Handlu i Dystrybucji;

28)Naczelna Rada Zrzeszeń Handlu i Usług;

29) Polska Izba Producentów Urządzeń i Usług na rzecz Kolei;

30) Polskie Stowarzyszenie Marketingu SMB;

31)Amerykańska Izba Handlowa;

32) Federacja Konsumentów;

33) Polski Związek Przemysłu Motoryzacyjnego;

34)Ogólnopolskie Porozumienie Organizacji Radioamatorskich;

35) Polski Związek Krótkofalowców;

36)Business Centre Club;

37) Konfederacja Lewiatan;

38)Rada Dialogu Społecznego;

39) Krajowa Izba Gospodarki Morskiej;

40) Krajowa Izba Rozliczeniowa;

41) Polska Wytwórnia Papierów Wartościowych;

42) Towarzystwo Gospodarcze Polskie Elektrownie;

43) Fundacja Bezpieczna Cyberprzestrzeń;

44) Fundacja im. Stefana Batorego;

45) Fundacja Instytut Mikromakro;

46) Fundacja My Pacjenci;

47) Fundacja Przedsiębiorców Polskich Archiwizjoner;

48) Fundacja Pułaskiego;

49) Stowarzyszenie Inżynierów Telekomunikacji;

50) Sektorowa Rada ds. Kompetencji - Telekomunikacja i Cyberbezpieczeństwo;

51) Internet Society Poland Chapter

W ramach opiniowania zaproszenie skierowano do:

1) Prezesa Urzędu Komunikacji Elektronicznej;

2) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;

3) Prezesa Urzędu Ochrony Danych Osobowych;

4) Prezesa Głównego Urzędu Statystycznego;

5) Rzecznika Małych i Średnich Przedsiębiorców;

6) Wojskowego Biura Zarządzania Częstotliwościami;

7) Komisji Nadzoru Finansowego;

8) Rzecznika Praw Obywatelskich;

9) Krajowej Rady Radiofonii i Telewizji;

10) Polskiego Komitet Normalizacyjnego;

11)Urzędu Zamówień Publicznych;

12)Najwyższej Izby Kontroli;

13)Agencji Bezpieczeństwa Wewnętrznego;

14)Agencji Wywiadu;

15)Biura Bezpieczeństwa Narodowego;

16) Centralne Biura Antykorupcyjnego;

17) Służby Kontrwywiadu Wojskowego;

18) Służby Wywiadu Wojskowego;

19)Rządowego Centrum Bezpieczeństwa;

20) Służby Ochrony Państwa.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, pod warunkiem zgłoszenia tego faktu opiekunowi merytorycznemu projektu.

Do projektu ustawy w ramach konsultacji publicznych uwagi zgłosiły następujące podmioty:

1) Związek Banków Polskich,
2) Santander,
3) Narodowy Instytut Cyberbezpieczeństwa,
4) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM,
5) Bank Handlowy,

6) Q-PRO Jakub Stoparek,
7) RFCell Technologies Sp. z.o.o.,
8) KGHM/Związek Pracodawców Polska Miedź,
9) Stowarzyszenie Libertariańskie,
10) SayF, Transition Software,
11) Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze,
12) Izba Przemysłowo-Handlowa Polska-Azja,
13) Huawei Polska,
14) Business Centre Club,
15) Digital Poland, Excogitate,
16) Fundacja Bezpieczna Cyberprzestrzeń,
17) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT,
18) Narodowy Bank Polski,
19) Naczelna Organizacja Techniczna.
20) Federacja Stowarzyszeń Naukowo-Technicznych,
21) Polskie Centrum Badań i Certyfikacji,
22) Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile,
23) Federacja Przedsiębiorców Polskich,
24) 1Innosystems,
25) Polska Izba Komunikacji Elektronicznej,
26) Fabryka E-Biznesu,
27) Krajowa Izba Gospodarki Cyfrowej DigiCom,
28) Home.pl,
29) Install Tech, Polska Izba Handlu,
30) ISACA Warsaw Chapter,
31) Krajowy Sekretariat Łączności NSZZ Solidarność,
32) MJC Sp. z.o.o., IAB Polska,
33) Federacja Konsumentów,
34) Stowarzyszenie „Miasta w Internecie”,
35) Stowarzyszenie Inżynierów Telekomunikacji,
36) Uniwersytet Jagielloński Collegium Medicum,
37) PKP Energetyka,
38) Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo,
39) Polskie Towarzystwo Informatyczne,
40) ISSA Polska,
41) Związek Przedsiębiorców i Pracodawców,
42) Krajowy Depozyt Papierów Wartościowych,
43) Politechnika Wrocławska.
44) Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL,
45) S4IT Michał Podgórski,
46) Orange Polska,
47) Polsko-Chińska Główna Izba Gospodarcza SinoCham,
48) Aberit,
49) Młodzieżowy Delegat RP przy NATO,
50) ERSTAR,
51) ETOB-RES,
52) Fundacja Alatum,
53) GBX Soft,
54) Instytut Lema,

55) Mobile Logic,
56) Mobilne Miasto,
57) Nanocoder,
58) NeuroGames Lab,
59) SmartWeb Media,
60) TELDATA,
61) TEP Doradztwo Biznesowe,
62) TILT, Związek Cyfrowa Polska,
63) Signum Edward Kuś Marcin Kuś,
64) PKN Orlen,
65) Skandynawsko-Polska Izba Gospodarcza,
66) Liquid Systems,
67) Instytut Staszica,
68) Akademia Sztuki Wojennej,
69) Krajowa Izba Komunikacji Ethernetowej,
70) Qualitel Service,
71) JARTEL,
72) Izba Gospodarki Elektronicznej,
73) Konfederacja Lewiatan
74) Porozumienie Zielonogórskie.
75) Federacja Związków Pracodawców Ochrony Zdrowia

Ponadto, w trybie opiniowania, opinie przedstawiły następujące podmioty:

1) Biuro Bezpieczeństwa Narodowego
2) Rzecznik Małych i Średnich Przedsiębiorców
3) Prezes Urzędu Komunikacji Elektronicznej
4) Agencja Wywiadu
5) Prezes Urzędu Ochrony Danych Osobowych
6) Komisja Nadzoru Finansowego
7) Najwyższa Izba Kontroli
8) Urząd Zamówień Publicznych
9) Prezes Urzędu Ochrony Konkurencji i Konsumentów
10) Polski Komitet Normalizacyjny
11) NASK-PIB

W procedurze opiniowania i konsultacji publicznych projektu ustawy wszystkim podmiotom umożliwiono zajęcie stanowiska w sprawie projektu, a także poddano analizie przedłożone przez te podmioty uwagi.

W ramach konsultacji publicznych i opiniowania zgłoszono szereg uwag do projektu ustawy: w ramach konsultacji: 548 uwag, a w ramach opiniowania: 53 uwagi.

Ponadto, tabele zawierające stanowisko Ministra Cyfryzacji do zgłoszonych uwag opublikowano na stronie RCL, w zakładce „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach procesu konsultacji i opiniowania znaczna liczba podmiotów zwracała szczególną uwagę na kwestie dotyczące uregulowania w przepisach prawa oceny dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa pod kątem uznania tych dostawców za dostawców wysokiego ryzyka. Wskazano na potrzebę zapewnienia transportowości procesu oceny (najlepiej w oparciu o przepisy Kodeksu postępowania

administracyjnego) oraz zapewnienia skutecznej drogi odwoławczej od ewentualnej negatywnej decyzji.

Ponadto, zwracano uwagę na doprecyzowanie stosowania nowych instrumentów w krajowym systemie cyberbezpieczeństwa tj.: ostrzeżeń i poleceń zabezpieczających.

Wiele uwag dotyczyło także kwestii włączenia do ustawy o krajowym systemie cyberbezpieczeństwa, przepisów prawa wdrażających Europejski Kodeks Łączności Elektronicznej. Podmioty wskazywały, że kwestie wymagań bezpieczeństwa oraz zgłaszania incydentów bezpieczeństwa powinny pozostać w regulacji sektorowej, która ma być równolegle procedowana z projektem ustawy - Prawo komunikacji elektronicznej.

2. Przedstawienie wyników konsultacji projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt ustawy nie wymagał przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

3. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa

Zgodnie z przepisami ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy został udostępniony w Biuletynie Informacji Publicznej. W toku prac nad projektem zgłoszenie zainteresowania projektem wysłały następujące podmioty:

1) Excogitate sp. z o.o.
2) Loopus Górski Opęchowski sp. j.
3) Signum Edward Kuś.

Należy podkreślić, że wskazane wyżej podmioty nie prowadzą zawodowej działalności lobbingowej.

Zbiorcza tabela uwag zgłoszonych do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (poprzedni tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa (UD68).

Część I.

Liczba organizacji, które otrzymały zaproszenia:
Organizacje, które zgłosiły swoje uwagi: Związek Banków Polskich, Santander, Narodowy Instytut Cyberbezpieczeństwa, Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, Bank Handlowy, Q-PRO Jakub Stoparek, RFCell Technologies Sp. z.o.o., KGHM/Związek Pracodawców Polska Miedź, Stowarzyszenie Libertariańskie, SayF, Transition Software, Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze, Izba Przemysłowo-Handlowa Polska-Azja, Huawei Polska, Business Centre Club, Digital Poland, Excogitate, Fundacja Bezpieczna Cyberprzestrzeń, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT, Narodowy Bank Polski, Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych, Polskie Centrum Badań i Certyfikacji, Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile, Federacja Przedsiębiorców Polskich, 1Innosystems, Polska Izba Komunikacji Elektronicznej, Fabryka E-Biznesu, Unia Metropolii Polskich, Krajowa Izba Gospodarki Cyfrowej DigiCom, Home.pl, Install Tech, Polska Izba Handlu, ISACA Warsaw Chapter, Krajowy Sekretariat Łączności NSZZ Solidarność, MJC Sp. z.o.o., IAB Polska, Federacja Konsumentów, Stowarzyszenie „Miasta w Internecie", Stowarzyszenie Inżynierów Telekomunikacji, Uniwersytet Jagielloński Collegium Medicum, PKP Energetyka, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne, ISSA Polska, Związek Przedsiębiorców i Pracodawców, Krajowy Depozyt Papierów Wartościowych, Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL, S4IT Michał Podgórski, Orange Polska, Polsko-Chińska Główna Izba Gospodarcza SinoCham, Aberit, Młodzieżowy Delegat RP przy NATO, ERSTAR, ETOB-RES, Fundacja Alatum, GBX Soft, Instytut Lema, Mobile Logic, Mobilne Miasto, Nanocoder, NeuroGames Lab, SmartWeb Media, TELDATA, TEP Doradztwo Biznesowe, TILT, Związek Cyfrowa Polska, Signum Edward Kuś Marcin Kuś, PKN Orlen, Skandynawsko-Polska Izba Gospodarcza, Liquid Systems, Instytut Staszica, Akademia Sztuki Wojennej, Krajowa Izba Komunikacji Ethernetowej, Qualitel Service, JARTEL, Izba Gospodarki Elektronicznej, Konfederacja Lewiatan
Podmioty, które odpowiedziały na zaproszenie, ale nie zgłosiły uwag do projektu: Porozumienie Zielonogórskie. Federacja Związków Pracodawców Ochrony Zdrowia
Podmioty, które zrezygnowały z udziału w konsultacjach:

	Podmiot wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Zgłoszone uwagi	Stanowisko KPRM/DC
1.	Związek Banków Polskich	Uwaga ogólna	ISAC powinien również wspomagać podmioty z danego sektora, sektorów lub podsektorów, niezależnie od wydania decyzji o uznaniu konkretnego podmiotu za operatora usługi kluczowej – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od wielu innych podmiotów, w szczególności pozostałych banków, dostawców usług płatniczych, czy też izb rozliczeniowych. Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym. W związku z tym ustawa powinna przyznawać ISAC kompetencje umożliwiające taką współpracę.	**Wyjaśnienie** ISAC nie jest jednostką operacyjną, nie zajmuje się reagowaniem na incydenty. Nie ma przeszkód, żeby ISAC wspomagał inne podmioty spoza ksc.
2.	Związek Banków Polskich	Uwaga ogólna	Za krytyczny należy uznać brak w ramach krajowego systemu cyberbezpieczeństwa dostawców usług płatniczych, krajowych instytucji płatniczych i izb rozliczeniowych, co powoduje stworzenie luki w systemie płatniczym kraju oraz oznacza faktyczną niemożność wykrywania, przeciwdziałania i zwalczania cyberincydentów w obszarze realizacji i rozliczeń transakcji płatniczych	**Uwaga nieuwzględniona** Niemożliwe jest uwzględnienie dostawców usług płatniczych z powodu kolizji ustawowej. Działalność dostawców usług płatniczych regulują inne przepisy powstałe w oparciu o dyrektywę PSD2.
3.	Związek Banków Polskich	Uwaga ogólna	Za krytyczne należy uznać wprowadzenie podstawy prawnej do przetwarzania tajemnic prawnie chronionych oraz danych osobowych w celu skutecznego działania CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych oraz ISAC	**Uwaga nieuwzględniona** Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione.

4.	Związek Banków Polskich	Uwaga ogólna	Za krytyczne należy uznać brak przepisów umożliwiających przetwarzanie prawnie chronionych pomiędzy OUK, DUC, przedsiębiorcami komunikacji elektronicznej oraz ISAC, co uniemożliwia sprawną wymianę informacji o incydentach w celu ich wykrywania, analizowania, zapobiegania i zwalczania – propozycja dodania nowego przepisu.	**Uwaga nieuwzględniona** ISAC jest centrum wymiany informacji ale nie informacji prawnie chronionych. Chyba że podmioty tworzące ISAC umówią się, że będą sobie przekazywać tajemnicę przedsiębiorstwa.
5.	Związek Banków Polskich	Uwaga ogólna	Za krytyczny należy uznać fakt, że sektor bankowy własnym kosztem wytworzył wiele systemów wspierających bezpieczeństwo banków oraz ich klientów. Istotne jest, aby wprowadzić możliwość wykorzystania ich w ramach krajowego systemu cyberbezpieczeństwa. Również obowiązki informacyjne o incydentach np. względem CSIRT MON, CSIRT NASK i CSIRT GOV mogłyby być realizowane z ich użyciem. Pozwoli to uniknąć dublowania czynności związanych z notyfikacją incydentów do wielu instytucji państwowych, np. KNF, PUODO, prokuratury, policji itp. W związku z powyższym proponujemy dodanie przepisu, który będzie dawał możliwość wykorzystywania sektorowych systemów IT z centralnym systemem do zgłaszania incydentów. ZBP uczestniczył projekcie NASK – Narodowej Platformie Cyberbezpieczeństwa, której osiągnięcia są wykorzystywane w tworzonym Systemie S46. Ten projekt i integracja systemu sektorowego (BRIBIT) z NPC potwierdził deklarowane korzyści z integracji, która umożliwi niezakłócony dwukierunkowy przepływ informacji pomiędzy operatorami usług kluczowych a Instytucjami wchodzącymi w skład krajowego systemu cyberbezpieczeństwa.	**Wyjaśnienie** Centralnym systemem zarządzania cyberbezpieczeństwem w Polsce jest system utworzony na podstawie art. 46 ustawy ksc. Do systemu będą mogli dołączyć użytkownicy np. operatorzy usług kluczowych czy dostawcy usług cyfrowych na podstawie porozumienia zawartego z ministrem właściwym ds. informatyzacji
6.	Santander	Uwaga ogólna	Mamy CSIRT NASK do którego raportujemy incydenty poważne i to samo musimy raportować do powołanego CSIRT KNF sektorowego. Czy nie powinno być tak, że zgłaszamy do naszego sektorowego i tam informacja jest zarządzona a do obsługi incydentu zdarzenia wykorzystywany jest jeden, spójny system?	**Wyjaśnienie** CSIRT poziomu krajowego koordynuje obsługę incydentów. CSIRT sektorowy zajmuje się bezpośrednim wsparciem operatora.

7.	Santander	Uwaga ogólna	Czy zostaną zmodyfikowane Rozporządzenia do Ustawy, odzwierciedlające aktualny stan pracy zdalnej, poza wydzielonymi strefami bezpiecznymi w kontekście pandemii COVID-19 np. pracowników SOC czy Threat Intelligence?	**Wyjaśnienie** Rozporządzenie to straci moc z chwilą wejścia w życie ustawy. Operator usługi kluczowej będzie wdrażał zabezpieczenia w oparciu o *risk based approach*, także dotyczące pracy zdalnej.
8.	Narodowy Instytut Cyberbezpieczeństwa	Uwaga ogólna	Przedłożony projekt budzi pewne wątpliwości w zakresie zgodności z polskim systemem prawnym. Znaczna część proponowanych rozwiązań dotyczy kryteriów oceny stosowanych podczas postępowania, które prowadzone ma być przez Kolegium do Spraw Cyberbezpieczeństwa. Zakłada się brak obecności w jego trakcie ocenionego dostawcy sprzętu czy też oprogramowania. Pozostałe wątpliwości związane są z ochroną konkurencji, a także dalszym rozwojem sieci 5G w Polsce. W proponowanej wersji projektu nie wskazano konkretnych kryteriów według których oceniany będzie dostawca sprzętu lub oprogramowania. Aby stworzyć sytuację pewności po stronie ocenianego, kryteria te powinny być jasno i precyzyjnie określone. W przeciwnym razie mamy do czynienia z oceną uznaniowa, nie zaś merytoryczną. Ponadto, cały proces odbywa się bez udziału stron postępowania. To również może wpłynąć na ocenę całego procesu i powinno zostać zmienione w ostatecznej wersji aktu. Warto zaznaczyć, że te kwestie mogą być argumentem dla niektórych ze stron postępowania do kwestionowania dokonanego wyboru. Oceniany bowiem powinien mieć zagwarantowane prawo do czynnego udziału w postępowaniu, które zaważyć może na przyszłości prowadzonej przez niego działalności gospodarczej. Biorąc pod uwagę skutki w postaci zakazu wprowadzania przez niego nowego sprzętu lub oprogramowania na rynek oraz usunięcia tego, który jest już na nim obecny, jeżeli taka decyzję podjęłoby Kolegium. To może	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.

			mieć negatywny wpływ na wizerunek Polski wśród inwestorów z branż, z uwagi na niepewność środowiska biznesowego. Niejasne pozostają także kryteria, które służyć będą do wyboru dostawcy sprzętu i oprogramowania sieci 5G, jak i określania przez Kolegium ich ryzyka. Dostawcy ci nie mają również możliwości odwołania się od wydanej decyzji o wyborze innego podmiotu niż Kolegium. To w praktyce może prowadzić do nadużyć oraz stawiać znak zapytania przy zgodności proponowanych przepisów z zasada równości wobec prawa. Wszyscy dostawcy powinni być traktowani w jednolity sposób, które będzie gwarantem wspomnianej wcześniej równości, a który wyrażony byłby właśnie poprzez określenie konkretnych kryteriów oceny. Te, które zostały wskazane w projekcie ustawy są bardzo szerokie i dotyczą głównie kwestii polityczno-gospodarczych. W postępowaniu oceniającym pomija się specyfikacje techniczne, które maja równorzędne, jeśli nie nawet większe, znaczenie w przypadku przedmiotowej regulacji i to głównie na nich powinien się opierać wybór dostawcy sprzętu bądź oprogramowania przez operatora sieci telekomunikacyjnej, a także sam proces oceny ryzyka prowadzonej przez Kolegium. Niezastosowanie kryterium technicznego może się negatywnie odbić na rozwoju technologii 5G w Polsce, ponieważ operatorzy będą mieć ograniczony wybór dostawców, z których będą mogli korzystać. Opisane wątpliwości mogą mieć wpływ na rynek konkurencji w Polsce. Ograniczenie ilości podmiotów oferujących sprzęt bądź oprogramowanie spełniające należyte wymogi w zakresie cyberbezpieczeństwa w wyniku stosowania niejasnych bądź niepełnych kryteriów, może doprowadzić do załamania rynku, a także pogorszenia się sytuacji konsumenta. Odnosząc się do kwestii niejasnych kryteriów należy także zauważyć, że także	Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o

			konsumenci odczują wspomniane wcześniej skutki z uwagi na wyższe ceny usług, spowodowane mniejszą konkurencją na rynku i wyższymi kosztami operatorów. Pozostając w obszarze ochrony konkurencji należałoby także zastanowić się, czy kompetencje przyznane Kolegium do Spraw Cyberbezpieczeństwa nie pokrywają się z kompetencjami innego podmiotu nadzorującego rynek telekomunikacyjny, także w zakresie konkurencji. Konsekwencją rozwiązań ujętych w projekcie ustawy jest opóźnienie wprowadzenia sieci 5G w Polsce. Z tym jest bezpośrednio związane ryzyko pozostania Polski w tyle w stosunku do pozostałych krajów europejskich pod względem tempa rozwoju 5G. Ma to znaczenie dla innych powiązanych sektorów gospodarki, takimi jak chociażby nowoczesny przemysł, medycyna, edukacja zdalna, czy nawet rolnictwo. Opóźnienie wpłynie także na możliwość utworzenia nowych miejsc pracy. Wspomniany wyżej wpływ na konkurencję może natomiast przyczynić się do zwiększonego wykluczenia społecznego, z uwagi na wyższe koszty usług dostępu do sieci 5G. Rozwój siei 5G będzie mieć fundamentalny wpływ na rozwój polskiej gospodarki. Dlatego tez istotne jest, by nowa regulacja stwarzała ku temu dobre warunki. Podstawa przyjaznego środowiska dla rozwoju sieci 5G jest przede wszystkim konkretna, jasna i przejrzysta regulacja prawna. Regulacja ta powinna zawierać kryteria oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa oparte na precyzyjnej specyfikacji technicznej tak, aby zaistniała pewność co do tego, jakie warunki należy spełnić, by móc funkcjonować na rynku. Ponadto, samo postępowanie oceniające powinno być bardziej przejrzyste i należałoby je poszerzyć o możliwość odwołania się dostawców od decyzji wydanej przez Kolegium do Spraw Cyberbezpieczeństwa do innego, niezależnego podmiotu.	uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			Aktualnie proponowana regulacja, która przewiduje odwołanie od decyzji wydanej przez Kolegium do tego samego gremium budzi wątpliwości co do szans na inną decyzję w ostatecznym rozstrzygnięciu. Stwarza to również możliwość pojawiania się nadużyć.	
9.	Osoba fizyczna	Uwaga ogólna	W mojej opinii, w ustawie brakuje jasno zdefiniowanych odpowiedzialności dot. edukacji. Są zapisy mówiące o "budowaniu świadomości podmiotów systemu". Powinny być jasne zapisy mówiące o tym: kto i w jakim zakresie jest odpowiedzialny za edukację. Dotyczy to edukacji zarówno podmiotów publicznych, organów administracji jak i społeczeństwa. Szkolenia i promowanie dobrych praktyk będzie miało bezpośrednie przełożenie na wzrost cyberbezpieczeństwa.	**Uwaga nieuwzględniona, nie dotyczy nowelizacji**
10.	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	Uwaga ogólna	Biorąc pod uwagę powyższe, oraz treść pisma zawiadamiającego o konsultacjach, z którego wynika, że PKE ma zostać uzupełnione o przepisy regulujące obowiązki przedsiębiorców w zakresie zapewnienia bezpieczeństwa ciągłości świadczenia usług komunikacji elektronicznej oraz dostarczania sieci telekomunikacyjnej poprzez włączenie obowiązków zawartych w konsultowanym projekcie do PKE, nie jest do końca jasne przyjęty sposób regulacji. Czy konsultowane przepisy mają znaleźć się w dwóch równoległych ustawach? Czy też mają one być wprowadzone do PKE i usunięte z konsultowanej ustawy? Mediakom postuluje, by kwestie bezpieczeństwa sieci i usług uregulowane zostały w jednym akcie prawnym, tak by maksymalnie uprościć przyjęte rozwiązania i zapewnić czytelność i możliwą łatwość stosowania przez przedsiębiorców komunikacji elektronicznej. Zbędne jest też powielanie tożsamych przepisów w dwóch niezależnych ustawach.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.

				Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
11.	Q-PRO Jakub Stoparek	Uwaga ogólna	W ostatnim czasie, dotarły do nas niepojące opinie umieszczane w prasie lub Internecie dotyczące nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jako firma Q-PRO Jakub Stoparek, z branży telekomunikacyjnej będziemy świadczyć usługi dla wielu firm telekomunikacyjnych. Po przeczytaniu wielu artykułów na ten temat niepokoi nas projekt ustawy, który może mieć negatywny wpływ na naszą firmę i pokrewne branże. Jesteśmy przekonani, że polski rynek jest rynkiem otwartym, przejrzystym, gdzie panuje równość i uczciwa konkurencja. Rozumiemy, że Rząd chce chronić cyberbezpieczeństwo kraju, ale obawiamy się, że wykluczenie niektórych dostawców usług telekomunikacyjnych przyniesie skutki odwrotne do zamierzonych i wpłynie negatywnie na zatrudnienie i rozwój branży. Wydaje się niezasadnym stosowanie kryterium wskazywania firm podwyższonego ryzyka na podstawie ich pochodzenia, gdyż nie mierzy on poziomu ryzyka dla cyberbezpieczeństwa naszego państwa. Logicznym rozwiązaniem byłoby wprowadzenie ściśle określonych technicznych wymogów dotyczących sprzętu w strategicznych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju ich pochodzenia. Wydaje się, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa. Mamy nadzieję, że liczne wątpliwości ujawnione na etapie konsultacji społecznych, pozwolą ministerstwu opracowanie projektu ustawy pozbawionego ryzyka	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			negatywnego wpływu na branżę teleinformatyczną lub bezpośrednio na konsumentów. Dziękujemy za wysłuchanie naszych opinii.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
12.	RFCell Technologies Sp. z.o.o.	Uwaga ogólna	W ostatnim czasie, dotarły do nas niepojące opinie umieszczane w prasie lub Internecie dotyczące nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jako firma RFCell Technologies Sp. z.o.o**.** z branży telekomunikacyjnej będziemy świadczyć usługi dla wielu firm telekomunikacyjnych. Po przeczytaniu wielu artykułów na ten temat niepokoi nas projekt ustawy, który może mieć negatywny wpływ na naszą firmę i pokrewne branże. Jesteśmy przekonani, że polski rynek jest rynkiem otwartym, przejrzystym, gdzie panuje równość i uczciwa konkurencja. Rozumiemy, że Rząd chce chronić cyberbezpieczeństwo kraju, ale obawiamy się, że wykluczenie niektórych dostawców usług telekomunikacyjnych przyniesie skutki odwrotne do zamierzonych i wpłynie negatywnie na zatrudnienie i rozwój branży. Wydaje się niezasadnym stosowanie kryterium wskazywania firm podwyższonego ryzyka na podstawie ich pochodzenia, gdyż nie mierzy on poziomu ryzyka dla cyberbezpieczeństwa naszego państwa. Logicznym rozwiązaniem byłoby wprowadzenie ściśle określonych technicznych wymogów dotyczących sprzętu w strategicznych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju ich pochodzenia. Wydaje się, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

			cyberbezpieczeństwa. Mamy nadzieję, że liczne wątpliwości ujawnione na etapie konsultacji społecznych, pozwolą ministerstwu opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną lub bezpośrednio na konsumentów. Dziękujemy za wysłuchanie naszych opinii.	sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast

				przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
13.	KGHM/Związek Pracodawców Polska Miedź	Uwaga ogólna	Związek Pracodawców Polska Miedź pozytywnie ocenia fakt, iż przygotowane przez Ministra Cyfryzacji zmiany zawarte w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych, mają na celu stworzenie podstaw prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym.	**Wyjaśnienie** Dziękujemy za pozytywne stanowisko.
14.	Stowarzyszenie Libertariańskie	Uwaga ogólna	Rządowy projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych przewiduje możliwość wydawania przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa „poleceń zabezpieczających" nakazujących np. wprowadzenie „reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL" lub „zakaz korzystania z określonego sprzętu lub oprogramowania". Polecenia te będą mogły być wydawane między innymi: - przedsiębiorcom o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców, czyli na przykład	**Uwaga nieuwzględniona** Projektowane przepisy dot. ostrzeżenia i polecenia zabezpieczającego nie mają na celu ograniczenie wolności słowa i dostępu do internetu. . Ich stosowanie jest ograniczone tylko do niektórych grup podmiotów z sektorów gospodarki kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa m.in. do operatorów usług kluczowych, administracji publicznej, czy przedsiębiorców telekomunikacyjnych. Co więcej, środki te mogą być aktywowane w sytuacji zagrażającej wystąpieniu incydentu krytycznego (ostrzeżenie) lub w trakcie jego trwania, w związku z potrzebą zapewnienia

			przedsiębiorcom telekomunikacyjnym, takim jak: Orange Polska, T-Mobile Polska, Netia, Polkomtel, Telefonia Dialog, EmiTel, Exatel, Multimedia Polska, TTcomm, TK Telekom czy nadawcom takim jak Telewizja Polska i Polskie Radio; - podmiotom, o których mowa w art. 4 pkt 1-16 ustawy o krajowym systemie cyberbezpieczeństwa, czyli na przykład dostawcom usług cyfrowych, przez które rozumie się internetowe platformy handlowe (wszelki handel i usługi z umowami zawieranymi na stronie internetowej, czyli również usługi hostingu), wyszukiwarki internetowe oraz usługi przetwarzania w chmurze; - krajowym instytucjom płatniczym. „Polecenia zabezpieczające" będą mogły być wydawane w przypadku wystąpienia „incydentu krytycznego", czyli incydentu skutkującego „znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi", klasyfikowanego przez właściwy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. Da to możliwość nakazania zablokowania dostępu do dowolnego serwera, strony internetowej czy usługi, zarówno głównym operatorom telekomunikacyjnym, jak i dostawcom hostingu, operatorom płatności lub samym właścicielom stron czy usług. Decyzją urzędnika, od której nie będzie przysługiwać odwołanie do sądu, bo takiej procedury nie przewidziano. Wystarczy uznanie przez odpowiedni państwowy zespół, że wystąpił „incydent krytyczny", gdy – na przykład – zagrożone zostały czyjeś interesy gospodarcze w wyniku ujawnienia jakichś niewygodnych informacji. Za niezastosowanie poleceń	koordynacji i odpowiednio szybkiej reakcji na zażeganie sytuacji kryzysowej wywołanej cyberatakiem (polecenie zabezpieczające).

			zabezpieczających ma grozić kara pieniężna, jeszcze nie wiadomo w jakiej wysokości, bo tu w projekcie wydaje się być luka. Jest to zagrożenie dla wolności słowa i furtka do stosowania faktycznej cenzury w cyberprzestrzeni. Dla ochrony przed cyberatakami wystarczy jedynie instytucja ostrzeżeń. W związku z powyższym apeluję o wykreślenie z projektu przepisów dotyczących „poleceń zabezpieczających".	
15.	Izba Przemysłowo-Handlowa Polska-Azja	Uwaga ogólna	**Prace Legislacyjne** Charakter proponowanym przez Resort zmianom nadały między innymi **ostatnie** **ustalenia na poziomie europejskim**, a więc **Europejski Kodeks Łączności Elektronicznej oraz zalecenia Komisji Europejskiej, dotyczące bezpieczeństwa 5G.** Nowy projekt wdraża zalecenia i standardy opublikowane **w tak zwanym 5G Toolbox**, czyli **zestawie narzędzi** przygotowanych przez Komisję Europejską i Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Czy nasi Partnerzy w UE pracują nad podobnymi czy tożsamymi rozwiązaniami jakie zaproponował Resort Cyfryzacji w tym zakresie ? Przy wyborze dostawcy sprzętu i oprogramowania uwzględniane będą: • analiza zagrożeń bezpieczeństwa narodowego o charakterze **ekonomicznym, kontrwywiadowczym i terrorystycznym** oraz zagrożeń dla realizacji **zobowiązań sojuszniczych** i europejskich; • prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się **pod wpływem państwa spoza UE lub NATO**, • jaki jest stopień i rodzaj powiązań pomiędzy dostawcą i tym państwem, **jakie jest prawodawstwo** tego państwa w zakresie **ochrony praw obywatelskich i praw człowieka**,	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			• jakie w tym państwie istnieje **prawodawstwo w zakresie ochrony danych osobowych**, • **strukturę własnościową** dostawcy sprzętu lub oprogramowania, • **zdolność ingerencji państwa** spoza UE lub NATO w swobodę działalności gospodarczej dostawcy. MC chce, by ustawa weszła w życie 21 grudnia br. – tj. wraz z ustawą – Prawo komunikacji elektronicznej. W efekcie na prace wewnątrz Rządu i w Parlamencie pozostaje niewiele czasu na debatę i poważny proces legislacyjny. **Rola i skład Kolegium ds. Cyberbezpieczeństwa** Oceniające dostawców **Kolegium ds. Cyberbezpieczeństwa** powstało przy Radzie Ministrów na mocy ustawy KSC z 2018 r. **Przewodniczy mu premier**, a zasiadają w nim: pełnomocnik rządu ds. cyberbezpieczeństwa, szefowie resortów właściwych do spraw wewnętrznych, informatyzacji, służb specjalnych, obrony narodowej i spraw zagranicznych, a także szef Kancelarii Prezesa Rady Ministrów i szef Biura Bezpieczeństwa Narodowego. **Przewodnictwo Premiera** Uważam, że w tym rozwiązaniu kryją się duże ryzyka, bowiem będą przenosić każdą decyzję Kolegium od razu w przestrzeń dyplomatyczną i polityczną. Rozumiem, że taka przyjęta konstrukcja miała pokazywać wagę państwową cyberbezpieczeństwa. Jednak w praktyce, tym bardziej, że po drugiej stronie procesu decyzyjnego będą stały często międzynarodowe konsorcja firm czy globalne firmy, w efekcie będzie dochodzić do dodatkowych napięć, konsekwencji czy reakcji nie tylko po stronie właścicieli czy udziałowców firm, ale też polityki i dyplomacji ich Państw.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

			Dzisiaj, ze zrozumiałych względów, mówimy o koordynacji działań wynikających z naszego członkostwa w NATO czy UE, ale nie da się wykluczyć sytuacji, także znaczących, różnic interesów przy kolejnych decyzjach dotyczących już tylko firm państw członkowskich NATO czy UE. W efekcie, każdy polski wybór techniki, technologii czy partnera może skutkować oskarżeniami o polityczną ingerencję bez dochowania zasad konkurencji i praw rynku i może tworzyć dodatkowy obszar konfliktu dla Premiera i Jego najbliższego otoczenia z zagranicznymi partnerami na innych płaszczyznach i w innych obszarach współpracy. Zwracam uwagę na te kwestie tym bardziej że pod osobistym kierunkiem i głosem stanowiącym Premiera analizowane będą: • jaki jest stopień i rodzaj powiązań pomiędzy dostawcą i tym państwem, **jakie jest prawodawstwo** tego państwa w zakresie **ochrony praw obywatelskich i praw człowieka**, • jakie w tym państwie istnieje **prawodawstwo w zakresie ochrony danych osobowych**, • **strukturę własnościową** dostawcy sprzętu lub oprogramowania, • **zdolność ingerencji państwa** spoza UE lub NATO w swobodę działalności gospodarczej dostawcy. **Odpowiedzi na te pytania, tak zredagowane będą miały określoną siłę w dyplomacji i polityce międzynarodowej, często zapewne także** **stygmatyzującą międzynarodowych Partnerów.** Tak Pan Premier i kierownictwo Państwa poprzez obecne możliwości (rozwiązania ustawowe, procesy przetargowe etc) ma skuteczny wpływ na proces decyzyjny. Jeśli Pan Minister będzie zainteresowany, to przekażę kilka moich praktycznych doświadczeń w tym zakresie (na przykład realizacji	musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			umów offsetowych i konsekwencji przeniesienia relacji firmy atlantyckie czy europejskie-Państwo Polskie z poziomu rynkowo-operacyjnego na poziom dyplomacji i polityki). Problem pominięcia ofert czy wykluczenia z przetargów może też wydarzyć się w przyszłości w relacjach z firmami z Krajów NATO czy UE. **Do tego jeszcze dochodzi konstrukcja rozpatrywania odwołań od decyzji. Planuje się, że odwołania będzie rozpatrywał ten sam skład decydentów co na 1 etapie postępowania.** Podjęto, i słusznie, już ważne decyzje kierunkowe o tym, że **sieć 5G zbuduje w Polsce spółka POLSKIE 5G, w której dominującym podmiotem będzie Skarb Państwa i to Państwo w ramach tej spółki wybierze technologię i ewentualnych dostawców techniki i technologii. Proces ten ze względu na decyzje o udziale kapitałowym i decyzjach personalnych będzie transparentnie monitorowany i zarządzany przez stosowne organa z kierownictwem Państwa na czele.** **Doświadczenia Komitetu Offsetowego są jak najbardziej pozytywne** **i nie wymagają bezpośredniego zaangażowania w proces decyzyjny w ocenie propozycji firm Premiera co grozi konsekwencjami napięć dyplomatycznych i politycznych. Państwo poprzez spółkę POLSKIE 5G będzie decydowało, jakie rozwiązania technologiczne, techniczne i oprogramowanie przez jaką firmę dostarczone będą stosowane w Polsce**. Polskie 5G *ma być właścicielem jednolitej infrastruktury dla pasma 700 a Skarb Państwa ma zapewnić pasmo 700 MHz oraz dostęp do infrastruktury pasywnej na własnych nieruchomościach, a wybrane współpracujące podmioty prywatne ewentualnie dla potanienia procesu istniejącą albo*	

			rozbudowywaną infrastrukturę pasywną i aktywną (aport lub długoletnie dzierżawy) oraz ewentualne środki finansowe. **Jakie wnioski Resort Cyfryzacji wyciągnął z wdrożonych już rozwiązań i podjętych decyzji przez Kraje UE i NATO? Jak widzi analizowane i dyskutowane propozycje rozwiązań zapewniających cyberbezpieczeństwo w innych Krajach UE i NATO? Na przykład Wielkiej Brytanii?** Brytyjskie telekomy po 31 grudnia 2020 roku nie będą mogły kupować sprzętu 5G od pozaeuropejskiego dostawcy, a jeśli już takiego używają, muszą go usunąć ze swoich sieci do 2027 roku. Izba Gmin podjęła decyzję o zakazie współpracy operatorów telekomunikacyjnych w Wielkiej Brytanii z jednym producentem przy rozbudowie sieci. Decyzja jest konsekwencją sankcji, które na tę firmę nałożyły władze amerykańskie. Oliver Dowden, sekretarz ds. cyfryzacji poinformował, że łączny koszt tego i wcześniejszego ograniczenia nałożonego na dotychczasowego dostawcę na początku roku, wyniesie **do 2 mld funtów**. W związku z decyzją podjętą przez Izbę Gmin, po **31 grudnia tego roku** brytyjscy operatorzy nie będą mogli współpracować z tą firmą przy rozbudowie swojej infrastruktury sieciowej. Dodatkowo, **do 2027 roku muszą zdemontować wszystkie urządzenia sieciowe 5G tego producenta, jeśli takie już posiadają**. Ponieważ **amerykańskie sankcje dotyczą tylko przyszłego sprzętu, brytyjski rząd poinformował, że nie ma wystarczającego uzasadnienia dla usuwania urządzeń 2G, 3G i 4G.** Najnowsze ograniczenie może mieć wpływ również na szerokopasmowe łącza stacjonarne. Rząd Wielkiej Brytanii chce, aby telekomy całkowicie zrezygnowały z kupowania sprzętu od tej firmy, także w przypadku łączy światłowodowych. Według Ministra Dowdena ma się to stać w ciągu dwóch	

			lat. Dodatkowy czas ma zapobiec uzależnieniu się Wielkiej Brytanii od Nokii, jako jedynego dostawcy niektórych urządzeń. **Budując sieci telekomunikacyjne operatorzy nie będą mogli się zaopatrywać u dostawców uznanych za firmy wysokiego lub umiarkowanego ryzyka.** **Urządzenia i oprogramowanie kupione wcześniej od tych pierwszych trzeba będzie usunąć z sieci najpóźniej w ciągu pięciu lat.** Ministerstwo w uzasadnieniu projektu przyznaje, że nakładając na firmy nowe obowiązki, „ogranicza się konstytucyjną wolność gospodarczą", tłumacząc to celem, którym jest „zapewnienie bezpieczeństwa w cyberprzestrzeni". Pański Resort cyfryzacji przyznaje, że dostosowanie się do wymogów ustawy oznacza koszty dla przedsiębiorców. W uzasadnieniu podkreśla jednak, że to inwestycja „we własne cyberbezpieczeństwo" pozwalająca „skuteczniej dbać o cyberbezpieczeństwo w swojej działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat". **Mam nadzieję, że Resort starannie rozpatrzył w tej sprawie możliwe roszczenia podmiotów rynkowych od Skarbu Państwa.** Przypomnę, że jeszcze borykamy się z konsekwencjami decyzji z 2016 r. w obszarze energetyki wiatrowej, kiedy to decyzje podjęte na poziomie menedżerskim, a nie państwowym, doprowadziły do konieczności ugód i wymuszonych przejęć niezadowolonych z decyzji podmiotów prywatnych w tym także kapitału obcego z ewidentną stratą Skarbu Państwa. **Europa może mieć wielką trudność w rezygnacji z dostaw od pozaeuropejskiego dostawcy, gdyż podstawą budowy sieci 5G ma być starsza sieć 4G, tymczasem w 16 państwach europejskich sieci 4G/LTE w ponad 50 proc. zostały zbudowane z wykorzystaniem sprzętu pozaeuropejskich dostawców. W**	

			Polsce wskaźnik ten wynosi 60 proc. Takie estymacje przedstawiła duńska firma Strand Consult, która przeanalizowała **i**nfrastrukturę sieci 4G u 102 operatorów obsługujących w sumie 673 mln **u** żytkowników telefonów komórkowych. Stuprocentowy udział pozaeuropejskiego sprzętu jest w Belgii, na Cyprze i Wyspach Owczych. **W Polsce jest to 60 proc. –** przy czym w sieci 4G Plusa nie ma wcale, w sieciach Orange i T-Mobile jego udział Strand ocenia na 70 proc., a w Playu – na 90 proc. (udział w proc. jest obliczony według liczby abonentów podłączonych do sieci zbudowanej ze sprzętu danego dostawcy). W Niemczech udział pozaeuropejskich dostawców wynosi 57 proc., na Węgrzech 55 proc., w Wielkiej Brytanii 40 proc., a we Francji 25 proc. Najmniej – 6 proc. – pozaeuropejskiego sprzętu stosuje Słowacja. **Według umiarkowanego scenariusza budowa 5G bez wiodącego do tej pory pozaeuropejskiego dostawcy miałaby europejskie telekomy kosztować dodatkowo 3 mld euro rocznie przez 10 lat – czyli prawie o jedną piątą zwiększyć nakłady na nową sieć. To koszt dla 27 państw UE oraz Wielkiej Brytanii, Norwegii, Szwajcarii i Islandii. Na Polskę przypada z tej sumy 120 mln euro rocznie. Optymistyczny scenariusz to 1,4 mld euro wydatków dla 31 państw, a pesymistyczny – 4,5 mld euro.** Dostawcami na polskim rynku są chiński Huawei, szwedzki Ericsson i fińska Nokia. Szef działu analiz Haitong Banku Konrad Księżopolski wyliczył łączny koszt wymiany obecnie zainstalowanego w sieciach 4G/5G sprzętu pozaeuropejskiego dostawcy na 2,5–2,9 mld zł. Największa kwota – 1,3–1,5 mld zł – przypada na Play, po ok. 0,55–0,6 mld zł będzie to kosztowało Orange i T-Mobile, a 100–200 mln zł – Polkomtel. Wyliczenia mogą być obarczone „istotnym ryzykiem błędu” ze względu na bardzo	

			ograniczony dostęp do danych i nie obejmują kosztów uruchomienia sieci 5G, a jedynie wymianę starego sprzętu. Dla porównania: w USA Huawei ma 3,3 tys. anten 4G. A według oficjalnych danych przytaczanych przez amerykańskie media usunięcie tego sprzętu będzie kosztować 1,9 mld USD czyli ponad 7 mld zł. W Polsce trzej operatorzy - T-Mobile, Orange i Play - korzystają w sumie z 20 tys. anten. Jedynym telekomem, który nie poniesie strat związanych z wejściem w życie tego prawa, jest Plus w zdecydowanej większości korzystający z anten szwedzkiego Ericssona. Orange i Play to pod względem liczby obsługiwanych kart SIM to **największe firmy telekomunikacyjne w Polsce**. Pierwsza na koniec czerwca br. zanotowała wzrost o 3,5 proc. wobec ub.r. – do 15,49 mln kart. Play zaliczył zaś niewielki spadek o 0,1 proc. – do 14,98 mln. **Operatorzy staną więc przed niesamowicie trudnym wyborem**: wystąpić z roszczeniami wobec Państwa za nieplanowane dodatkowe koszty, czy najpierw budować nowoczesną sieć 5G, czy przeznaczać środki na odbudowę od podstaw istniejących sieci. A w końcu o przeniesieniu kosztów tej operacji na finalnego klienta. Nawet z tych szacunków widać, że polski rynek operatorów znajdzie się w nowych warunkach zdolności konkurencyjnych, bo nie wszyscy operatorzy będą musieli wydąć dodatkowo podobne środki na wymianę używanego sprzętu. **Dodatkowo nie znamy konsekwencji ograniczenia grona dostawców, czy nie zmniejszyłoby konkurencji i stanowiło bodziec do podwyżki cen sprzętu.** **I przyznam, że nie podzielam w tej sprawie Pańskiego optymizmu:** *„Nie myślimy o żadnych rekompensatach ani nie jesteśmy przekonani, że sprzęt uznany za bezpieczniejszy koniecznie będzie*	

			również droższy. Dostawcy konkurują ze sobą w skali globalnej, część operatorów też działa w takiej skali. Liczymy, że to wpłynie hamująco na ceny". Moje wątpliwości budzi też założenie Resortu, że wymiana sprzętu pochodzącego od dostawcy wysokiego ryzyka i tak nastąpiłaby w procesie normalnego modernizowania sieci. **W rezultacie, taka decyzja bez rekompensat dla operatorów i wydłużenia czasu wymiany sprzętu może istotnie spowolnić rozwój sieci nowej generacji. Niejasne także pozostają konsekwencje proponowanych zmian dla pozostałych poza telekomunikacją, a już wdrożonych w technologiach pozaeuropejskich** **dostawców na przykład realizowanego przez PKP PLK Programu sterowania ruchem kolejowym. Czy zainstalowane w polskich transporcie, sterowaniu ruchem urządzenia także mają podlegać wymianie ?** PKP Polskie Linie Kolejowe od 2018 r. realizują projekt o nazwie: „Budowa infrastruktury systemu ERTMS/GSM-R na liniach kolejowych zarządzanych przez PKP PLK w ramach Narodowego Planu Wdrożenia ERTMS". Do końca tej dekady systemy ERTMS (który składa się z systemu ETCS i GSM-R) mają być zbudowane na tzw. sieci bazowej TEN-T. **Jakie będą konsekwencje dla modernizacji i inwestycji realizowanych na polskiej sieci kolejowej?** A przypomnę uzasadnienie dla powtórzenia aukcji o pasmo częstotliwości dla 5G: „Intencją rządu jest jak najszybsze wprowadzenie do Polski komercyjnie funkcjonującej **sieci piątej generacji (5G)** i dotrzymanie terminów określonych w Europejskiej Agendzie Cyfrowej. Dlatego mając na uwadze możliwe	

			konsekwencje, a także kwestie związane z bezpieczeństwem, podjęto decyzję o konieczności powtórzenia całego postępowania". **Jaka w nowej sytuacji jest więc prognoza uruchomienia 5 G w Polsce?**	
16.	TEP	Uwaga ogólna	Szanowny Panie Ministrze, odbywające się aktualnie konsultacje społeczne nad propozycją zmiany ustawy o krajowym systemie cyberbezpieczeństwa są korzystnym i potrzebnym procesem. Poprzez niniejsze pismo pragniemy wziąć udział w pracach nad nowymi przepisami, które są kluczowe zarówno dla branży, jak i dla polskich obywateli i przedsiębiorców. Cieszy nas, że rządzący chcą wysłuchać naszego głosu, który - w co głęboko wierzymy - będzie miał wpływ na ustanowienie możliwie najlepszych społecznie i gospodarczo przepisów, które będą zabezpieczały nasz wspólny narodowy interes. Jako jeden z podmiotów szczególnie zainteresowanych nowymi regulacjami chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby: a) naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów; b) wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży; c) pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko; d) Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania.	**Uwaga częściowo uwzględniona**
17.	KIKE	Uwaga ogólna	Biorąc pod uwagę możliwe ograniczenia w zakresie dostarczania sprzętu telekomunikacyjnego od określonych dostawców, wdrożona ustawa będzie miała niebagatelny wpływ nie tylko na działalność dostawców sprzętu, technologii i oprogramowania	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

			wykorzystywanego w sieciach telekomunikacyjnych, ale także na działalność samych operatorów telekomunikacyjnych zrzeszonych w Izbie. Wymiar faktyczny nowych regulacji wpłynie na ciągłość działania dostawców sieci i usług łączności elektronicznej oraz na konkurencję na rynku telekomunikacyjnym, co może mieć także istotne przełożenie na sytuację i interesy konsumentów, będących ostatecznymi odbiorcami usług telekomunikacyjnych, jak również będzie wpływać na dalszy rozwój społeczeństwa cyfrowego, co jest jednym z priorytetów Unii Europejskiej. Skutki te niestety nie zostały w dostatecznym stopniu przeanalizowane ani w uzasadnieniu, ani w Ocenie Skutków Regulacji.	przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
18.	KIKE	Uwaga rozdziału 4a	Przechodząc szczegółowo do uwag, zdaniem KIKE ustawa o krajowym systemie cyberbezpieczeństwa (dalej KSC) w ogóle nie powinna mieć zastosowania do operatorów telekomunikacyjnych, szczególnie z segmentu małych i średnich przedsiębiorców. Należy przypomnieć, iż KSC stanowi implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. (dalej Dyrektywa). Również nowelizacja jest motywowana jej implementacją. Zgodnie z motywem (7) Dyrektywy, Obowiązki nakładane na operatorów usług kluczowych i dostawców usług	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do

			cyfrowych nie powinny jednak mieć zastosowania do przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej w rozumieniu dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady, które podlegają szczegółowym wymogom w zakresie bezpieczeństwa i integralności ustanowionym w tej dyrektywie, ani nie powinny mieć zastosowania do dostawców usług zaufania w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014, którzy podlegają wymogom w zakresie bezpieczeństwa określonym w tym rozporządzeniu. Dyrektywa wprost wyłącza spod jej stosowania określonych przedsiębiorców, podlegających w zakresie cyberbezpieczeństwa innym regulacjom. Z tego względu podczas uchwalania KSC w 2018 roku, spod zakresu podmiotowego wyłączono przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów. Powyższe zostało podkreślone w uzasadnieniu do KSC, Wzorem podejścia przyjętego w dyrektywie 2016/1148 ustawa nie ma zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa. Dyrektywa w zakresie podmiotów wyłączonych spod jej stosowania nie uległa zmianie. Nie ma więc powodu ani podstawy, aby ponad 2 lata po uchwaleniu ustawy implementującej Dyrektywę zmienić zakres podmiotowy i objąć stosowaniem KSC przedsiębiorców, którzy dotychczas nie byli objęci regulacją. Zmiana terminologii – przedsiębiorcy telekomunikacyjnego na przedsiębiorcę komunikacji elektronicznej nie spowoduje, że podmioty te z dnia na dzień	właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			zmienią zakres swojej działalności, będą bardziej podatni na cyberzagrożenia i będą w stanie sprostać wymogom stawianym przez KSC. Co więcej, obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego są określone w dziale 1 rozdziale 5 projektowanej ustawy prawo komunikacji elektronicznej (projekt ustawy z dnia 29 lipca 2020 r. – dalej jako PKE). To przepisy PKE będą regulować, jakie obowiązki ciążą na przedsiębiorcach komunikacji elektronicznej. Zgodnie z przepisami PKE (art. 39 i nast. PKE) przedsiębiorcy komunikacji elektronicznej będą zobowiązani m.in. do zgłaszania Prezesowi UKE informacji o wystąpieniu incydentu, kwalifikując go zgodnie z rozporządzeniem wykonawczym. Ponadto przedsiębiorca komunikacji elektronicznej zobowiązany będzie do systematycznego przeprowadzania oceny wystąpienia sytuacji szczególnego zagrożenia czy podejmowania środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka. Nie ma zatem powodu, aby obowiązki w zakresie bezpieczeństwa sieci i usług rozdrabniać na dwie regulacje – KSC i PKE. Dodatkowo wskazać należy, że PKE zawiera własną definicję incydentu bezpieczeństwa. Nie ma potrzeb, aby obok tego pojęcia wprowadzać pojęcie incydentu telekomunikacyjnego. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (dalej EKŁE), którą implementuje PKE, również nie przewiduje innych, szczególnych obowiązków w zakresie bezpieczeństwa sieci i usług niż te już zaprojektowane w PKE. W szczególności EKŁE nie nakazuje stosowania Dyrektywy do	

			przedsiębiorców komunikacji elektronicznej czy też nie nakazuje jej stosowania w zakresie nieuregulowanym w EKŁE. Wszelkie odesłania do Dyrektywy zawarte w EKŁE dotyczą współpracy organów państwowych, a nie obowiązków poszczególnych przedsiębiorców komunikacji elektronicznej (patrz: motyw 98 EKŁE oraz art. 41 ust. 4 i 5 EKŁE).	

19.	KIKE	Uwaga ogólna	W zakresie nowych obowiązków niewynikających z PKE wskazać należy, że CSIRT MON, CSIRT NASK i CSIRT GOV w sektorze telekomunikacyjnym uzyskają nowe kompetencje kosztem uprawnień Prezesa UKE oraz CSIRT Telco. Incydenty telekomunikacyjne będą badane przez ww. CSIRT, co należy uznać za błędną regulację - w zakresie bezpieczeństwa usług komunikacji elektronicznej i sieci telekomunikacyjnych główną rolę powinny odgrywać wyspecjalizowane organy telekomunikacyjne. Art. 42 PKE będzie zobowiązywać przedsiębiorcę komunikacji elektronicznej do zgłaszania incydentu bezpieczeństwa Prezesowi UKE, wobec czego nie ma potrzeb, aby przedsiębiorca ten musiał dodatkowo zgłaszać wystąpienie incydentu telekomunikacyjnego do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV i obok tego do CSIRT Telco oraz współdziałać z nimi przy obsłudze incydentu (projektowany art. 20c ust. 1 i 3 KSC). Ocena Skutków Regulacji błędnie zakłada, że wobec przedsiębiorców telekomunikacyjnych nowelizacja będzie oddziaływać w ten sposób, iż będą oni *zobowiązani do zgłaszania incydentów do zespołów CSIRT, <u>zamiast</u> do UKE.* Obowiązek zgłoszenia incydentu do UKE wynikający z PKE będzie niezależny od obowiązku przewidzianego w KSC. Dodatkowo projektowany art. 26 KSC wyraźnie wskazuje na działania CSIRT MON, CSIRT NASK i CSIRT GOV przy badaniu m.in. incydentów telekomunikacyjnych oraz przygotowywaniu materiałów dla Pełnomocnika, gdzie wyklucza się zarówno Prezesa UKE jak i CSIRT Telco. Przedsiębiorcy telekomunikacyjni będą zatem zobowiązani zgłaszać ten sam incydent dwa razy – do Prezesa UKE (na podstawie PKE), oraz do zespołów CSIRT (na podstawie KSC).	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

20.	KIKE	Uwaga do art. 20d	Na uwagę zasługuje również szczegółowe wyliczenie elementów zgłoszenia incydentu telekomunikacyjnego, zaproponowane w projektowanym art. 20d KSC. Takie określenie elementów zgłoszenia nie występuje ex lege w PKE i jest ono zbyt szczegółowe, a wręcz nadmierne (np. wpływ na usługi kluczowe innych podmiotów, czego przedsiębiorca komunikacji elektronicznej może nie wiedzieć). Taka szczegółowość utrudni przedsiębiorcom telekomunikacyjnym zgłaszanie incydentów i będzie wprowadzać ich w błąd – przedsiębiorcy do zgłaszania incydentów telekomunikacyjnych będą zobowiązani do stosowania art. 20d KSC, a do zgłaszania incydentów bezpieczeństwa na podstawie PKE zobowiązani będą do stosowania formularza określonego w rozporządzeniu wydanym na podstawie art. 42 ust. 2 pkt. 2) PKE. Zdaje się, że przepisy z zakresu cyberbezpieczeństwa powinny być spójne, a uchwalenie takich samych obowiązków w dwóch odrębnych aktach prawnych i dołożenie kolejnych z tego samego zakresu, nie będzie sprzyjać spójności przepisów.	**Uwaga nieuwzględniona** Podobna szczegółowość zgłoszenia występuje przy art. 12 KSC.
21.	KIKE	Uwaga ogólna	Nowelizacja KSC rozszerza również kompetencje Kolegium. Zgodnie z art. 64 KSC Kolegium ma stanowić organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa. Zgodnie z projektowanymi przepisami art. 66a-66c KSC, Kolegium na wniosek jego członka może sporządzić ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (czyli	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z

			również sprzętu telekomunikacyjnego, zarówno wprowadzenia do użytkowania nowego jak i użytkowania starego), przekazywaną następnie Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". **Dostawca sprzętu podlegający ocenie nie ma realnej możliwości odwołania się od decyzji**. Po pierwsze, termin na ewentualne odwołanie od oceny określającej ryzyko jako wysokie, wynosi 14 dni od publikacji komunikatu. Oznacza to, że *de facto* dostawcy sprzętu będą musieli codziennie śledzić Dziennik Urzędowy w poszukiwaniu informacji, czy czasem nie zostali objęci oceną ryzyka, o której mowa w art. 66a KSC. Po drugie, ewentualne odwołanie wnoszone jest do tego samego organu, który wydał zaskarżaną ocenę. Mało prawdopodobne, aby Kolegium chciało dokonać samokontroli swojej oceny na korzyść odwołującego. Po trzecie, dostawca sprzętu w ogóle nie ma możliwości odwołania się od oceny Kolegium w przypadku, gdy ryzyko zostało ocenione jako umiarkowane lub niskie – w takiej sytuacji możliwe jest jedynie zgłoszenie środków zaradczych i planu naprawczego poniekąd przyjmując, że w takiej sytuacji ocena Kolegium nie podlega kontroli.	urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne

				związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy

				usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

22.	KIKE	Uwaga ogólna	Dalej, w przypadku oceny ryzyka określonego jako umiarkowane, podmioty krajowego systemu cyberbezpieczeństwa mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania (projektowany art. 66b ust. 2 pkt 2) KSC). Oznacza to, że podmioty korzystające ze sprzętu/oprogramowania danego dostawcy (w tym zrzeszeni w KIKE przedsiębiorcy), nie będą mogły dokonywać ani upgrade'u, ani update'u wykorzystywanych urządzeń/oprogramowania, co ma bezpośredni, negatywny wpływ na cyberbezpieczeństwo i jest wprost sprzeczne z celami KSC. Wszelkie luki zwiększające podatność sprzętu/oprogramowania na cyberataki usuwane są najczęściej poprzez aktualizację sprzętu/oprogramowania. Wyłączenie takiej możliwości spowoduje zmniejszenie poziomu cyberbezpieczeństwa, co stoi w sprzeczności z ogólnym celem KSC.	**Wyjaśnienie** Zrezygnowano z poziomów umiarkowany, niski, brak zidentyfikowanego ryzyka.

23.	KIKE	Uwaga ogólna	Cała powyższa koncepcja przeczy charakterowi Kolegium, które – pomimo, że ma być organem opiniodawczo-doradczym – będzie na podstawie art. 66a KSC wydawać opinie wywołujące wprost określone w art. 66b KSC skutki prawne w sferze praw i obowiązków stron. Może to być m.in. zakaz wprowadzenia do użytkowania sprzętu określonego dostawcy czy obowiązek wycofania jego sprzętu/oprogramowania z rynku. Kolegium będzie mogło arbitralnie wywierać wpływ na danego dostawcę decydując o tym, czy jego sprzęt lub oprogramowanie będzie mogło być użytkowane w Polsce czy nie. Jest to uprawnienie leżące poza kompetencjami opiniodawczo-doradczymi. Nie ma przy tym obiektywnych przesłanek, jakimi ja kierować się Kolegium przy dokonywaniu oceny.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie

24.	KIKE	Uwaga ogólna	Projektowany art. 66a ust. 4 KSC przewiduje, że przy wydawaniu oceny Kolegium ma się kierować m.in. tym, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniając jednocześnie: stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem, strukturę własnościową dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Są to nieobiektywne przesłanki niemożliwe do zweryfikowania bez podejmowania nadzwyczajnych środków kontrolnych. Kolegium nie ma instrumentów prawnych ani faktycznych aby badać strukturę własnościową zagranicznego dostawcy sprzętu/oprogramowania czy zdolność ingerencji państwa w swobodę działalności gospodarczej tego dostawcy. Powyższe wymagałoby również wnikliwej analizy prawodawstwa tego państwa w zakresie ochrony praw człowieka i ochrony danych osobowych. W konsekwencji Kolegium będzie mogło arbitralnie decydować o wykluczeniu z rynku określonego dostawcy sprzętu lub oprogramowania, pod pretekstem konieczności zapewnienia cyberbezpieczeństwa, co w praktyce będzie nieweryfikowalne.	**Uwaga nieuwzględniona** Kryteria oceny nawiązują do kryteriów określonych w Toolbox 5g.

25.	KIKE	Uwaga ogólna	Nie jest zrozumiałe, dlaczego pod uwagę mają być brane indywidualne cechy dostawcy, a pomijane będą najistotniejsze z punktu widzenia cyberbezpieczeństwa aspekty informatyczno-technologiczne. W infrastrukturze wykorzystywane są również urządzenia pasywne, co do których z punktu widzenia cyberbezpieczeństwa bez znaczenia jest, od jakiego są dostawcy. Konkludując, na podstawie opinii organu opiniodawczo-doradczego nie można zakazać korzystania z określonych urządzeń telekomunikacyjnych czy oprogramowania bez możliwości realnej obrony przed taką opinią przez zainteresowane podmioty, w tym przedsiębiorców telekomunikacyjnych, którzy będą zmuszeni ewentualnie ponieść koszt wymiany urządzeń dostawcy objętego oceną.	**Uwaga nieuwzględniona** Kryteria oceny nawiązują do kryteriów określonych w Toolbox 5g. Zawierają aspekty techniczne i nietechniczne.

26.	KIKE	Uwaga ogólna	Co ważne, przepisy projektowanych art. 66a-66c KSC nie mają oparcia w Dyrektywie. Procedura sprawdzająca dostawcę nie jest w niej przewidziana, a 5G toolbox przywołany w uzasadnieniu zawiera wytyczne wyłącznie w zakresie zapewnienia bezpieczeństwa przy wdrażaniu sieci 5G, a nie przy infrastrukturze jako takiej. Zgodnie z motywem (50) Dyrektywy, Mimo iż producenci sprzętu i twórcy oprogramowania nie są operatorami usług kluczowych ani dostawcami usług cyfrowych, ich produkty zwiększają bezpieczeństwo sieci i systemów informatycznych. Odgrywają oni zatem ważną rolę w umożliwianiu operatorom usług kluczowych i dostawcom usług cyfrowych zabezpieczenia ich sieci i systemów informatycznych. Taki sprzęt i oprogramowanie są już objęte obowiązującymi przepisami dotyczącymi odpowiedzialności za produkt. Dyrektywa (którą, jak podkreślamy, ma implementować KSC) nie przewiduje dodatkowej odpowiedzialności dostawców sprzętu czy oprogramowania. W polskim porządku prawnym dostawcy sprzętu i programowania odpowiadają za dostarczany produkt na podstawie art. 449^1 kodeksu cywilnego (odpowiedzialność za produkt niebezpieczny).	**Uwaga nieuwzględniona** Dyrektywa NIS pozwala na przyjmowanie środków z zakresu bezpieczeństwa, jakie Państwa Członkowskie uznają za stosowne. Art. 1 ust. 6 Dyrektywy NIS stanowi: *6. Niniejsza dyrektywa pozostaje bez uszczerbku dla działań podejmowanych przez państwa członkowskie w celu zagwarantowania ich podstawowych funkcji państwowych, w szczególności w celu ochrony bezpieczeństwa narodowego – w tym działań na rzecz ochrony informacji, których ujawnienie państwa członkowskie uważają za sprzeczne z podstawowymi interesami swojego bezpieczeństwa – oraz w celu utrzymania porządku publicznego, w szczególności w celu umożliwienia prowadzenia postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.* Odpowiedzialność z art. 449^1 KC dotyczy odpowiedzialności cywilnej za produkt niebezpieczny. Jest to relacja prywatnoprawna między producentem a osobą poszkodowaną. Odpowiedzialność następuje dopiero po wyrządzeniu szkody. Natomiast projektowane przepisy dotyczą sfery *imperium* Państwa, prawa administracyjnego. Państwo może przyjmować regulacje dotyczące wykonywania działalności gospodarczej, w celu ograniczenia ryzyka wystąpienia szkody, która będzie zagrażała
27.	KIKE	Uwaga ogólna	5G toolbox przewiduje, iż państwa członkowskie powinny mieć możliwość zastosowania odpowiednich ograniczeń dla dostawców uznanych za stwarzających wysokie ryzyko, w tym	**Wyjaśnienie** Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny

			niezbędnych wyłączeń w odniesieniu do kluczowych zasobów. Z powyższego wynika, że: - wobec dostawców uznanych za stwarzających wysokie ryzyko mogą być stosowane odpowiednie ograniczenia, - niezbędne wyłączenia mogą być zastosowane w odniesieniu do kluczowych zasobów, - 5G toolbox nie rozróżnia, czy chodzi o dostawcę pochodzącego z Europejskiego Obszaru Gospodarczego czy z państwa trzeciego, wobec czego (1) przesłanki i ograniczenia przewidziane w art. 66a-66b KSC są niewspółmierne, (2) nie ma wskazanych kluczowych zasobów, wobec których mogą być zastosowane wyłączenia o najdonioślejszych skutkach, (3) każdy dostawca powinien móc podlegać ocenie, również krajowy. W żadnym wypadku dokonując oceny Kolegium nie powinno kierować się przesłankami zaproponowanymi w projektowanym art. 66a ust. 4 KSC. Należy jeszcze podkreślić, że 5G toolbox stanowi tzw. soft law i nie jest instrumentem o takiej samej mocy prawnej jak inne akty prawne. Zgodnie z art. 288 Traktatu o Funkcjonowaniu Unii Europejskiej, źródłami prawa europejskiego są rozporządzenia, dyrektywy i decyzje oraz niemające wiążącej mocy zalecenia i opinie. Ustanawianie tak rygorystycznych, niewspółmiernych do celu i nieobiektywnych przesłanek nie może nastąpić w oparciu o soft law. Powielenie odpowiedzialności dostawców sprzętu w przepisach KSC powinno być zatem niedopuszczalne, szczególnie, że przepisy KSC wprowadzają odpowiedzialność za hipotetyczne, a nie stwierdzone niebezpieczeństwo i to nawet nie tyle samego wykorzystywanego sprzętu/oprogramowania, co osoby dostawcy w oparciu o nieobiektywne przesłanki. Nie ma w polskim porządku prawnym przepisu, który zezwalałaby na	technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą każdego dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną. Dostawca sprzętu lub oprogramowania zostanie uznany za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wyniknie, że stwarza poważne zagrożenie dla bezpieczeństwa narodowego.

			represjonowanie przedsiębiorcy z uwagi na kapitał, który za danym przedsiębiorcą stoi w oderwaniu od jakości produkowanego sprzętu. Jeśli przepisy KSC koniecznie mają regulować bezpieczeństwo sprzętu/oprogramowania, to powinny skupiać się na sprzęcie/oprogramowaniu jako takim (model sprzętu, wersja oprogramowania, itp.), w oderwaniu od podmiotu, który go dostarcza. Zaproponowane przesłanki mogą w konsekwencji doprowadzić do wykluczenia wszelkich dostawców sprzętu o kapitale spoza Unii Europejskiej. Z uwagi na dalekoidące skutki regulacji, KIKE wykonało badania, obejmujące szczegółową analizę dot. wykorzystania sprzętu dostawców spoza UE. Wyniki załączonego do niniejszego stanowiska Badania o skali wykorzystania w sektorze telekomunikacyjnym sprzętu dostawców pochodzących spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (dalej jako „Badanie"), potwierdziło, że czołowi producenci sprzętu elektronicznego, najczęściej wykorzystywanego do budowy sieci w Polsce, mają swoją siedzibę właśnie poza Unią Europejską lub Organizacją Traktatu Północnoatlantyckiego (NATO), co stwarza możliwość objęcia ich oceną ryzyka. Są to przede wszystkim: i. Dasan (siedziba Seongnam, Korea Południowa), ii. D-Link (Siedziba: Tajpej, Tajwan), iii. Huawei (siedziba: Shenzhen, Chiny), iv. TP-Link (siedziba: Shenzhen, Chiny), v. ZTE (siedziba: Shenzhen, Chiny), vi. ZyXEL (siedziba: Xinzhu, Tajwan). Sprzęt producentów azjatyckich średnio stanowi ponad 80% ogólnie wykorzystywanego przez ISP sprzętu. Co ważne, ponad połowa ankietowanych ISP posiada sieć zbudowaną na	

			asortymencie jednym dostawcy! Są to w największej mierze Huawei (45%), Dasan (21%) oraz ZTE (21%). Wykluczenie z rynku któregokolwiek z producentów azjatyckich może „pogrążyć" małego lub średniego operatora, który de facto zmuszony będzie wymienić wszystkie urządzenia na urządzenia innego producenta. Szacowane koszty takiej wymiany liczone są w milionach złotych. Na koszt taki składałyby się nie tylko wygenerowana liczba elektrośmieci (tj. liczba wycofanych urządzeń, w tym wydane abonentom routery czy dekodery, co dodatkowo porusza kwestię wpływu regulacji na ochronę środowiska), ale zakup nowych, często kilkukrotnie droższych urządzeń, wynagrodzenie dla osób mających wdrożyć zmiany – zapewnienie kompatybilności urządzeń, wymiana urządzeń w terenie, dostosowanie systemów informatycznych, itp. Już tylko sami ankietowani mali i średni operatorzy telekomunikacyjni oszacowali koszt ewentualnej wymiany na ponad 160 mln zł, a część z nich wprost wskazywała, że konieczność wymiany urządzeń skutkowałaby bankructwem firmy. Średni koszt wymiany sprzętu przypadający na jednego ankietowanego wyniósłby 2,99 mln zł. Gdyby założyć, że tego rodzaju skutki i w takiej skali dotkną każdego, aktywnie działającego na rynku przedsiębiorcę telekomunikacyjnego (a trzeba dodać, że skala finansowego zaangażowania operatorów dużych będzie zapewne na znacznie wyższym poziomie), to przyjmując liczbę aktywnych w Polsce przedsiębiorców telekomunikacyjnych (tj. takich, którzy składają raporty o swojej infrastrukturze) , których wedle raportów UKE na koniec 2019 było 3000 , finansowy wpływ na rynek będzie ogromny, sięgając kwoty niemal 9 mld (8.970.000.000 zł).	
28.	KIKE	Uwaga ogólna	Dalszym skutkiem uchwalenia nowelizacji KSC będzie zaburzenie konkurencji. Po pierwsze, konsekwencją zmuszenia operatora do	**Wyjaśnienie**

			wycofania sprzętu dostawcy azjatyckiego i zastąpienia go sprzętem innego dostawcy, będzie konieczność przekalkulowania swojej oferty. To użytkownicy końcowi poniosą finansowe konsekwencje nowelizacji. Oferty operatorów staną się droższe i przez to będą mniej atrakcyjne dla użytkowników końcowych, a w konsekwencji przestaną być konkurencyjne. Po drugie, operator taki nie będzie ryzykować wymiany sprzętu na sprzęt dostawcy „zwiększonego ryzyka" (tj. spoza UE/NATO), co do którego w najbliższym czasie również może zapaść decyzja o wykluczeniu z rynku. Dostawcy spoza UE/NATO staną się tym samym stygmatyzowani i to w oderwaniu od jakichkolwiek aspektów technicznych. Nie będzie istotne, czy sprzęt danego dostawcy rzeczywiście jest bezpieczny czy nie, tylko czy jest to dostawca spoza, czy z obszaru UE/NATO. Sami ankietowani wskazali, że 95% z nich wydało swoim abonentom w ramach umowy o świadczenie usług, urządzenie producenta spoza UE/NATO. Ankietowani zadeklarowali, że dotyczy to łącznie ok. 222.903 abonentów. Ewentualna konieczność wymiany tego sprzętu finansowo dotnie przede wszystkich tych ostatnich, poniosą oni bezpośrednie koszty wymiany urządzenia końcowego, oraz pośrednie koszty wymiany kompatybilnych z tymi urządzeniami urządzeń sieciowych operatora. Nadmienić należy, że projektowana regulacja stawia pod znakiem zapytania celowość wszystkich projektów POPC (w tym podłączenie do sieci szerokopasmowych placówek oświatowych), w których sprzęt jakiegokolwiek z ww. dostawców został wykorzystany. Zgodnie z podsumowaniem I, II i III naboru , w ramach projektów POPC zasięgiem zostało objętych łącznie 1 891 254 gospodarstw domowych oraz 13 246 placówek oświatowych. Wedle informacji przekazywanych przez członków Izby, w	Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą **każdego dostawcy sprzętu lub oprogramowania** dla podmiotów krajowego systemu cyberbezpieczeństwa. Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną. Dostawca sprzętu lub oprogramowania zostanie uznany za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wyniknie, że stwarza poważne zagrożenie dla bezpieczeństwa narodowego.

			znacznej mierze w takich projektach wykorzystywany był sprzęt ww. dostawców, co potwierdziło Badanie. Spośród operatorów realizujących POPC i OSE: - przy realizacji POPC (lub podobnego programu), 82% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła ok. 49,34 mln zł, - przy realizacji OSE, 90% operatorów zadeklarowało wykorzystanie sprzętu producenta spoza UE/NATO, gdzie szacowana łączna cena zakupu takich urządzeń wyniosła prawie 1,5 mln zł. Na zakup takich urządzeń wydane zostały środki publiczne w kwocie ponad 50 mln zł. Wykluczenie z rynku któregokolwiek z ww. dostawców spowoduje m.in. to, że placówki oświatowe (a więc podmioty z sektora finansów publicznych) korzystające ze sprzętu któregokolwiek z ww. dostawców, będą zmuszone do ich wymiany. Projektowana regulacja przyczyni się do stworzenia sytuacji konfliktogennych, gdyż pierwszymi podmiotami, do których będą kierowane roszczenia związane z koniecznością zmiany sprzętu, będą beneficjenci POPC – a więc w tym i zrzeszeni w KIKE przedsiębiorcy telekomunikacyjni. Co więcej, dalsze procedowanie zmian w przyjętym projekcie może doprowadzić do chaosu organizacyjnego i niewykonania projektu Ogólnopolskiej Sieci Edukacyjnej (OSE) a to z uwagi na to, że szerokie grono wykonawców korzysta właśnie ze sprzętu i oprogramowania dostawców spoza UE. Z punktu widzenia gospodarności – art. 44 ust. 3 pkt 1) ustawy o finansach publicznych, wydanie ponad 50 mln zł na zakup sprzętu, który następnie decyzją ustawodawcy najpewniej będzie musiał zostać wycofany z rynku, nie jest wydatkowaniem środków publicznych w sposób celowy i oszczędny. Urządzenia takie zostały zakupione	

			właśnie z uwagi na ich konkurencyjną cenę i wówczas nie było powodów aby przypuszczać, że w najbliższym czasie będą zagrożone koniecznością wycofania z rynku.	
29.	KIKE	Uwaga ogólna	Ocena Skutków Regulacji nie bierze pod uwagę jeszcze innych, istotnych kwestii – ewentualnych kosztów i roszczeń związanych z koniecznością wymiany użytkowanych urządzeń, jeśli zgodnie z KSC przedsiębiorcy komunikacji elektronicznej będą zmuszeni je wymienić, a także skutków („czarny PR") opublikowania w Dzienniku Urzędowym informacji Pełnomocnika zawierającej ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Są to koszty i roszczenia na chwilę obecną trudne do przewidzenia i oszacowania z uwagi na to, iż przesłanki, którymi ma się kierować Kolegium są nieobiektywne i nie pozwalają na przewidzenie, jaki dostawca może zostać wykluczony z rynku. Ryzyko to jest jeszcze wyższe, jeśli weźmie się pod uwagę fakt, że zgodnie z treścią obecnie obowiązującej ustawy Kolegium jest organem de facto politycznym, a nie specjalistycznym. Wykluczenie może zatem objąć teoretycznie każdego dostawcę spoza EOG. Stawia to przedsiębiorców komunikacji elektronicznej w stanie niepewności. Co więcej, nie wiadomo jakie przedsiębiorcom komunikacji elektronicznej będą przysługiwać roszczenia i przeciwko komu, skoro zgodnie z kodeksem cywilnym, przy ocenianiu bezpieczeństwa produktu nie bierze się pod uwagę cech dostawcy (w szczególności tego czy jest to dostawca spoza EOG czy też nie) lecz wyłącznie cechy samego produktu (tj. niebezpieczny jest produkt niezapewniający bezpieczeństwa, jakiego można oczekiwać, uwzględniając normalne użycie produktu).	**Wyjaśnienie** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.

30.	KIKE	Uwaga ogólna	Z kolei opublikowanie w Dzienniku Urzędowym informacji o konkretnym dostawcy sprzętu/oprogramowania może doprowadzić do nieuczciwej walki konkurencyjnej pomiędzy przedsiębiorcami działającymi na tym samym rynku, z których część korzysta ze sprzętu znajdującego się w opublikowanej informacji. Nie trudno wyobrazić sobie sytuację, w której dojdzie do masowego rezygnowania z usług konkretnego przedsiębiorcy telekomunikacyjnego przez abonentów tylko dlatego, że dojdzie do swoistej stygmatyzacji takiego przedsiębiorcy	**Uwaga uwzględniona** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania.
31.	KIKE	Uwaga ogólna	Mając na uwadze powyższe, KIKE rekomenduje: 1) pozostawienie wyłączenia wskazanego w art. 1 ust. 2 KSC tak, aby objąć wyłączeniem spod nowelizacji przedsiębiorców komunikacji elektronicznej, o których mowa w PKE. W konsekwencji część projektowanych przepisów (w szczególności art. 20a i nast. KSC) powinny zostać całkowicie usunięte. Uregulowanie tej samej materii w dwóch różnych aktach prawnych jest sprzeczne z zasadami legislacji i spowoduje wprowadzenie w błąd adresatów obowiązków. PKE będzie kompleksowo regulować obowiązki przedsiębiorców komunikacji elektronicznej w zakresie zgłaszania incydentów cyberbezpieczeństwa. Nie ma powodu, dla którego obowiązki te	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.

			powinny być powielone i rozszerzone w osobnym akcie prawnym;	Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
32.	KIKE	Uwaga ogólna	2) zapewnienie przejrzystego postępowania w zakresie art. 66A-66C KSC w oparciu o obiektywne, konkretne i niebudzące wątpliwości kryteria, w szczególności kryteria informatyczno-technologiczne, które powinny być nadrzędne przy podejmowaniu decyzji o wyłączeniu z rynku danego sprzętu; 3) zapewnienie dostawcy sprzętu, którego dotyczy postępowanie, możliwości czynnego udziału w każdym stadium postępowania. KIKE proponuje, aby wzorem postępowania przewidzianego w prawie przedsiębiorców, postępowanie mogło być przeprowadzone dopiero po uprzednim dokonaniu analizy prawdopodobieństwa naruszenia prawa w ramach wykonywania działalności gospodarczej (art. 47 ust. 1 prawa przedsiębiorców) oraz aby o zamiarze przeprowadzenia kontroli zawiadomić zainteresowany podmiot (art. 48 ust. 1 prawa przedsiębiorców). Umożliwi to podmiotowi zainteresowanemu możliwość wypowiadania się na bieżąco do uwag i spostrzeżeń Kolegium na każdym etapie postępowania i co ważne – zainteresowany podmiot będzie wiedzieć, że poddany zostaje kontroli;	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania.

			4) zobowiązanie Kolegium do wydania decyzji administracyjnej w przedmiocie uznania danego dostawcy za stwarzającego ryzyko dla cyberbezpieczeństwa – niezależnie od tego, czy ryzyko zostanie ocenione jako wysokie, umiarkowane, czy niskie. W każdym przypadku zainteresowany podmiot musi mieć możliwość obrony przed decyzją wywołującą tak dalekoidące skutki, co sprowadza się do rekomendacji opisanej w pkt. 5) poniżej; 5) zapewnienie dwuinstancyjności postępowania, oraz możliwość zaskarżenia decyzji organu dwuinstancyjnego do Sądu Administracyjnego. Kolegium nie może być jedynym, nieomylnym organem, którego decyzje nie podlegają kontroli. Regulacja w obecnym kształcie jest sprzeczna z konstytucyjną zasadą dwuinstancyjności postępowania administracyjnego. 6) wprowadzenie procedury, że publikacja ogłoszenia w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" można następować wyłącznie na podstawie ostatecznej decyzji, a ewentualne zaskarżenie decyzji do sądu administracyjnego wstrzymałoby publikację automatycznie. Mając na względzie daleko idące skutki rozszerzenia kompetencji Kolegium i Pełnomocnika, KIKE rekomenduje, aby zmienić treść projektowanych przepisów zgodnie z powyższymi rekomendacjami, jako że w obecnej treści są one wysoce szkodliwe, sprzeczne z Dyrektywą i nierealizujące 5G toolbox.	Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

33.	Huawei Polska	Uwaga ogólna	Zawartość projektu pozostaje w sprzeczności zarówno z polskim prawem, jak i prawem Unii Europejskiej, w szczególności: 1. Kryteria oceny ryzyka dostawcy zdefiniowane w projekcie to czynniki zupełnie nietechniczne: w tym m.in. relacje między dostawcą a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy, zdolność ingerencji kraju macierzystego w działalność dostawcy, itp. 2. Projekt ustawy daje Kolegium ds. Cyberbezpieczeństwa prawo wyboru dostawców dla operatorów telekomunikacyjnych, a rynek komercyjny podlega silnym wpływom politycznym, co nie sprzyja zachowaniu konkurencji rynkowej. 3. Ustawa nie precyzuje jednolitych i przejrzystych kryteriów oceny technicznej i nie określa zakresu ocenianych urządzeń: nabywcy są zobowiązani do zaprzestania zakupów wszystkich urządzeń od dostawców wysokiego / średniego ryzyka zidentyfikowanego przez rząd, a operatorzy są również zobowiązani do wycofania z użytkowania urządzeń dostawców wysokiego ryzyka w ciągu 5 lat. 4. Projekt dyskryminuje dostawców pochodzących spoza Unii Europejskiej oraz tych, którzy pochodzą z państw, które nie są członkami NATO. Projekt nie ustanawia ujednoliconych i przejrzystych kryteriów oceny, oraz nie spełnia wymogów w zakresie cyberbezpieczeństwa, a co więcej, narusza wiele przepisów polskiego prawa: 1. zasady praworządności, proporcjonalności, wolnego i równego handlu, o których mowa w art. 2, art. 14, art. 32 Konstytucji RP.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td>2. prawa podmiotu do udziału w procesie oceny na podstawie art. 9 Kodeksu Postępowania Administracyjnego.
3. przepisy art. 24 Kodeksu Cywilnego o ochronie praw osobistych podmiotów cywilnych.
4. podstawowe zasady wolnej konkurencji i wolnego rynku w polskim Prawie Konkurencji.
Jednocześnie, Projekt ten narusza również zasady Unii Europejskiej oraz Handlu Międzynarodowego, w tym:
1. zasadę niedyskryminacji oraz równego traktowania określone w art. 18 „Traktatów o Funkcjonowaniu Unii Europejskiej”, oraz w art. 20 i art. 21 Karty Praw Podstawowych UE.
2. art. 2 „Traktatu Północnoatlantyckiego”, określającego zasadę równości.
3. zalecenia „Nie wykluczania żadnego konkretnego kraju czy dostawcy” określonego w Toolboxie 5G Unii Europejskiej.
4. zasady Światowej Organizacji Handlu (WTO) dotyczące zasady wzajemności oraz klauzuli największego uprzywilejowania.
Regulacje przedstawione w Projekcie Ustawy noszą znamiona dyskryminacji i wykraczają daleko poza ustalenia dokonane przez kraje członkowskie UE, a także inne kraje na świecie:
<table>
<tr><th></th><th>Polska</th><th>Inne kraje UE (Niemcy, Szwecja, Finlandia itp.)</th></tr>
<tr><td></td><td>Dostawcy sprzętu</td><td>Operatorzy</td></tr>
<tr><td>Zakres oceny</td><td>Wyłącznie tożsamość dostawcy</td><td>Kluczowe urządzenia 5G</td></tr>
</table>
</td>
<td>zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.
W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.
Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku</td>
</tr>
</table>

			Kryteria oceny	Pod uwagę brane są wyłącznie czynniki nietechniczne: relacje między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i zdolność ingerencji kraju macierzystego w działalność dostawcy	1. Zarządzanie operatorów w zakresie cyberbezpieczeństwa. regulacyjne dokonują przeglądu z wyprzedzeniem, a później ew. nakładają kary. Brak wykluczeń poszczególnych dostawców a priori 2. Neutralność technologiczna: do oceny ryzyka używane są weryfikowalne standardy techniczne, takie jak mechanizm zapewniania bezpieczeństwa urządzeń sieciowych NESAS.		do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			Sposoby zarządzania	Zabrania się kupowania sprzętu i oprogramowania od dostawców wysokiego i średniego ryzyka.	Zarządzane są tylko krytyczne produkty i określone wrażliwe obszary.		
			Proces oceny	Bezpośrednie podejmowanie decyzji przez Kolegium ds Cyberbezpieczeństwa bez udziału interesariuszy z branży	1. Ocena sporządzona i decyzja podejmowana przez operatorów. Ocena może polegać na oświadczeniu złożonym przez dostawcę i fakcie, że kluczowe sprzęty dla bezpieczeństwa są certyfikowane. 2. Instytuty regulacyjne nakładają potencjalne karyna operatorów w		

					przypadku wykrycia ryzyk.	
			Projekt, który dotyczy zagadnienia cyberbezpieczeństwa, został opracowany w sposób, który wyklucza konkretnego dostawcę. Jeżeli firma Huawei zostanie wykluczona z listy dostawców sprzętu ICT w Polsce, spowoduje to straty gospodarcze szacowane na dziesiątki miliardów euro dla całego społeczeństwa i wygeneruje koszty dla branży ICT w wysokości 8,5 miliarda euro. W znacznym stopniu wpłynie to również na zaufanie inwestycyjne operatorów, może zmniejszyć ich gotowość do zakupu pasma częstotliwości i tym samym zmniejszy dochody z rządowej aukcji o setki milionów euro. Przewiduje się od 3 do 5 lat opóźnienia rozwoju sieci 5G w Polsce i krajowego procesu cyfryzacji, oraz negatywny wpływ na PKB dla wszystkich powiązanych branż szacowany na 3%, natomiast ceny taryf telefonii komórkowej dla użytkowników mogą wzrosnąć od 1 do 3 razy. Projekt wpływa na środowisko inwestycyjne w Polsce i kształcenie talentów teleinformatycznych z najwyższej półki. Sama firma Huawei zatrudnia w Polsce ponad 3000 osób, zatem polska kolebka talentów ICT w Europie również ulegnie degradacji. Projekt zahamuje rozwój 5G w Polsce, przez co zmniejszy się jej konkurencyjność jej gospodarki w erze cyfrowej. Jako technologia komunikacyjna nowej generacji o ultra-dużej przepustowości i ultra niskim opóźnieniu, 5G nie tylko zapewnia szybkie połączenia dla zwykłych obywateli, ale także umożliwia cyfrową rewolucję przemysłową tysięcy branż. A więc utrudnienie budowy sieci 5G spowoduje zahamowanie rozwoju polskiej gospodarki cyfrowej.	

			W związku z powyższym Polska, a nawet Unia Europejska, aktywnie wprowadza politykę promującą rozwój sieci komunikacyjnej 5G. Aby zapewnić harmonijny rozwój polskiej gospodarce ICT i stworzyć uczciwe i sprawiedliwe otoczenie rynkowe i przemysłowe, chcielibyśmy poprosić Państwa o ponowną weryfikację Projektu Ustawy. Równocześnie, chcielibyśmy zarekomendować następujące rozwiązania: **Opcja 1** Realizacja ostatniego rozporządzenia (z dnia 29 czerwca) dotyczącego cyberbezpieczeństwa i usunięcie klauzuli opartych na przesłankach politycznych czy dyskryminacyjnych z obecnego Projektu Ustawy o KSC. **Opcja 2** 1. Proces Uwzględnienie publicznych konsultacji i przeprowadzenie kompleksowej oceny (koszty, konkurencja, rozwój branży, ekonomia i praworządność); 2. Przedmiot oceny a) Powinien uwzględniać: krytyczny sprzęt i oprogramowanie 5G, a nie dostawcę; b) Powinien być oparty na faktach i obiektywnych kryteriach, a nie politycznych; c) Powinien być podejmowany przez wyspecjalizowaną instytucję, a nie Kolegium ds. Cyberbezpieczeństwa. 3. Korzystnym byłoby przyjęcie globalnych standardów, które są przyjęte w takich krajach jak Niemcy czy Korea Południowa - np. uzyskanie certyfikacji NESAS od GSMA. W trosce o zdrowy rozwój polskiej gospodarki cyfrowej mamy nadzieję i głęboko wierzymy, że niniejszy list dostarczy Panu rzetelną i bezstronną informację zwrotną. Jednocześnie, jako przedstawiciele Huawei, mamy nadzieję i prosimy o spotkanie z	

			Panem Ministrem, w celu omówienia Pana potencjalnych wątpliwości oraz w celu poinformowania o naszych przyszłych planach współpracy w Polsce. Z chęcią wysłuchamy Pańskiej opinii w tej sprawie.	
34.	Huawei Polska	Uwaga ogólna	Na wstępie chcielibyśmy podkreślić, iż w pełni rozumiemy i popieramy cel, jaki przyświeca autorom projektowanej ustawy, a jakim jest zwiększenie bezpieczeństwa infrastruktury i usług telekomunikacyjnych/teleinformatycznych. Zapewnienie bezpieczeństwa produkowanej infrastruktury i dostarczanych usług telekomunikacyjnych jest również priorytetem naszej spółki. Ważne jednak, aby środki do tego celu były przejrzyste, proporcjonalne i w sposób równy traktowały wszystkich zainteresowanych. Z tej perspektywy nie możemy nie zauważyć, że niektóre istotne proponowane w projekcie rozwiązania są nieobiektywne i mogą skutkować dyskryminacją podmiotową opartą o kryteria niekoniecznie związane z cyberbezpieczeństwem. Powyższe nie jest wyłącznie naszą opinią, ale podzielane jest przez innych przedsiębiorców z szeroko rozumianej branży telekomunikacyjnej i teleinformatycznej oraz ekspertów ds. cyberbezpieczeństwa. W efekcie działania zaproponowanych mechanizmów ustawowych może dochodzić do wykluczenia z polskiego rynku niektórych podmiotów dostarczających sprzęt lub usługi elektroniczne, bez jednoczesnego zwiększenia bezpieczeństwa sieci telekomunikacyjnych, w szczególności sieci 5G, a w niektórych sytuacjach nawet ze skutkiem w postaci pogorszenia tego bezpieczeństwa. wkontekście regulacji krajowych warto wziąć pod uwagę zdanie Rady Europejskiej, przedstawione na posiedzeniu w dniach 1-2 października 2020 r. (EUCO 13/20; CO EUR 10 CONCL 6). W punkcie 7 i 11 swojego stanowiska, Rada Europejska zatwierdziła	

			konkluzje z dnia 9 czerwca 2020 r. w sprawie kształtowania cyfrowej przyszłości Europy. Apeluje do UE i państw członkowskich o wykorzystanie przyjętego w dniu 29 stycznia 2020 r. unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G (Toolbox). Wskazuje jednak, że: • po pierwsze, ewentualne ograniczenia wobec dostawców wysokiego ryzyka, dotyczyć powinny tylko kluczowych aktywów określonych jako krytyczne i wrażliwe w unijnych skoordynowanych ocenach ryzyka; • po drugie, Rada Europejska podkreśla, że potencjalni dostawcy 5G muszą być poddawani ocenie opartej na wspólnych obiektywnych kryteriach. • po trzecie wreszcie, podkreśla, że UE pozostanie otwarta dla wszystkich przedsiębiorców przestrzegających europejskich norm i przepisów. Przedstawiony przez Ministra Projekt, wprowadza mechanizm szacowania ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa (art. 1 punkt 29 Projektu). Oceny takiej miałoby dokonywać działające przy Radzie Ministrów Kolegium ds. Cyberbezpieczeństwa („Kolegium”). Jeśli tak przeprowadzona ocena wskazałaby wysokie ryzyko konkretnego dostawcy, podmioty krajowego systemu cyberbezpieczeństwa (w tym m.in., po wejściu w życie przewidzianej w Projekcie zmiany art. 4 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa („KSC”), przedsiębiorcy telekomunikacyjni), nie mogłyby nabywać od takiego dostawcy sprzętu, oprogramowania czy też usług określonych w rozstrzygnięciu Kolegium, zaś w ciągu 5 lat od dnia ogłoszenia komunikatu o ocenie, musieliby taki sprzęt, oprogramowanie czy też usługi	

			wycofać z użytkowania. Dostawca taki mógłby również zostać wykluczony z ubiegania się o zamówienia publiczne. W hipotetycznym więc przypadku arbitralnego zakazania wykorzystywania w Polsce urządzeń i oprogramowania pochodzącego od podmiotów chińskich (np. Huawei lub ZTE), struktura krajowego rynku urządzeń radiowej sieci dostępowej zbliżyłaby się do ustabilizowanego duopolu. Realizacja takiego scenariusza z pewnością doprowadziłaby do wzrostu kosztów budowy sieci 5G w Polsce, opóźnienia w oddaniu jej do użytkowania, a w konsekwencji do wyższych cen dla abonentów. Dla poparcia tezy o szkodliwości sztucznego „przerzedzenia" polskiego rynku urządzeń radiowej sieci dostępowej wskazać można, iż Komisja Europejska nigdy nie wyraziłaby zgody na doprowadzenie do analogicznego skutku w wyniku fuzji lub przejęć przedsiębiorstw. W Wytycznych w sprawie oceny horyzontalnego połączenia przedsiębiorstw na mocy rozporządzenia Rady w sprawie kontroli koncentracji przedsiębiorstw (2004/C31/03) wskazała ona, że „połączenia na rynkach oligopolistycznych, powodujące wraz z obniżeniem presji konkurencyjnej pozostałych konkurentów wyeliminowanie istotnych ograniczeń związanych z konkurencją, które poprzednio nakładały na siebie łączące się strony, mogą również stworzyć istotną przeszkodę dla konkurencji, nawet jeśli istnieje niewielkie prawdopodobieństwo koordynacji pomiędzy członkami oligopolu. Rozporządzenie WE w sprawie kontroli łączenia przedsiębiorstw wyjaśnia, że wszystkie połączenia powodujące takie nieskoordynowane efekty zostaną również uznane za niezgodne ze wspólnym rynkiem". Zaniepokojeni możliwymi negatywnymi konsekwencjami przyjęcia Projektu w zaproponowanym brzmieniu, zarówno w stosunku do wszystkich przedsiębiorców działających w Polsce,	

			jak i do polskich konsumentów (o czym szerzej mowa w załączonej do niniejszego stanowiska „Analizie planowanej nowelizacji ustawy z 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa i jej konsekwencji" przygotowanej przez Squire Patton Boggs na zlecenie Huawei Polska sp. z o.o. w dniu 2 października br. zwanej dalej "Memorandum") pragniemy wskazać poniżej najważniejsze uchybienia Projektu, których usunięcie powinno zostać dokonane w toku dalszych prac legislacyjnych:	
35.	PIIT		Poniższe stanowisko przedstawia odniesienie do wszystkich kluczowych zidentyfikowanych obszarów projektu ustawy. Odnotowujemy przedstawione w tym zakresie uzasadnienie dotyczące konieczności przyspieszenia prac z uwagi na implementację Europejskiego Kodeksu Łączności Elektronicznej (EKŁE) do krajowego porządku prawnego, jednak **w naszej ocenie prezentowany projekt ustawy zdecydowanie wykracza poza zakres niezbędny do implementacji przepisów unijnych**, a zatem trudno uznać ww. uzasadnienie za trafne. Projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa (KSC) przedstawia plany bardzo istotnych, fundamentalnych wręcz reform w obszarze bezpieczeństwa, które jednocześnie wykraczają dalece poza zakres niezbędny dla implementacji EKŁE. Podkreślić należy, że **zakres przedłożonego do konsultacji projektu ustawy jest bardzo rozległy, a jego treść trudna w interpretacji, co dodatkowo potęguje skromna treść uzasadnienia, brak wcześniej dyskusji nad kształtem planowanych zmian z ich adresatami oraz nakładanie się przepisów na projektowane nowe Prawo Komunikacji Elektronicznej, i to na 3 miesiące przed jego planowanym wejściem w życie.** Tym samym, przedmiotowy **projekt powinien być procedowany jako odrębna inicjatywa legislacyjna, w warunkach**	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			<u>konstruktywnego dialogu</u> z podmiotami, do których kierowane są tak daleko idące zmiany i nowe obowiązki. W innym przypadku, z uwagi na pośpiech, jaki towarzyszy pracom nad PKE, kluczowa tematyka cyberbezpieczeństwa zostanie zatracona w masie innych przepisów i dogłębna debata, także na poziomie parlamentu nie będzie mogła się odbyć w sposób należny tak ważnym zmianom. Tymczasem, dla budowy systemu cyberbezpieczeństwa niezbędna jest dobra współpraca wszystkich podmiotów, która właśnie w ramach wspólnego dochodzenia do odpowiednich rozwiązań powinna być budowana. **W zakresie planowanego wprowadzenia mechanizmów oceny dostawców, niezależnie od dalszych uwag szczegółowych, <u>przede wszystkim uważamy, że faktycznie efektywnym narzędziem poprawy bezpieczeństwa będzie wprowadzenie i stosowanie mechanizmów certyfikacji, w szczególności opartych o unijny „Cybersecurity act”</u>**. Obszar sieci 5G jest jednym z obszarów jakie zostały zidentyfikowane do takiej certyfikacji, która powinna być uniwersalna i wymagana na poziomie całej UE. Jedynie w ten sposób UE będzie w stanie w spójny i oparty na merytorycznych przesłankach badać i dopuszczać lub odrzucać sprzęt lub oprogramowanie, które nie spełniają wymagań bezpieczeństwa. Ewentualna ocena w oparciu o kryteria nietechniczne powinna być rozważana dopiero w drugim kroku po ustabilizowaniu i ocenie stosowania mechanizmów certyfikacyjnych. Mając na uwadze powyższe, obok uwag szczegółowych (w dalszej części wystąpienia), **poniżej przedstawiamy nasze kluczowe postulaty oraz określenie ram nowelizacji.** Liczymy, że będą one podstawą do wspólnej dyskusji z Państwem, czy to podczas konferencji uzgodnieniowej, czy innej formule w ramach dialogu Projektodawcy z rynkiem.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

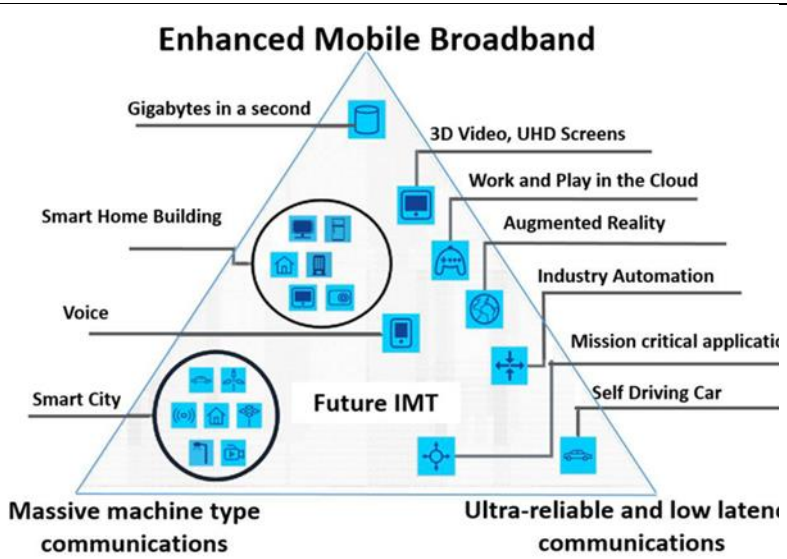
			1. **<u>Dotychczasowe wyłączenie przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania z zakresu obecnej regulacji ustawy KSC musi zostać utrzymane</u>**, z uwagi na fakt, że nawet, jeśli zostałyby wprowadzone dla nich dodatkowe obowiązki, z pozostałego zakresu ustawy KSC implementującego bezpośrednio dyrektywę NIS przedsiębiorcy ci muszą pozostać wyłączeni. 2. **<u>Na tym etapie należy zrezygnować z dodatkowej regulacji obowiązków przedsiębiorców komunikacji elektronicznej na gruncie ustawy KSC oraz włączenia tej kategorii przedsiębiorstw do krajowego systemu cyberbezpieczeństwa. Wdrożenie nowych obowiązków przedsiębiorców komunikacji elektronicznej jest niemożliwe w przewidzianym w projekcie ustawy terminie, a przedstawiony projekt przepisów jest jeszcze niedojrzały i wymaga dalszych istotnych prac, zarówno w zakresie samej koncepcji, jak i właściwego uzasadnienia i oceny skutków regulacji.</u>** Nie jest to niezbędne do wdrożenia z uwagi na transpozycję EKŁE, za takim rozwiązaniem nie przemawiają faktyczne potrzeby wskazane w uzasadnieniu, a wysoce problematyczny jest brak czasu na wdrożenie, dublowanie się obowiązków z tymi przewidzianymi już w PKE (także w zakresie cyberataków), niespójność i nierozłączność definicji incydentu, brak przepisów wykonawczych, czy nawet brak powołanego CSIRT Telco, wobec, którego miałaby być wykonywana część nowych obowiązków. Część przepisów PKE została przepisana do ustawy KSC bez wyjaśnienia intencji czy demarkacji, czego skutkiem byłoby np. wprowadzenie dwóch identycznych upoważnień do	musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			wydania rozporządzenia przez Ministra Cyfryzacji dla rozporządzenia w zakresie środków technicznych i organizacyjnych, jak i rozporządzenia w sprawie progów incydentów. Jednocześnie, absolutną koniecznością jest utrzymanie jednego kanału zgłaszania incydentów ze spójną siatką pojęciową, przejrzystą procedurą, nawet, jeśli miałby on zostać rozszerzony o dodatkowe zagadnienia związane z cyberbezpieczeństwem. Za zupełnie niezasadne uważamy przy tym całkowite przeniesienie obowiązków w zakresie bezpieczeństwa i integralności sieci i usług telekomunikacyjnych, z PT/PKE do KSC. Zakres ten jest o wiele szerszy niż samo cyberbezpieczeństwo i nie znajdujemy podstaw do takiego działania. Zakładamy, że znajdujące się w OSR sformułowanie, że *przedsiębiorcy telekomunikacyjni będą zgłaszali incydenty do zespołów CSIRT poziomu krajowego oraz do CSIRT Telco, zamiast do regulatora* ma charakter omyłki lub braku odpowiedniego zrozumienia charakteru incydentów zgłaszanych do UKE, z których większość to naruszenia wynikające z przyczyn fizycznych awarii lub problemów w systemach, a nie cyberataków. To UKE jako organ wyspecjalizowany w obszarze telekomunikacji jest właściwy od przyjmowania takich zgłoszeń oraz podejmowania w związku z nimi dalszych działań, w tym informowania podmiotów krajowego systemu cyberbezpieczeństwa jeśli incydenty. Warto w tym kontekście przypomnieć, że samo Ministerstwo Cyfryzacji w uzasadnieniu do przyjętego ostatnio rozporządzenia do art. 175d PT wskazało na marginalny udział cyberataków: *Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16*	Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE**.**

			naruszeń, przerwa w zasilaniu – 6, a błąd ludzki – 5. Marginalne były przyczyny spowodowane klęską żywiołową i cyberatakiem.”. 3. **Uwzględniając przedstawianą przez Ministerstwo Cyfryzacji ocenę o kluczowej roli sektora komunikacji elektronicznej dla spójności krajowego systemu cyberbezpieczeństwa uważamy, że <u>do dyskusji o rozszerzeniu aktualnych obowiązków należy wrócić po wdrożeniu ustawy PKE oraz w ramach trwającej aktualnie dyskusji na temat rewizji dyrektywy NIS</u>, której jednym z wątków jest właśnie włączenie przedsiębiorstw komunikacji elektronicznej do zakresu jej regulacji. Deklarujemy gotowość do udziału w takiej dyskusji** i wypracowaniu optymalnych i niezbędnych rozwiązań, w tym w zakresie ich spójności z obowiązującymi już regulacjami w zakresie obsługi i zgłaszania incydentów. Podobnie jak udało się to zrealizować w przypadku dyskutowanych i wydanych ostatnio rozporządzeń do art. 175d i 176a PT. Aktualnie jednak to implementacja EKŁE do krajowego porządku prawnego, a następnie wdrożenie ustawy PKE są absolutnie priorytetowe i z uwagi na bardzo krótkie terminy wejścia w życie będą stanowiły ogromne wyzwanie dla przedsiębiorców. W świetle tak znaczącej rewolucji porządku prawnego w obszarze komunikacji elektronicznej, w naszej ocenie konieczne jest urealnienie oczekiwań Projektodawcy w tym zakresie. 4. **<u>Projekt ustawy może, więc zostać ograniczony do wprowadzenia mechanizmów oceny dostawców, który wynika wprost z unijnych dokumentów takich jak tzw. 5G</u>**	

			<u>Toolbox</u>. Projekt ten powinien być procedowany odrębnie od projektu PKE. Kluczową osią naszych postulatów jest doprecyzowanie przepisów w taki sposób, aby uwzględnienie ewentualnych rekomendacji Kolegium odbywało się z poszanowaniem naturalnych procesów rozwoju i utrzymania, m.in. w zakresie sieci telekomunikacyjnych, tak, aby ograniczyć potencjalnie istotne skutki dla możliwości zachowania ciągłości i jakości usług dla ich użytkowników. 5. **<u>Procedura oceny powinna zostać wprowadzona zgodnie z zalecaniami Toolbox 5G,</u>** tj. w przypadku oceny ryzyka, jako wysokiego oraz ewentualnych restrykcji nakładanych na danego dostawcę powinny one być ograniczone do kluczowych zasobów (key assets). Zakres kluczowych zasobów powinien zostać określony na podstawie raportu w sprawie unijnej skoordynowanej analizy ryzyka oraz zakresu kluczowej infrastruktury określanej przez operatorów na podstawie par. 2 pkt 2 rozporządzenia do art. 175d PT, tj. *elementów infrastruktury telekomunikacyjnej i systemów informatycznych, których naruszenie bezpieczeństwa lub integralności będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy*. Potencjalnie możliwe byłoby na ich podstawie wydanie rozporządzenia określającego przekrojowo co jest rozumiane jako kluczowe zasoby na potrzeby oceny w zakresie 5G. Po drugie ocena powinna opierać się o jasne i precyzyjne kryteria. 6. Zauważamy również, że projekt ustawy może skutkować istotnym poziomem **ingerencji, również w działalność gospodarczą podmiotów prywatnych,** a także na świadczone przez nie usługi przy jednoczesnym dość ogólnym i w rzeczy samej, uznaniowym podejściu do określenia kryteriów opisu	

			sytuacji, w jakich po odpowiednie narzędzia, w szczególności Pełnomocnik Rządu może sięgać. Stąd, w poniższym stanowisku przedstawiamy nasze propozycje modyfikacji przedłożonego projektu. 7. Projekt ustawy powinien również uwzględnić podmioty, które działają na szeroko rozumianym rynku komunikacji elektronicznej. Warto wskazać, iż rynek telekomunikacyjny obecnie definiowany jest jako rynek komunikacji elektronicznej, na którym sieci oraz usługi dostarczają nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni ale również inne podmioty dzisiaj funkcjonujący poza rynkiem telekomunikacyjnym. 8. Punktem wyjścia jest przyjęcie założenia, iż przyszłe usługi łączności elektronicznej są (lub będą) świadczone w układzie trójkąta charakterystycznego dla sieci 5G:	



Dla tak sformułowanego trójkąta usług łączności elektronicznej, rozszerza się liczba podmiotów/funkcji realizowanych w ramach komunikacji. Usługi łączności elektronicznej to nie tylko połączenie głosowe, szybki dostęp do sieci Internet (enhanced mobile broadband) ale również:

- sieci dedykowane dla komunikacji masowej IoT np. LTE-M, NB-IoT (massive machine type communication),
- sieci o wysokich parametrach jakościowych np. campus network (ultra-reliable and low latency communication).

Dodatkowo sieci te będą świadczyć usługi w ramach tzw. network slicing, dedykując odpowiednie parametry jakościowe

			dla określonych usług np. usługi bankowe mogą wymagać wydzielonego zasobu sieciowego o określonych parametrach bezpieczeństwa, tworząc rozwiązanie E2E w ramach network slicing. Każdy podmiot, który bierze udział w realizacji komunikacji/przesyłaniu sygnałów jest podmiotem, który świadczy usługi łączności elektronicznej, czyli: • „tradycyjni" przedsiębiorcy telekomunikacyjni; • dostawcy urządzeń końcowych oraz systemów operacyjnych biorący udział w transmisji; • dostawcy rozwiązań chmurowych (np. Paas, Iaas); • dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0. (np. sieci campus network). Wszystkie te podmioty (nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni) powinny realizować działania w zakresie cyberbezpieczeństwa, w zależności od zakresu świadczonych usług oraz posiadanych możliwości technicznych, operacyjnych. Pominięcie, któregoś z tych podmiotów będzie oznaczało, iż albo część usług komunikacji elektronicznej nie będzie spełniać wymagań w zakresie cyberbezpieczeństwa (np. sieci prywatne różnych sektorów gospodarki, dostawców urządzeń końcowych wraz z oprogramowaniem). W tym zakresie niezbędne jest zweryfikowanie pojęć stosowanych w projekcie prawa komunikacji elektronicznej dotyczących przedsiębiorców świadczących usługi komunikacji elektronicznej oraz dostarczających sieci komunikacji elektronicznej, ponieważ projekt prawa komunikacji	

			elektronicznej wprowadza tutaj odmienne podejście od tego, co jest w przypisach europejskich. Przykładowo proponowane przepisy najprawdopodobniej nie będą dotyczyć: • dostawców urządzeń końcowych oraz oprogramowania, biorących udział w transmisji i świadczeniu usług (np. masowa usługa RCS). Wynika to z przyjętej definicji sieci telekomunikacyjnej (w projekcie PKE), który wyłącza urządzenia końcowe (w domyśle wraz z oprogramowaniem) z pojęcia sieci telekomunikacyjnej. Jest to odmienne podejście od zastosowane EKŁE, gdzie pojęcie sieci łączności elektronicznej nie wyłącza urządzeń końcowych. • dostawców rozwiązań chmurowych (np. usługi Paas, Iaas), pomimo tego, iż biorą udział w transmisji sygnałów. Wynika to z przyjętej definicji usługi komunikacji elektronicznej (w projekcie PKE), wyłącza usługi, które głównie nie zajmują się transmisji sygnałów. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie usług łączności elektronicznej obejmuje usługi, które częściowo (nie głównie, jak to jest w PKE), zajmują się transmisją sygnałów. • dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0., pomimo tego, iż realizują sieci oraz usługi, które mają bardzo często charakter kluczowy dla bezpieczeństwa określonych branż. Wydaje się, że wynika to z przyjętej definicji	

			przedsiębiorcy komunikacji elektronicznej (w projekcie PKE), która koncentruje się na dostarczaniu publicznych sieci telekomunikacyjnych. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie dostarczania sieci łączności elektronicznej abstrahuje od charakteru sieci, czy ma ona charakter publiczny, bądź niepubliczny oraz obejmuje urządzenia końcowe, które są zainstalowane w maszynach.	
36.	Business Centre Club	Uwaga Ogólna	W ocenie BCC jednym z podstawowych problemów dla sektora telekomunikacyjnego jest brak przyjaznego otoczenia prawnego, pozwalającego na sprawne i efektywne inwestowanie w infrastrukturę telekomunikacyjną. O istnieniu tych barier Pan Minister ma wiedzę, BCC bowiem dostrzega i docenia podejmowane od ponad 10 lat inicjatywy mające na celu ich likwidację. Tymczasem Nowela nie tylko nakłada na sektor telekomunikacyjny nowe obowiązki w zakresie cyberbezpieczeństwa, ale przede wszystkim projektuje rozwiązania, które na przedsiębiorców branży telekomunikacyjnej będą wywierać ogromy wpływ. Nowela może spowodować dla operatorów telekomunikacyjnych konieczność poniesienia trudnych do oszacowania nakładów inwestycyjnych związanych ze skutkami oceny ryzyka dostawcy sprzętu lub oprogramowania, jak również wydanych poleceń zabezpieczających lub ostrzeżeń. Ocena Skutków Regulacji Noweli zupełnie pomija aspekt finansowy i wpływ proponowanych rozwiązań na budżety poszczególnych podmiotów gospodarczych. Tymczasem, nie ulega wątpliwości,	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do

			że konieczność wycofania sprzętu lub oprogramowania danego dostawcy musi się wiązać z: 1. zakupieniem nowego sprzętu lub oprogramowania, 2. zutylizowaniem wycofanego sprzętu, 3. zawarciem nowych umów serwisowych i utrzymaniowych, 4. przeorganizowaniem struktury przedsiębiorstwa, w tym nabyciem nowych kompetencji przez osoby odpowiedzialne za obsługę nowego sprzętu lub oprogramowania, 5. przeprojektowaniem sieci celem dostosowania jej do nowego sprzętu i oprogramowania, w tym pozyskaniem nowych zgód w procesie inwestycyjnym, co stanowić będzie istotne, nieprzewidziane w normalnym trybie działalności nakłady finansowe. Sieci telekomunikacyjne to skomplikowane, składające się z wielu elementów przedsięwzięcia, które swoim zasięgiem pokrywają terytorium całego kraju. Zatem wycofanie sprzętu lub oprogramowania danego dostawcy będzie oznaczać dokonywanie modyfikacji w zakresie wszystkich tych elementów sieci. W konsekwencji Ocena Skutków Regulacji powinna jednoznacznie wskazywać na wpływ przepisów Noweli na gospodarkę krajową, w skali zarówno mikro, jak i makroekonomicznej. Odnosząc się do kwestii dotyczących ryzyka i rozwiązań w zakresie cyberbezpieczeństwa, BCC wyraża stanowisko, że kompromisowym rowiązaniem może być wdrożenie neutralnych technologicznie kryteriów oceny , a przedmiotem oceny ryzyka może być sprzęt i oprogramowanie uznane za krytyczne z technicznego punktu widzenia. BCC pragnie zwrócić uwagę, że	materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy

			istnieją rozwiązania w postaci norm technicznych i certyfikacji, umożliwiające obiektywną ocenę bezpieczeństwa sprzętu i oprogramowania. Są to przykładowo ENISA, czyli unijne ramy certyfikacji cyberbezpieczeństwa oraz NESAS, czyli schemat kompleksowego audytu cyberbezpieczeństwa, wypracowany wspólnie przez 3GPP i GSMA. W przypadku określenia wysokiego ryzyka sprzętu, oprogramowania i usług danego dostawcy, BCC wskazuje również na możliwość zastosowania podejścia geograficznego, czyli eliminacji danego sprzętu, oprogramowania czy usług z określonych obszarów, zdefiniowanych jako wrażliwe bądź krytyczne z punktu widzenia krajowego systemu bezpieczeństwa. Niniejsze podejście może stanowić *salomonowe* rozwiązanie, gwarantując wysoki poziom cyberbezpieczeństwa w wyżej wskazanych strefach, przy równoczesnym zapewnieniu ciągłości działania sieci komórkowych na obszarach nie będących strategicznymi z punktu widzenia krajowego systemu cyberbezpieczeństwa. W świetle powyższych uwag, zwracamy się z uprzejmą prośbą do Pana Ministra o ponowną, szczegółową analizę rozwiązań proponowanych w Noweli, w kontekście ich proporcjonalności, analizy alternatywnych rozwiązań dostępnych w obszarze cyberbezpieczeństwa oraz skutków wdrożenia przepisów w proponowanym kształcie dla sektora telekomunikacji w Polsce.	sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

37.	Digital Poland	Uwaga Ogólna	***Opis problemu*** Wedle rozdziału 4a KSC pt. „obowiązki przedsiębiorców komunikacji elektronicznej" integralną częścią krajowego systemu cyberbezpieczeństwa mają zostać „przedsiębiorcy komunikacji elektronicznej". Art. 2 pkt 41 projektu Prawa Komunikacji Elektronicznej (dalej „PKE") definiuje zbiór przedsiębiorców komunikacji elektronicznej jako przedsiębiorcy telekomunikacyjni **oraz podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów** (w rozumieniu art. 2 pkt 77 projektu PKE, którego nie ma potrzeby w tym miejscu przytaczać). W zakres drugiego z wymienionych podzbiorów wchodzi właśnie dostarczanie usługi poczty elektronicznej czy czatów internetowych, bowiem tak właśnie rozumie tę usługę motyw 17 zd. 1 EKŁE: „*Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych*". Podsumowując powyższych wątek definicyjny, wedle projektowanych przepisów **licznymi i bardzo kosztownymi obowiązkami w zakresie cyberbezpieczeństwa państwa winny zostać objęci również m.in dostawcy poczty elektronicznej.** ***Brak uzasadnienia*** Dla nałożenia takich ciężarów i obowiązków, które w wymiarze ekonomicznym mogą unicestwić ten sektor, nie ma żadnego racjonalnego uzasadnienia, poczynając już od tego, że usługa poczty elektronicznej zasadniczo różni się od usługi telekomunikacyjnej. Owa różnica jest wyraźnie wyeksponowana w motywie 95 EKŁE:	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			„Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. ***Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze*** *(*podkr. własne*). Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału”.* Wskazany motyw nakazuje zatem różnicowanie sytuacji prawnej podmiotów w zależności od ich faktycznego wpływu na bezpieczeństwo sieci. Poza sporem pozostaje, że dostawcy poczty elektronicznej nie sprawują faktycznej, realnej kontroli nad transmisją danych – inaczej niż przedsiębiorcy telekomunikacyjni, którzy dysponują	

			infrastrukturą techniczną. Ci ostatni, właśnie dla zapewnienia możliwości nieprzerwanej łączności telekomunikacyjnej, już obecnie posiadają wszelkie środki gwarantujące bezpieczeństwo sieci. Oczywiste różnice występują także na poziomie elementarnej charakterystyki obu usług. O ile niezagrożona ciągłość świadczeń telekomunikacyjnych leży w żywotnym interesie całego społeczeństwa (przykładowo, konieczne jest zapewnienie możliwości nawiązania kontaktu telefonicznego ze służbami ratowniczymi w dowolnym czasie), o tyle nie można tego samego powiedzieć o znaczeniu kontaktu emailowego. Jakkolwiek ten ostatni ułatwia życie i w znacznym stopniu wyparł choćby tradycyjną pocztę, to potencjalna szkodliwość mikroprzerw w dostawie tej usługi jest nieporównywalnie mniejsza. Pojawia się także argument ekonomiczny. W przypadku, gdyby nowym obowiązkom mieli podlegać jedynie rodzimi (tj. polscy) dostawcy usług, pojawiłby się kolejny problem swoistej wewnętrznej dyskryminacji konkurencyjnej wobec globalnych dostawców takich usług, których pozycja rynkowa i tak jest już hegemoniczna. Mając to na uwadze oraz dodając zwiększone obciążenie finansowe w prowadzeniu takiej usługi, przyszłość takich serwisów ze strony rodzimych przedsiębiorców stanęłaby pod znakiem zapytania.	
38.	Huawei Polska	Uwaga ogólna	**Zasada proporcjonalności** W myśl sformułowanej w art. 31 ust. 3 Konstytucji RP zasady proporcjonalności, wynikającej z zasady demokratycznego państwa prawnego, ustawodawca powinien, spośród dostępnych środków wybrać najmniej uciążliwy dla podmiotów nim	**Uwaga nieuwzględniona** Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego.

			dotkniętych, bądź zapewnić by środek ten był stosowany wyłącznie w zakresie niezbędnym do osiągnięcia określonego celu. Mechanizm oceny ryzyka dostawcy, który nie bazuje na obiektywnych kryteriach, może zatem naruszać tę zasadę[1].	
39.	Huawei Polska	Uwaga ogólna	**Prawo do sądu** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci telekomunikacyjnych, w tym 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci telekomunikacyjnych, w tym 5G w oparciu o nieokreślone kryteria, które nie zawierają elementów analizy technicznej. Nie gwarantują również możliwości realnego odwołania od oceny Kolegium. Wobec tego pojawia się istotna wątpliwość, co do zgodności z konstytucyjną zasadą prawa do sądu (art. 45 Konstytucji RP)[2].	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

[1] Patrz str. 7 Memorandum.
[2] Patrz str. 10 Memorandum.

				sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).
40.	Huawei Polska	Uwaga ogólna	**Ograniczenie konstytucyjnej swobody działalności gospodarczej** Zgodnie z art. 22 Konstytucji RP *„ograniczenie wolności działalności gospodarczej jest dopuszczalne tylko w drodze ustawy i tylko ze względu na ważny interes publiczny*". Ustawodawca powinien każdorazowo wskazać „ważny interes publiczny" uzasadniający wprowadzanie jakiegokolwiek rodzaju ograniczeń. Tymczasem w uzasadnieniu Projektu temu jakże ważnemu zagadnieniu poświęcono zaledwie jedno zdanie, będące raczej stwierdzeniem faktu aniżeli jakąkolwiek analizą: *„Poprzez nałożenie różnych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą*" (s. 33 uzasadnienia Projektu). W takiej sytuacji należałoby oczekiwać pełnego i wyczerpującego uzasadnienia, dlaczego ochrona cyberbezpieczeństwa uzasadnia tak daleko idące ograniczenia prawa prowadzenia działalności gospodarczej. W szczególności należy oczekiwać, że projektodawca przedstawi argumenty (i) dlaczego i w jakim zakresie, dobru w postaci zapewnienia cyberbezpieczeństwa, mają ustąpić inne dobra, takie jak chociażby swoboda prowadzenia działalności gospodarczej i (ii) czy proponowany środek jest właściwy dla realizacji zamierzonego celu oraz proporcjonalny i nie wykracza poza ograniczenia konieczne do osiągnięcia celu. Tej analizy w uzasadnieniu Projektu brakuje (patrz zasada proporcjonalności wyrażona w art. 31 ust. 3 Konstytucji RP)[3].	**Uwaga częściowo uwzględniona** Uwaga nieuwzględniona Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego. Temat zostanie szczegółowy omówiony w poprawionym uzasadnieniu.

[3] Patrz str. 7 Memorandum.

41.	Huawei Polska	Uwaga ogólna	**Brak zastosowania przepisów procedury administracyjnej** W projektowanych przepisach nie przewidziano prawa dostawcy do udziału w postępowaniu przed Kolegium. Należy zaznaczyć, iż z Projektu nie wynika w jakim trybie będzie prowadzone postępowanie przed Kolegium. Przede wszystkim brak jest odesłania do procedury administracyjnej, co narusza m.in. zasadę czynnego udziału stron w postępowaniu, w tym zasadę że przed wydaniem decyzji organ administracji obowiązany jest umożliwić stronom wypowiedzenie się co do zebranych dowodów i materiałów (str. 10 k.p.a.), zasadę pogłębiania zaufania uczestników postępowania do władzy publicznej (art. 8 k.p.a.) czy zasadę informowania stron postępowania przez organy administracji publicznej (art. 9 k.p.a.).	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).
42.	Huawei Polska	Uwaga ogólna	Rozwiązania zawarte w Projekcie, które mogą nakazać operatorom telekomunikacyjnym rezygnację z dostaw wiodącego dostawcy sprzętu do budowy sieci 5G oraz wymianę infrastruktury już istniejącej, mogą skutkować daleko idącymi, negatywnymi skutkami społecznymi (takimi jak likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy

			cyfrowego) oraz gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz ograniczenie konkurencji).	usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
43.	Huawei Polska	Uwaga ogólna	Projekt nie wskazuje także potencjalnych konsekwencji finansowych, jakie zaproponowane w nim rozwiązania mogą za sobą pociągnąć. W szczególności wyliczone powinny zostać konsekwencje finansowe w postaci możliwości wzrostu cen usług telekomunikacyjnych dla obywateli oraz kosztów dla operatorów telekomunikacyjnych, albowiem tylko wtedy można będzie dokonać prawidłowej oceny skutków finansowych wprowadzonych ograniczeń. Obywatele i operatorzy telekomunikacyjni powinni wiedzieć jakie będą skutki finansowe i gospodarcze proponowanych regulacji. Tymczasem w uzasadnieniu Projektu na s. 33, w części poświęconej skutkom gospodarczym i finansowym, w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia) i obowiązkach informacyjnych. Sugeruje się w ten sposób, że skutków takich nie będzie, co jest niezgodne z prawdą, albowiem wpływ taki może być liczony nawet w setkach milionów lub nawet miliardach	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

			złotych, zwłaszcza w przypadku konieczności usunięcia przez operatorów telekomunikacyjnych infrastruktury pochodzącej od określonego dostawcy. Brak analizy skutków gospodarczych i finansowych dla operatorów telekomunikacyjnych i obywateli stanowić może istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, tj. M.P. z 2016 r. poz. 1006) i może stanowić o naruszeniu zasady demokratycznego państwa prawa (art. 2 Konstytucji RP).	
44.	Huawei Polska	Uwaga ogólna	Istotnym argumentem, który należy podnieść, jest także kwestia niedopełnienia obowiązku notyfikacji Projektu Komisji Europejskiej, który to obowiązek nakłada na projektodawcę *Rozporządzenie Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych*[4]. Zgodnie z tym rozporządzeniem, projekty aktów prawnych zawierające przepisy techniczne powinny zostać notyfikowane Komisji Europejskiej, tak by ta mogła zgłosić do nich ewentualne uwagi i zmiany. Projektodawcy błędnie uznali, że Projekt nie zawiera przepisów technicznych i tym samym notyfikacji takiej nie dokonali[5].	**Uwaga uwzględniona,** projekt będzie notyfikowany.
45.	Huawei Polska	Uwaga ogólna	EKPC stwierdza, że: „Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych przez ustawę oraz zgodnie z ogólnymi zasadami	**Uwaga nieuwzględniona** Projekt jest zgodny z EKPCz.

[4] Rozporządzenie implementuje dyrektywę 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.
[5] Patrz str. 11 Memorandum.

			prawa międzynarodowego"[6]. W przypadku wejścia w życie Projektu, operatorzy telekomunikacyjni zostaną *de facto* wywłaszczeni z posiadanego sprzętu, w takim znaczeniu, iż będą oni zmuszeni do wycofania sprzętu, który wcześniej zakupili, mimo, iż gdyby nie projektowane rozwiązanie, mogliby z tego sprzętu korzystać w dalszym ciągu.	
46.	Huawei Polska	Uwaga ogólna	Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, są w naszej ocenie sprzeczne z podstawowymi zasadami równego traktowania i niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), zasada swobodnego przepływu towarów (art. 26, 28-37) czy zakaz ograniczeń swobody przedsiębiorczości (art. 49) TFUE. Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której „każdy jest równy wobec prawa". Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość". Trybunał Sprawiedliwości Unii Europejskiej zauważył, że „zakaz dyskryminacji (…) jest tylko konkretnym wyrazem ogólnej zasady równości, która wynika z podstawowych zasad prawa wspólnotowego, w myśl której porównywalne sytuacje nie mogą	**Wyjaśnienie** Projekt jest zgodny z prawem europejskim.

[6] Artykuł 1 Protokołu nr 1 do Konwencji o ochronie praw człowieka i podstawowych wolności.

			być traktowane w odmienny sposób, chyba że to rozróżnienie jest uzasadnione względami obiektywnymi”[7]. Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów.	
47.	Huawei Polska	Uwaga ogólna	W sprawie C-331/88 Fedesa Trybunał Sprawiedliwości Unii Europejskiej stwierdził, iż ażeby zastosowany środek ograniczający swobodę prowadzenia działalności gospodarczej uznać za proporcjonalny musi on być (1) odpowiedni i niezbędny do osiągnięcia celu jaki przyświeca ustawodawcy (2) jeśli istnieje wybór pomiędzy kilkoma środkami, należy wybrać ten który jest najmniej uciążliwy oraz (3) niedogodności spowodowane przez ten środek nie mogą być nieproporcjonalne w stosunku do zamierzonych celów. Wykluczanie sprzętu danego dostawcy, w oparciu o kryteria pochodzenia tego dostawcy (a nie obiektywne kryteria techniczne dotyczące określonego sprzętu) jest nadmiernym ograniczeniem swobody i środkiem nadmiernie uciążliwym w stosunku do celu, jakim jest zapewnienie cyberbezpieczeństwa sieci teleinformatycznych.	**Wyjaśnienie** Projekt jest zgodny z prawem europejskim.
48.	Huawei Polska	Uwaga ogólna	Dyrektywa Komisji 2002/77/WE z dnia 16 września 2002 r. w sprawie konkurencji na rynkach sieci i usług łączności elektronicznej („Dyrektywa o konkurencji”) zakazuje przyznawania wszelkich specjalnych praw w sektorze łączności	**Wyjaśnienie** Projekt jest zgodny z prawem europejskim.

[7] Wyrok TSUE z dnia 1 marca 2011 r. w sprawie C-236/09, Association belge des Consommateurs Test-Achats ASBL i inni p. Conseil des ministres, ECLI:EU:C:2011:100, pkt 28.

			elektronicznej. Mechanizm oceny dostawcy w kształcie zaproponowanym w Projekcie, bezpodstawnie przyznawałby prawa specjalne określonym kategoriom dostawców, odmawiając ich innym, co mogłoby stanowić naruszenie art. 2 Dyrektywy o konkurencji[8].	
49.	Huawei Polska	Uwaga ogólna	Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę największego uprzywilejowania. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne.	**Wyjaśnienie** Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.
50.	Huawei Polska	Uwaga ogólna	Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania „podobnych" produktów, usług i usługodawców zagranicznych i krajowych w równym stopniu. Zgodnie z nią, zagraniczne produkty, usługi lub usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobne" produkty, usługi lub usługodawcy krajowi (art. III GATT). Tymczasem, projektodawca koncentruje się na ocenie cech podmiotowych dotyczących dostawców, nie zaś na bezpieczeństwie sprzętu czy oprogramowania, jakie ten dostawca zapewnia. Jedną z istotnych cech branych pod uwagę przy szacowaniu ryzyka danego dostawcy jest kryterium pochodzenia tego dostawcy z danego kraju. Rodzi to ryzyko, że Polska naruszy umowy	**Wyjaśnienie** Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.

[8] Patrz str. 8 Memorandum.

			międzynarodowe, zakazujące dyskryminacji ze względu na pochodzenie[9].	
51.	Huawei Polska	Uwaga ogólna	Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku podmiotów reprezentujących kapitał zagraniczny, narusza zobowiązania Polski na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może skutkować uznaniem za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy porozumień dwustronnych łączących Polskę i Chiny[10].	**Wyjaśnienie** Projekt jest zgodny z prawem międzynarodowym.
52.	Huawei Polska	Uwaga ogólna	Postanowienia Projektu, w przypadku ich wejścia w życie mogą doprowadzić do wykluczenia z rynku dostaw sprzętu do budowy sieci telekomunikacyjnych 5G pochodzącego od niektórych dostawców. Środki przewidziane przez Projekt są nieproporcjonalne do celu jaki przyświecał projektodawcom, wprowadzają nadmierne ograniczenia swobody prowadzenia działalności gospodarczej i czynią to w oparciu o kryteria oceny, które mogą być uznane za dyskryminującej, subiektywne i niemierzalne. Dodatkowo, środki takie mogą naruszać szereg innych przepisów obowiązującego prawa (patrz pkt I powyżej).	**Wyjaśnienie** Przepisy zaproponowane w projekcie są proporcjonalne do celu.

[9] Sformułowany w Projekcie mechanizm oceny ryzyka dostawcy może potencjalnie naruszać także art. 18 TFUE, który zakazuje wszelkich form dyskryminacji ze względu na narodowość. Patrz też pkt II.2.3 niniejszego dokumentu.

[10] Umowa z 7 czerwca 1988 r. między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji; Umowa z 8 czerwca 2004 r. między Rządem Rzeczypospolitej Polskiej a Rządem Chińskiej Republiki Ludowej o współpracy gospodarczej.

53.	Huawei Polska	Uwaga ogólna	Wykluczenie z rynku jednego z wiodących dostawców technologii 5G, jak również konieczność ogromnych zmian w ramach sieci komórkowych; wprowadzenie sieci 5G w Polsce może się opóźnić o okres 3-5 lat;	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. . Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw.

				model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
54.	Huawei Polska	Uwaga ogólna	Z powodu braku konkurencji cena sprzętu bez wiodącego dostawcy rozwiązań 5G wzrośnie o przynajmniej 30%, a koszty usług telekomunikacyjnych mogą wzrosnąć nawet 3-krotnie;	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub

				oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. . Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
55.	Huawei Polska	Uwaga ogólna	Według prezentowanych na rynku analiz, koszt wymiany infrastruktury przez operatorów może sięgać 3 mld złotych	**Uwaga nieuzwględniona, patrz stanowisko do uwagi 53.**

			(podawane też wyższe kwoty)[11]. Może to w konsekwencji rodzić odpowiedzialność odszkodowawczą po stronie Skarbu Państwa.	
56.	Huawei Polska	Uwaga ogólna	Istnieje ograniczona liczba dostawców elementów sieci 5G w Polsce i na świecie. W sytuacji, gdy jeden z dostawców zostanie wykluczony, ograniczy to innowacyjność, opóźni wprowadzenie technologii 5G oraz znacząco zmniejszy konkurencję na rynku. W konsekwencji może to spowodować wzrost cen dla konsumentów.	**Uwaga nieuwzględniona** Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest neutralny technologicznie, co oznacza, że przepisy prawa dotyczące m.in. procedury oceny ryzyka dostawców sprzętu lub oprogramowania, w tym samym stopniu dotyczą każdego dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Projekt nie przewiduje automatycznego wykluczenia czy specjalnego traktowania żadnego z dostawców. Ewentualne decyzje o wycofaniu konkretnego sprzętu lub oprogramowania z użytkowania w podmiotach krajowego systemu cyberbezpieczeństwa będą poprzedzone transparentną – prowadzoną zgodnie z przepisami Kodeksu postępowania administracyjnego – procedurą oceny ryzyka zakończoną decyzją administracyjną. Co istotne, analizy duńskiej firmy konsultingowej Strand Consult wskazują, że ewentualne wykluczenie niektórych dostawców nie wpłynie znacząco na koszt budowy sieci 5G. Podaje się przykład zakupu w Stanach Zjednoczonych przez Nokię w 2016 r. firmy Alcatel Lucent.

[11] Patrz s. 9 Memorandum.

				Mimo tego, że rynek dostawców zmalał z trzech dużych dostawców do dwóch dużych i jednego mniejszego, paradoksalnie, zamiast podwyżki i monopolizacji, doprowadziło to zmniejszenia kosztów sprzętu telekomunikacyjnego4 . Należy również dodać, że każdy operator telekomunikacyjny ma własną strategię pozyskiwania unikalnego sprzętu dostosowanego do jego potrzeb. Niektórzy z klientów operatorów telekomunikacyjnych oczekują usług telekomunikacyjnych opartych o sprzęt pochodzący od zaufanych dostawców, ponieważ wcześniej zmagali się ze skutkami ataków hakerskich ze strony państwa pochodzenia jednego z dostawców. Dlatego też, operatorzy starają się dostosować do potrzeb swoich klientów.
57.	Huawei Polska	Uwaga ogólna	Argument bezpieczeństwa narodowego i cyberbezpieczeństwa sieci teleinformatycznych nie powinien być nadużywany. Nadal zastosowanie powinny mieć zasady proporcjonalności, obiektywności, przejrzystości i minimalnej ingerencji.	**Uwaga nieuwzględniona** Państwo musi dbać o swoje bezpieczeństwo narodowe. Projekt spełnia wymogi proporcjonalności opisane w Konstytucji.
58.	Huawei Polska	Uwaga ogólna	Opóźnienia w rozwoju i implementacji technologii 5G mogą utrudnić osiągnięcie przez Polskę korzyści z tytułu rozwoju tej technologii; korzyści te szacowane są na 10-13 mld euro[12].	**Uwaga nieuwzględniona** Koszty zagrożeń bezpieczeństwa narodowego mogą być większe niż korzyści z korzystania z niebezpiecznych rozwiązań technologicznych.

[12] Kwotę 13 mld euro podaje raport Oxford Economics https://www.oxfordeconomics.com/recent-releases/The-Economic-impact-of-restricting-competition-in-5g-network-equipment, s. 65. Kwotę 10 mld potencjalnych korzyści wskazuje raport Assembly Research https://www.assemblyresearch.co.uk/press-comments/poland-5g-delay

59.	Huawei Polska	Uwaga ogólna	Przyjęcie przepisów zaproponowanych w Projekcie może mieć negatywny wpływ na gotowość podmiotów do składania ofert na spektrum 5G.	**Uwaga nieuzwględniona,** patrz stanowisko do uwagi 53.
60.	Huawei Polska	Uwaga ogólna	Ograniczenie operatorów w zakresie możliwości wyboru dostawcy opóźni uruchomienie sieci 5G w Polsce od 3 do 5 lat, co może przełożyć się na utratę konkurencyjności polskiej gospodarki.	**Uwaga nieuwzględniona,** patrz stanowisko do uwagi 55.
61.	Huawei Polska	Uwaga ogólna	Przedsiębiorcy, których swoboda prowadzenia działalności gospodarczej została ograniczona mogą wystąpić z roszczeniami odszkodowawczymi wobec polskiego rządu.	**Uwaga niezuwględniona** Konstytucja pozwala na ograniczenie swobody prowadzenia działalności gospodarczej ze względu na ważny interes publiczny (art. 22 Konstytucji). Projekt jest proporcjonalny i adekwatny do celu, jakim jest zapewnienie bezpieczeństwa narodowego**.** Dalej patrz stanowisko do uwagi 53.
62.	Huawei Polska	Uwaga ogólna	Opóźnienie wdrożenia technologii 5G może wywrzeć negatywny wpływ na prawie 570 tys. nowych miejsc pracy, które mogą zostać utworzone dzięki technologii 5G[13].	**Uwaga niezuwględniona** Dalej patrz stanowisko do uwagi 53.
63.	Huawei Polska	Uwaga ogólna	Wyłączenie producenta, zwłaszcza wiodącego w branży ICT, spowoduje opóźnienie postępu w całym ekosystemie (patrz pkt III.2.2 powyżej). Projekt ustawy będzie miał negatywny wpływ na realizację agendy Przemysł 4.0.	**Uwaga nieuwzględniona,** patrz stanowisko do uwagi 55.
64.	Huawei Polska	Uwaga ogólna	**Normy techniczne i schematy certyfikacji**	**Uwaga nieuwzględniona,** Toolbox 5g wymaga także oceny ryzyka pod kątem nietechnicznym.

[13] Patrz raport Oxford Economics, s. 65.

			Projekt ustawy powinien raczej koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone, takich jak Network Equipment Security Assurance Scheme (NESAS)[14] czy system certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych przewidziany w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.. Proces analizy ryzyka powinien być zgodny z uznanymi międzynarodowymi standardami, również w zakresie wyboru strategii ograniczenia ryzyka. Zgodnie z najlepszymi praktykami, znajdującymi odzwierciedlenie między innymi w normie ISO 31000, unikanie ryzyka (np. przez eliminację dostawcy sprzętu) jest tylko jedną z siedmiu opcji postępowania z ryzykiem, a wybór adekwatnej opcji powinien być przedmiotem ustaleń pomiędzy podmiotem Krajowego Systemu Cyberbezpieczeństwa, a odpowiednim regulatorem rynku lub ministerstwem. •	
65.	Business Centre Club	Uwaga ogólna	**Opinia do projektu ustawy z punktu widzenia branż niereprezentujących bezpośrednio sektora ICT, m.in. farmaceutycznej.** Przedmiotowy projekt ustawy wprowadza istotne zmiany w trzech strategicznych, z punktu widzenia podmiotu prowadzącego działalność gospodarczą, obszarach: **1. w zakresie obowiązków operatora usługi kluczowej** - obecne rozwiązanie opierające się na wewnętrznych lub zewnętrznych Zespołach zmienia się na zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie (tzw. SOC), nakładając przy tym dodatkowe obowiązki (np. zgłoszeniowe, rejestracyjne w zakresie takiego zespołu);	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi.

[14] https://www.gsma.com/security/network-equipment-security-assurance-scheme/

			- nałożenie dodatkowych obowiązków na nowe zespoły np. w zakresie wprowadzania nowych zabezpieczeń, przeprowadzania analiz ryzyka **2. w zakresie uznawania, iż sprzęt lub oprogramowanie mają wysokie ryzyko dla cyberbezpieczeństwa państwa** - dotyczy m.in. operatora usługi kluczowej, - ocena bez wyraźnych kryteriów; - obowiązek wycofania sprzętu lub oprogramowania w ciągu 5 lat od komunikatu; - zakaz instalacji nowego sprzętu (zakaz wprowadzania do użycia); - wysoka kara za niedostosowanie się do oceny; - brak odpowiedzialności odszkodowawczej Skarbu Państwa; **3. Ostrzeżenia i polecenia zabezpieczające Pełnomocnika Rządu** - polecenie zabezpieczające ma formę decyzji administracyjnej o rygorze natychmiastowej wykonalności; - ostrzeżenia nie mają ustalonej formy; - nakaz określonego zachowania się, w tym zakaz zaprzestania użytkowania określonego sprzętu lub oprogramowania; - okres obowiązywania to 2 lata (ostrzeżenie może być jednorazowo przedłużone); - brak odpowiedzialności odszkodowawczej Skarbu Państwa; - dotyczy: • operatora usługi kluczowej również • właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym • przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3	Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców. Wprowadzenie powyższych rozwiązań doprowadzi do sytuacji, w której dotychczasowa praktyka dbania o bezpieczeństwo ogólne – Państwa, poprzez opracowanie i wdrożenie rozwiązań gwarantujących bezpieczeństwo na poziomie poszczególnych podmiotów zastąpione zostanie systemem nakazowym, w którym to organy Państwa będą decydowały o tym jak zadbać o bezpieczeństwo poszczególnych podmiotów. Takie podejście do systemu bezpieczeństwa elektronicznego jest daleko nieefektywne z punktu widzenia rachunku ekonomicznego a także zarządzania ryzkiem w przedsiębiorstwach. To podmioty stosujące na co dzień rozwiązania w zakresie bezpieczeństwa, dbając o swoje własne bezpieczeństwo poprzez stosowanie najlepszych praktyk i metodologii dostępnych na rynku, są najlepszym gwarantem tego bezpieczeństwa. Dotychczasowe rozwiązania, wypracowane wraz z rozwojem cyberbezpieczeństwa i funkcjonujące już od dłuższego czasu, sprawdzały się w dotychczasowej praktyce i są stosowane powszechnie na całym świecie. Ponadto podnieść należy, iż koszty ekonomiczne proponowanego rozwiązania mogą być niezwykle wysokie i mogą prowadzić do bezpośredniego zagrożenia egzystencji wielu podmiotów. Szczególnie rozszerzenie zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej może przynieść katastrofalne skutki. Samodzielne zarządzanie bezpieczeństwem opierające się na wewnętrznej, odzwierciedlającej własną architekturę, analizie i szacowaniu ryzyka spowodowały, iż podmioty zbudowały złożone i powiązane wzajemnymi	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

			zależnościami systemy zabezpieczeń. Zabezpieczeń analizowanych pod kątem swej skuteczności i aktualności w sposób ciągły, co jest krytyczne dla reagowania na często pojawiające się nowe zagrożenia. Systemy te, w zaproponowanym rozwiązaniu zawartym w projekcie ustawy, mogą być narażone na ograniczenie swojej funkcjonalności lub w ogóle na likwidację w oparciu o komunikaty bezpieczeństwa ogłoszone przez odpowiednie organy Państwa. Podkreślić przy tym trzeba, że wszelkie koszty związane z zawieszeniem i wymianą stosowanych rozwiązań zostały przerzucone w całości na podmioty, które już raz poniosły wymierne koszty. W tej sytuacji brak odpowiedzialności odszkodowawczej po stronie Państwa może spowodować, iż podmioty gospodarcze nie będą w stanie udźwignąć nałożonych na nie zobowiązań, nawet w perspektywie 5 letniej, jaka została założona na wymianę sprzętu uznanego za niebezpieczny. Do tego dołożyć należy również astronomiczne kary nałożone na operatorów usługi kluczowej za brak realizacji obowiązków określonych w projektowanej ustawie. Podkreślić również należy, iż brak jest jednoznacznych kryteriów jakimi mają posługiwać się organy administracji publicznej w ocenie dostawców sprzętu i oprogramowania. Nie zostały ustalone również minima czasowe w jakich mogłyby się odbywać oceny poszczególnych dostawców co niesie za sobą ryzyko dodatkowego zaskakiwania przedsiębiorców i brakiem możliwości faktycznej reakcji w sytuacji gdy budżet na zapewnienie dostępu do określonego sprzętu został wyczerpany, a dany dostawca z dnia na dzień został uznany za niebezpiecznego. Brak jest również odniesienia, w jakich systemach dane rozwiązanie jest niebezpieczne, co powoduje	do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73

			konieczność wymiany całości sprzętu lub oprogramowania bez względu na to czy w danym podmiocie faktycznie mogą one prowadzić do naruszenia zasad bezpieczeństwa. Mając na uwadze przedstawioną argumentację należy stwierdzić, iż obiektywny i oparty o przejrzystą metodologie proces oceny ryzyka cybernetycznego dostępnych technologii lub produktów miałby dużo większą korzystną wartość dla poziomu bezpieczeństwa i kondycji gospodarczej podmiotów niż nakazowo/zakazowy mechanizm dyskwalifikowania określonych producentów. Kolejnym argumentem przemawiającym za odstąpieniem od proponowanych rozwiązań jest fakt, iż większość producentów sprzętu elektronicznego korzysta z poddostawców usytuowanych w państwach azjatyckich, które z automatu spełniają przynajmniej jedno kryterium uznania ich za niebezpieczne (ochrona danych osobowych, ale również prawa człowieka). W tej sytuacji bardzo groźnym może być sytuacja, w której przy braku możliwości zakupu sprzętu uznawanego za bezpieczny, podmioty gospodarcze nie będą w stanie sprostać wymaganiom stawianym przez Organy administracji publicznej i tym samym mogą stać przed dylematem: kończyć swoją działalność czy ryzykować nałożenie absurdalnie wysokich kar. Projekt ustawy nie odpowiada na pytanie co w takiej sytuacji powinien dany podmiot uczynić. Przedstawiając powyższe uwagi obawiamy się sytuacji, w której wskazanie któregoś z wiodących producentów urządzeń elektronicznych, sparaliżuje dostęp do produktów tego producenta a też pośrednio do innych bazujących na jego podzespołach. Może mieć to szczególny znaczenie dla przemysłu farmaceutycznego, gdzie wyśrubowane wymagania ze strony poszczególnych organów, w tym w szczególności na etapie	zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest

			wytwarzania leków – przez Głównego Inspektora Farmaceutycznego, dodatkowo zawężają już dość wąską niszę producentów automatyki i elektroniki przemysłowej, których urządzenia i podzespoły mogłyby stanowić bazę np. dla linii produkcyjnych. Finalnie może skończyć się to zablokowaniem możliwości technicznych produkowania leków, zachwiania dostępności do tanich i sprawdzonych leków dostępnych na rynku od lat, a w konsekwencji do paraliżu polityki lekowej państwa i gwałtownym wzroście wydatków płatnika publicznego na droższe leki pochodzące z importu. Mając na uwadze powyższe okoliczności uzasadnionym wydaje się odstąpienie od dalszego procedowania przedmiotowego projektu ustawy.	np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zespole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
66.	Excogitate	Uwaga ogólna	Ustawa w oczywisty sposób narusza zasady niedyskryminacji i uczciwej konkurencji przedsiębiorstw oraz podważa wielostronne oraz dwustronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami. Projekt ustawy oznacza, że rynek biznesowy będzie podlegał wpływom politycznym, co nie sprzyja wolnej konkurencji. Będzie to miało istotny negatywny wpływ na otoczenie biznesowe i całą branżę ICT w Polsce. Przedstawiamy następujące szczegółowe uwagi:	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji

			1. **Nadmierna ochrona handlu tworzy bariery handlowe i tarcia.** Jednostronny protekcjonizm handlowy wpłynie negatywnie na rozwój gospodarczy Polski. WTO stopniowo ustanowiła międzynarodowy porządek, którego rdzeniem jest ONZ, oraz wielostronny system handlowy, którego rdzeniem jest WTO. Naruszenie zasad międzynarodowego systemu handlowego, budowanego przez dziesięciolecia, utrudniłoby utrzymanie ładu handlowego i mogłoby wywołać tarcia handlowe między Polską, a innymi krajami. 2. **KSC może skutkować brakiem uczciwej konkurencji.** Protekcjonizm zagroziłby konkurencyjności polskiej gospodarki cyfrowej. W perspektywie krótkoterminowej, stosowanie protekcjonizmu w celu ograniczenia sprzedaży produktów z innych krajów wydaje się pomagać niekonkurencyjnym branżom i przedsiębiorstwom. W przypadku polskiej branży ICT pozbawi to branżę ICT i przedsiębiorstwa motywacji do większych inwestycji i ulepszania technologii, prowadząc do spadku konkurencyjności produktów. Z drugiej strony branża i przedsiębiorstwa w innych krajach podejmą więcej kroków w celu poprawy konkurencyjności. W rezultacie międzynarodowa konkurencyjność polskiej branży ICT i przedsiębiorstw będzie ulegać dalszemu osłabieniu. 3. **Wbrew podstawowej zasadzie wolnego handlu w gospodarce rynkowej, protekcjonizm niszczy ekosystem branży i zwiększa koszty dostaw.**	lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.

			Wolność i wzajemność są podstawą i warunkiem wstępnym handlu międzynarodowego. Poparcie dla wolnego handlu i sprzeciw wobec protekcjonizmu to podstawowe wartości i podstawowe zasady WTO. Żaden kraj nie jest w stanie w pełni posiadać wszystkich zasobów, technologii i zdolności wymaganych do nowej ery globalnej modernizacji technologicznej i przemysłowej. Ochrona handlu może jedynie osłabić globalny system wolnego handlu i utrudnić odbudowę światowej gospodarki w czasie po epidemii. **4. Potencjalny wpływ na dwustronne oraz wielostronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami.** Projekt zmiany ustawy KSC podważy wielostronne umowy handlowe podpisane przez Polskę z innymi krajami, np. Porozumienie WTO/GATT. Projekt zmiany ustawy KSC narusza zasadę równych i wzajemnych korzyści oraz klauzulę największego uprzywilejowania (KNU) w WTO, a także zasadę równej ochrony i traktowania KNU obiecaną w dwustronnych umowach handlowych i inwestycyjnych między Polską, a innymi krajami.	
67.	Excogitate	Uwaga ogólna	Jako podmiot odpowiedzialności społecznej, mamy za zadanie aktywnie rozpowszechniać racjonalne rozwiązania. Mając na uwadze utrzymanie dobrego kontaktu środowiska biznesowego z rządem wnosimy o rozważenie następujących uwag do projektu zmiany ustawy KSC: 1. Ministerstwo Cyfryzacji powinno zorganizować otwartą debatę i zaprosić odpowiednie ministerstwa, izby	**Wyjaśnienie** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W

			gospodarcze, operatorów i inne zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w projekcie. 2. Rząd powinien w pełni ocenić wpływ projektu, w tym koszty i straty, na konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. 3. Zasadniczo, zablokowanie niektórych dostawców nie może rozwiązać problemów związanych z bezpieczeństwem cybernetycznym. Wnosimy o przyjęcie spójnej strategii w ramach UE, w celu zarządzania za pomocą jasnych specyfikacji technicznych i zharmonizowanych norm, zamiast wykluczania dostawców z określonych krajów. Postulujemy odwołanie się do modelu niemieckiego i równe traktowanie wszystkich dostawców, nie tylko z powodów nietechnicznych. Z punktu widzenia racjonalności ekonomicznej, rząd musi promować dwustronny wolny handel i zmniejszać bariery w swobodnym przepływie towarów i usług. Rząd powinien ogłosić przepisy ustawowe i wykonawcze oraz środki, które sformułował i wdrożył, a także ich zmiany, jak również powinien informować o nich Światową Organizację Handlu.	ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Ministerstwo Cyfryzacji a obecnie KPRM umożliwiło zajęcie stanowiska do projektu ustawy w ramach konsultacji publicznych.
68.	Excogitate	Uwaga ogólna	Ustanowienie wspólnego unijnego mechanizmu certyfikacji krytycznego sprzętu i oprogramowania. Wymaganie od dostawców oświadczenia o wiarygodności. Ustalenie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu teleinformatycznego. Nawiązanie do modelu niemieckiego. **Uzasadnienie:**	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z

			1) Ustalenie obiektywnych i jasnych kryteriów, upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. 2) Skuteczniejszym będzie zmotywowanie dostawców do samokontroli i złożenia oświadczenia o wiarygodności. 3) Nietechnologiczne kryteria są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.	urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne

				związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
69.	Fundacja Bezpieczna	Uwaga ogólna	Fundacja Bezpieczna Cyberprzestrzeń od początku przygląda się pracą nad nowelizacją ustawy. Z uwagą analizowaliśmy wszystkie doniesienia na temat możliwych zmian. Jako Fundacja stoimy na stanowisku, że nowelizacja przepisów ustawy jest potrzebna i	**Wyjaśnienie** Dziękujemy za uwagi.

	Cyberprzestrzeń		oczekiwana przez podmioty krajowego systemu cyberbezpieczeństwa. Uważamy jednak, że nie wszystkie proponowane przepisy i rozwiązania zostały należycie ujęte w w/w projekcie, dlatego pozwoliliśmy sobie przedstawić nasze uwagi do zaproponowanego projektu.	
70.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Konieczne jest dodanie vacatio legis dla przepisów art. 14 – co najmniej 6 miesięcy.	**Uwaga nieuwzględniona** Zmiana przepisu jest podyktowana zmianą podejścia na *risk based approach*. Jest to zmniejszenie obciążeń regulacyjnych w stosunku do aktualnie obowiązującego tekstu ustawy.
71.	Fundacja Bezpieczna Cyberprzestrzeń	Uwaga ogólna	Ustawa powinna zapewniać środki budżetowe na realizacje proponowanych zmian, a nie tylko możliwość ubiegania się o nie.	**Uwaga nieuwzględniona** Środki budżetowe zapewnia ustawa budżetowa.
72.	KIGEIT	Uwaga ogólna	Zgodnie z dyrektywą 2016/1148 (art. 1 ust. 3), wymogi dotyczące bezpieczeństwa i zgłaszania incydentów nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Podlegają one bowiem wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014. Jednocześnie dyrektywa 2002/21/WE została zastąpiona przez Europejski Kodeks Łączności Elektronicznej („EKŁE"), który zawiera odpowiednie regulacje sektorowe dotyczące integralności i bezpieczeństwa sieci i usług komunikacji elektronicznej (implementowane w projekcie PKE). W związku z powyższym uważamy, iż możliwe jest przy uwzględnieniu skonsultowanych postanowień PKE oraz	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów

			przyjętego rozporządzenia z dnia 22 czerwca 2020 r. z art. 175d p.t., zaproponować, aby wraz z wejściem w życie PKE przyjąć rozporządzenie z art. 39 ust. 4 PKE, które modyfikowałoby obecne rozporządzenie z art. 175d p.t. i wprowadzało model ochrony infrastruktury powiązany z nadzorem Prezesa UKE w porozumieniu z CRSIT Telko, a także certyfikacją składników infrastruktury, które uznane zostałyby za krytyczne.	usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
73.	KIGEIT	Uwaga ogólna	**Zasada dwuinstancyjności postępowania i prawo do sądu** Izba jest zaniepokojona przewidzianym w projekcie przyznaniem Pełnomocnikowi oraz Kolegium kompetencji do wydawania rozstrzygnięć w sprawach indywidualnych bez zachowania należytych procedur przewidzianych w prawie administracyjnym oraz z pominięciem podstawowych uprawnień stron oraz gwarancji ochrony ich interesów, na czele z naruszeniem konstytucyjnej zasady dwuinstancyjności postępowania administracyjnego (art. 78 Konstytucji RP) oraz prawa do jawnego rozpatrzenia sprawy przez właściwy, niezależny, bezstronny i niezawisły sąd (art. 45 Konstytucji RP). Choć w ustawie zostało wprost określone, że Kolegium jest organem jedynie opiniodawczo-doradczym (art. 64 KSC), a Pełnomocnik – podmiotem koordynującym działania i realizującym politykę rządu (art. 60 KSC), jednak w Projekcie przyznane im zostały kompetencje do wydawania decyzji administracyjnych. W przypadku polecenia zabezpieczającego zostało to wyraźnie wskazane (projektowany art. 67c ust. 1), natomiast w przypadku ostrzeżenia i oceny ryzyka wynika z *meritum* projektowanych przepisów. Nie powinno więc ulegać wątpliwości, że wydawanie przez Pełnomocnika i Kolegium	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za

			decyzji administracyjnych będzie następować w drodze ogólnego postępowania administracyjnego (w trybie przepisów Kodeksu postępowania administracyjnego) oraz że powinny od nich przysługiwać środki odwoławcze – zarówno w ramach kontroli instancyjnej, jak i na drodze sądowej. Uważniej powinny również zostać uregulowane kwestie proceduralne, jeśli wymagają szczególnej regulacji. Nie powinny być wprowadzane mechanizmy, które nie tyle przewidują dopuszczalne zmiany proceduralne wobec regulacji KPA, co pozostają w sprzeczności z przewidzianymi założeniami systemowymi, jak np. zatwierdzanie przez dany organ decyzji wydawanej przez inny podmiot. Luki i wady procedur przewidzianych w Projekcie są tak znaczące, że w praktyce unicestwiają cele, jakim ma służyć ustawa. Zachowanie projektowanych przepisów w obecnym brzmieniu spowoduje bowiem, że wadliwe decyzje nie będą mogły w państwie prawa stanowić podstawy do nałożenia kar, o których mowa w projektowanych art. 73 ust. 1 pkt 14 i ust. 2, a jedynie do odpowiedzialności Skarbu Państwa za szkodę wyrządzoną ich wydaniem. Trudno w tym przypadku oczekiwać efektywności projektowanych środków.	wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę

				wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
74.	KIGEIT	Uwaga ogólna	**Naruszenie przepisów WTO** a) Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę o najbardziej uprzywilejowanej pozycji. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne. b) Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania "podobnych" produktów zagranicznych i krajowych, usług i usługodawców w równym stopniu. W przypadku stosowania krajowego obowiązku podejścia, produkty zagraniczne, usługi lub zagraniczni usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobny” produkt krajowy, usługodawca lub usługodawca krajowy (art. III GATT).	**Uwaga nieuwzględniona** Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.

			c) Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie.	
75.	KIGEIT	Uwaga ogólna	**Zobowiązania dwustronne w ramach umów międzynarodowych** Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku podmiotów reprezentujących kapitał zagraniczny narusza zobowiązania podmiotów na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może to zostać uznane za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy Traktatu o Dwustronnej Inwestycji.	**Uwaga nieuwzględniona** Projekt jest zgodny z dwustronnymi umowami międzynarodowymi, w których stroną jest Polska.
76.	KIGEIT	Uwaga ogólna	**Uwagi techniczne dotyczące ryzyka i rozwiązań bezpieczeństwa** **1. Kryteria powinny być neutralne technologicznie, a nie uwzględniać względy polityczne:** 1) Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne (takie jak sieć bazowa), zaś charakterystyka dostawcy powinna zostać poddana ocenie pod kątem bezpieczeństwa procesu produkcji i zapewnienia dostaw. 2) Kryteria powinny mieć charakter techniczny, być obiektywne, rozsądne i proporcjonalne oraz zawierać odniesienie do oceny ryzyka zawartej w Toolbox 5G i specyfikacjach technicznych. 3) Projekt ustawy musi być zgodny zarówno z wymogami prawnymi dotyczącymi dobrych praktyk legislacyjnych,	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji

			jak i z obowiązującymi przepisami, takimi jak prawo Unii Europejskiej, międzynarodowe prawo inwestycyjne, prawami człowieka i Konstytucją RP. **2. Normy techniczne i normy certyfikacji** 1) Projekt ustawy powinien raczej koncentrować się na normach technicznych i normach certyfikacji, które powinny zostać wprowadzone, takich jak NESAS, system certyfikacji ENISA. 2) **NESAS:** Określany wspólnie przez 3GPP i GSMA. Jest to dobrowolny program stosowany przez sektor telefonii komórkowej, zapewniający podstawowy i kompleksowy audyt bezpieczeństwa dowodzi, że sprzęt sieciowy spełnia wymogi bezpieczeństwa, a sprzedawcy sprzętu sieciowego – standardy bezpieczeństwa w procesie rozwoju produktów i cyklu życia. GSMA posiada radę akredytacyjną, która jest odpowiedzialna za monitorowanie i opracowywanie planów oraz udzielanie akredytacji. 3) **ENISA**: Unijne ramy certyfikacji bezpieczeństwa cybernetycznego: wspólne ramy dla obowiązujących w całej UE systemów certyfikatów bezpieczeństwa cybernetycznego. Unijne ramy certyfikacji bezpieczeństwa cybernetycznego mają na celu przyjęcie wspólnego podejścia i ustanowienie europejskich ram certyfikacji bezpieczeństwa cybernetycznego, które określają główne wymogi dla europejskich systemów bezpieczeństwa cybernetycznego i europejskich certyfikatów zgodności produktów ICT, usługi ICT lub procesy ICT, które mają być uznane i stosowane we wszystkich państwach członkowskich.	będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności

			3. Stymulacja budowy krajowego potencjału technologicznego w zakresie cyberbezpieczeństwa Projektowane zmiany w ustawie kreują ciała decyzyjne i podmioty opiniotwórcze, których obszar kompetencji ogranicza się wyłącznie do incydentów w obszarze programowania i usług. Pominięto potrzebę prawnego usankcjonowania obowiązku prowadzenia działań zmierzających do zabezpieczenia interesu państwa polskiego na poziomie **rozwiązań sprzętowych.** Kwestia zapewnienia bezpieczeństwa sprzętowego od lat jest podnoszona na poziomie zarówno krajowym jak i europejskim. Na poziomie międzynarodowym działają różne organizacje skupione wokół zagadnienia cyberbezpieczeństwa. Na poziomie europejskim jest to m.in. European Union Agency for Cybersecurity (ENISA), której członkiem jest również Polska. Publicznie dostępne informacje dotyczące polskiej strategii cyberbezpieczeństwa obejmują wyłącznie organizacyjne i softwareowo-systemowe aspekty (cyber)bezpieczeństwa, deklaracje powoływania ciał, gremiów i zespołów analizujących incydenty bezpieczeństwa realizowane, zabezpieczane i neutralizowane na poziomie usług, z podziałem na incydenty: • wpływające na działalność operatorów usług kluczowych (incydenty poważne), • dostawców usług Cyfrowych (incydenty istotne), • incydenty w podmiotach publicznych. Incydenty te zgodnie z zapisami ustawy są raportowane do jednego z krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), zaś zgodnie z zapisami	gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			projektu zmian w ustawie przebudowany ma zostać model współpracy w ramach krajowego systemu cyberbezpieczeństwa	
77.	KIGEIT	Uwaga ogólna	**ZASTRZEŻENIA DO USTAWY** 1. Jedyne miejsce, w którym ustawodawca zbliża się do zagadnień **na poziomie sprzętu** związanych z (cyber)bezpieczeństwem urządzeń przewidzianych do użytku jest ograniczone do warunkowej wzmianki (cyt.): „*Dostawcy **sprzętu** lub oprogramowania będą mogli zostać poddani **procedurze sprawdzającej***”. a. Nie jest w żaden sposób określony merytoryczny zakres wspomnianej wyżej **procedury sprawdzającej**. b. Z załączonych w projekcie zmian szacunków pracochłonności wynika, że pod uwagę brana jest niezwłoczna akceptacja gotowych rozwiązań przewidzianych do kwalifikacji i dopuszczenia, poprzedzona jedynie pobieżną analizą stanu faktycznego prowadzącą do ewentualnego wykrycia problemów z oprogramowaniem. c. Dotyczy to również rozwiązań przewidzianych dla infrastruktury krytycznej (brak ustawowego rozróżnienia) dla bezpieczeństwa państwa. Dla uzmysłowienia poziomu złożoności zagadnienia wystarczy wziąć pod uwagę, że współczesne rozwiązania układowe (sprzętowe zaszyte w układach scalonych) zawierają nierzadko wiele miliardów elementów składowych ukrytych w monolitycznych strukturach krzemowych, których weryfikacja o ile w ogóle technicznie możliwa – wymaga wielomiesięcznej pracy całych zespołów fachowców a także dostępu do	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania

			technologii i projektów, które w Polsce w chwili obecnej nie występują. Lektura skojarzonych z ustawą dokumentów jak „Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022”, a także planowane działania z zakresu cyberbezpieczeństwa w latach 2021-2027 w ramach programu operacyjnego Polska Cyfrowa 2.0, choć adresują wzmiankowaną w nich **potrzebę zwiększenia polskiego potencjału R&D w obszarze cyberbezpieczeństwa** to wciąż brak jest jakichkolwiek konkretnych zapisów zmierzających do kreowania takowego potencjału w kraju zarówno w obszarze dostępnej w kraju infrastruktury technologicznej jak i sprzętu polskiego pochodzenia.	poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący

				w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
78.	KIGEIT	Uwaga ogólna	**SUGESTIE / REKOMENDACJE** 1. Rzeczywisty poziom cyberbezpieczeństwa z **uwzględnieniem sprzętowych aspektów cyberbezpieczeństwa** powinien być kluczowym czynnikiem decyzyjnym warunkującym konkretny zakup/inwestycję/prace R&D. 2. Obowiązek oceny poziomu cyberbezpieczeństwa (dalej ***CyberSecEval***) na poziomie sprzętowym **powinien być ustawowo zapisanym elementem decyzyjnym** towarzyszącym działaniom wpływającym na poziom cyberbezpieczeństwa w Polsce. 3. Niezbędne jest ustawowe **określenie grupy urządzeń**, usług, procesów itd. (***Obszar Zastosowania***) poddawanych **CyberSecEval** „obowiązkowo / opcjonalnie / nie poddawanych" badaniu i / lub ocenie, z uwzględnieniem poziomu szczegółowości prowadzonych działań badawczych i / lub ocennych. Należy ustawowo **określić warunki definiujące zakres (kwalifikacja poziomu) i sposób przeprowadzenia działań badawczych/ocennych CyberSecEval** w odniesieniu do zastosowanych rozwiązań sprzętowych. 4. Obowiązek prowadzenia kompleksowych działań badawczych **CyberSecEval** zakończonych raportem dotyczącym poziomu ryzyka / bezpieczeństwa, powinien być poprzedzony kwalifikacją poziomu	**Wyjaśnienie** **Podmioty krajowego systemu cyberbezpieczeństwa (przede wszystkim operatorzy usług kluczowych) muszą prowadzić systematyczną analizę ryzyka.** **Nie można zmienić definicji incydentu, ponieważ wynika ona z Dyrektywy NIS.**

			analizy, zależną od prawdopodobieństwa wystąpienia w układzie tzw. hardware trojans oraz potencjalnej szkodliwości ich aktywności w danym zastosowaniu układu. Stąd, najbardziej rygorystyczne i szczegółowe analizy powinny dotyczyć zastosowań krytycznych dla bezpieczeństwa państwa urządzeń. W szczególności badaniu / ocenie danego rozwiązania powinny podlegać krytyczne dla bezpieczeństwa rozwiązania komponenty, w szczególności ich struktura i zastosowane rozwiązania. Hardware Trojans - czyli intencjonalne modyfikacje sprzętowe wprowadzane na etapie projektu lub produkcji podzespołów (mikroprocesory, pamięci, elementy wykonawcze) fragmentów, modułów lub całych rozwiązań umożliwiają przejęcie kontroli nad sprzętem i pozostają fizycznie niewykrywalne większości behawioralnych analiz bezpieczeństwa. Umożliwiają kontekstowe otwarcie dostępu do systemu prowadzące do kompromitacji zabezpieczeń lub pozyskania kluczy kryptograficznych przez jednostki do tego nieupoważnione. 5. Krytycznym zagadnieniem prawnym jest **stworzenie wymogu formalnego** wobec podmiotów krajowych stymulującego do wyjścia poza obecnie dominujący (o ile nie jedynie obowiązujący) model businessowy krajowych podmiotów w branży bazujący na zastosowaniu gotowych komponentów nieznanego pochodzenia w tzw. „polskich produktach” – w tym w produktach warunkujących bezpieczeństwo na poziomie jednostki i społeczeństwa. Z nielicznymi wyjątkami, gdy w zaawansowanych technologiach	

			mikroelektronicznych w kraju wytwarzane są pojedyncze komponenty urządzeń (jak np. specjalizowane detektory promieniowania), opracowanie gotowych urządzeń rynkowych zasadza się na imporcie kluczowych, o ile nie wszystkich (poza PCB i obudową) komponentów systemu od producentów europejskich lub z dowolnego miejsca na świecie (dominuje daleki wschód). 6. Definicja „**incydentu**" powinna zostać rozszerzona o **możliwość** wykorzystania gotowych urządzeń lub podzespołów zawierających świadomie wcześniej zaimplementowane, lecz niewykryte luki w zabezpieczeniach lub nigdy nieujawnione funkcjonalności. Sama możliwość zastosowania urządzeń z ukrytą opcją ukrytego podsłuchu, podglądu w krytycznych urzędach lub miejscach, urządzeń z ukrytą funkcją zdalnej dezaktywacji lub uruchomienia dodatkowych funkcjonalności zakłócających działanie innych urządzeń lub maskowanej transmisji kluczy kryptograficznych (i bardzo wiele innych scenariuszy) samo w sobie **stanowi Incydent** (bezpieczeństwa) **obecnie nieuwzględniony** przez Ustawodawcę. 7. Powinien zostać utworzony dodatkowy CSIRT skupiony wokół analiz: • prawdopodobieństwa wystąpienia intencjonalnych modyfikacji sprzętowych (Hardware Trojans) wprowadzanych do układów i podzespołów na etapie projektu lub ich produkcji, • szkodliwości aktywacji i działania Hardware Trojans zależnie od konkretnych zastosowania konkretnego podzespołu,	

			• poziomu istotności zagrożenia oraz jego kwalifikacji CyberSecEval na poziomie sprzętu - (gadżety / AGD / mobilność / komunikacja / dane / zdrowie / infrastruktura krytyczna / zastosowania militarne. 8. Prawne usankcjonowanie: a. wymogu pozyskiwania krajowych podzespołów, które w obecnej chwili nie istnieją i nie są produkowane w kraju z uwagi na zniszczenie krajowego przemysłu mikroelektronicznego w okresie transformacji ustrojowej. b. uruchomienia procesu rewitalizacji krajowego przemysłu mikroelektronicznego zmierzającej do zbudowania w Polsce zaplecza technologicznego posiadającego potencjał produkcyjny krajowych podzespołów mikroelektronicznych (układy scalone), które w obecnej chwili nie istnieją i nie są produkowane w kraju (nieliczne przypadki krajowej myśli technicznej są produkowane na liniach technologicznych poza granicami Polski).	
79.	KIGEIT	Uwaga ogólna	**OCZEKIWANE DZIAŁANIA** Niezależnie od okoliczności, iż czas na odniesienie się do materii projektu mimo wydłużenia go o kolejne 14 dni, jest zbyt krótki i praktycznie uniemożliwia przeprowadzenie analiz potencjalnego wpływu przedmiotowego aktu na funkcjonowanie całej branży elektronicznej, zdecydowaliśmy się przedłożyć powyższe wstępne uwagi oraz propozycje zmian. Jednocześnie zwracamy się z prośbą o przeprowadzenie następujących działań: **1. POSTULAT ZORGANIZOWANIA KONFERENCJI UZGODNIENIOWEJ ORAZ WCZEŚNIEJSZEGO WYSŁUCHANIA PUBLICZNEGO**	**Wyjaśnienie** Umożliwiono wypowiedzenie się interesariuszy poprzez konsultacje publiczne. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy. **2. POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH, GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI** W zakresie skutków społecznych należy opisać wpływ na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce. **3. PROPONOWANY KIERUNEK ZMIAN** Rynek usług łączności elektronicznej powinien nadal pozostać kompleksowo regulowany sektorowo, ze względu na jego szczególne cechy. Dlatego uważamy, że docelowym miejscem uregulowania kwestii obowiązków operatorów telekomunikacyjnych w zakresie bezpieczeństwa sieci i usług jest projektowana ustawa Prawo Komunikacji Elektronicznej. Należy więc pozostawić kompetencje Prezesa UKE uregulowane w art. 39-49 projektu PKE. Model przedstawiony w PKE zapewnia bowiem szereg narzędzi pozwalających zapewnić cyberbezpieczeństwo infrastruktury telekomunikacyjnej.	Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			Jednocześnie zgodnie z prośbą otrzymaną w toku konsultacji wewnątrzizbowych, od trzech członków Izby, firmy EXATEL S.A., NASK-PIB, oraz Nokia Solutions and Networks Sp. z o.o., informuję o wyłączeniu poparcia tych firm dla treści powyższego stanowiska	
80.	Pracodawcy RP	Uwaga ogólna	Opiniowana ustawa procedowana jest równocześnie z projektem ustawy - Prawo komunikacji elektronicznej. Te dwa zasadnicze projekty aktów prawnych stworzą nowe otoczenie prawno-regulacyjne w sektorze telekomunikacyjnym na najbliższe lata. Do obu tych projektów Pracodawcy RP mają zasadnicze uwagi i zastrzeżenia, o czym w przypadku nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa będzie w dalszej części niniejszego stanowiska. Zanim przejdziemy do uwag należy jednak poświęcić miejsce fatalnej sytuacji, jaką jest rekonstrukcja rządu i związana z tym procesem likwidacja Ministerstwa Cyfryzacji - autora i gospodarza zarówno Prawa komunikacji elektronicznej, jak też nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. W naszej ocenie niedopuszczalne jest, aby podstawy nowego ładu prawnego w kluczowym dla funkcjonowania państwa sektorze, jakim jest telekomunikacja, powstawały w sytuacji, w której odpowiedzialne za to departamenty i urzędnicy mają na głowie zmianę podległości służbowej, być może przeprowadzkę, zmianę szyldu, pieczątek czy stopek w e-mailach. Przechodząc do oceny projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, należy stwierdzić, iż wywołuje on liczne i poważne wątpliwości. Począwszy od kwestii zgodności z Konstytucją RP, przez zgodność z prawem międzynarodowym, po zgodność z prawem unijnym. Zarzuty w tych obszarach przedstawiamy poniżej. W dalszej części stanowiska zwracamy też uwagę na zagrożenie dla konkurencji, możliwy wzrost kosztów i pogorszenie jakości świadczonych	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			usług, a także naruszenie zasady zaufania do państwa oraz swobody działalności gospodarczej. Podkreślenia wymaga fakt, iż projektowane przepisy wprowadzają nową procedurę decyzyjną, która w sposób całkowicie uznaniowy - i ostateczny - rozstrzygnie o możliwości korzystania ze sprzętu określonego dostawcy. Procedura ta nie ma nic wspólnego z zasadą demokratycznego państwa prawnego, zasadą transparentności i zaufania państwa do przedsiębiorcy. Poniżej prezentujemy szczegółowe uwagi oraz propozycje poprawek do opiniowanego projektu ustawy. Liczymy na to, że projektodawca pochyli się nad naszym stanowiskiem. Cyfryzacja pozwoliła nam kontynuować pracę i naukę w okresie pandemii, zapewniła dostęp do ochrony zdrowia, dóbr kultury i rozrywki. Dzięki cyfryzacji urzędy oraz instytucje publiczne mogły funkcjonować, załatwiać sprawy zgłaszane przez obywateli i przedsiębiorców. Cyfryzacja to, w naszej ocenie, jeden z podstawowych priorytetów Rządu RP na najbliższe lata. Aby procesy cyfryzacyjne mogły być kontynuowane, potrzebne są stabilne, przejrzyste i przyjazne dla rozwoju sektora teleinformatycznego przepisy. Jesteśmy gotowi takie przepisy współtworzyć, wspierać decydentów poprzez wskazywanie słabych punktów istniejących oraz projektowanych regulacji, a także wskazywać - w ramach dialogu społecznego - potencjalne najlepsze rozwiązania. Opiniowany projekt jest przykładem regulacji, które tego dialogu bardzo potrzebują.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
81.	Narodowy Bank Polski	Uwaga ogólna	Na wstępie uprzejmie informujemy, iż co do zasady Narodowy Bank Polski przyjmuje z aprobatą propozycje zmian w projekcie ustawy, w szczególności dotyczące utworzenia podmiotów mających zapewnić dostęp oraz wymianę wiedzy eksperckiej dotyczącej cyberzagrożeń. Niemniej jednak zwracamy	**Uwaga nieuwzględniona** Proponowane przepisy nie wpływają na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczą jego zadań konstytucyjnych i ustawowych.

			uwagę, że w projekcie ustawy pomimo braku bezpośrednich odwołań do Narodowego Banku Polskiego, propozycje niektórych przepisów mogą wydawać się niezgodne z rolą przypisaną NBP w przepisach Konstytucji RP i ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim w zakresie wartości fundamentalnych z punktu widzenia podstaw funkcjonowania banku centralnego w Polsce, w szczególności jego niezależności. Powyższe odnosi się do propozycji przepisów wedle których projektodawca nadał Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa kompetencje do wydawania, na podstawie projektowanego art. 67a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą o KSC", ostrzeżeń i poleceń zabezpieczających w odniesieniu do podmiotów, o których mowa w art. 4 pkt 1–16 ustawy o KSC. Narodowy Bank Polski, jako jeden z podmiotów tworzących krajowy system cyberbezpieczeństwa (vide art. 4 pkt 9 ustawy o KSC) może być zatem adresatem tego rodzaju działań Pełnomocnika.	
82.	Narodowy Bank Polski	Uwaga ogólna	Narodowy Bank Polski jest operatorem systemów płatności o kluczowym znaczeniu dla stabilności całego systemu finansowego w Polsce (tj. SORBNET2 i TARGET2-NBP). Potencjalne zakłócenie funkcjonowania tych systemów może nieść za sobą skutki w postaci zaburzeń transmisji pieniądza w skali całego kraju. Dlatego też, w ocenie NBP, powierzanie Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa kompetencji umożliwiających ingerowanie w systemy IT będące komponentem infrastruktury płatniczej, której operatorem jest bank centralny, nie znajduje uzasadnienia. Warto w tym miejscu podkreślić, iż w przypadku, w którym projektowane przepisy wykraczają poza wdrożenie właściwej dyrektywy, wymagają zasięgnięcia opinii Europejskiego Banku	**Wyjaśnienie** Proponowane przepisy nie wpływają na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczą jego zadań konstytucyjnych i ustawowych.

			Centralnego (EBC). W przypadku opiniowanego projektu ustawy, właściwość EBC do wydania opinii wynika z art. 127 ust. 4 oraz art. 282 ust. 5 Traktatu o funkcjonowaniu Unii Europejskiej, jak również z art. 2 ust. 1 tiret trzecie, piąte i szóste decyzji 98/415/WE gdyż projekt ustawy zawiera postanowienia odnoszące się do zadań NBP, tj. banku centralnego współtworzącego Europejski System Banków Centralnych. Zwracamy uwagę, że ewentualne niezastosowanie się polskich władz publicznych do obowiązku zasięgnięcia opinii EBC w trakcie niniejszego procesu legislacyjnego może przyczynić się do stwierdzenia naruszenia przez władze krajowe przepisów wspólnotowych, określających obowiązek konsultacji poszczególnych projektów aktów prawnych z organami wspólnotowymi. Konkludując powyższe, w związku z koniecznością zagwarantowania niezależności przy realizowaniu przez bank centralny zadań wynikających zarówno z polskiego porządku prawnego jak i ze zobowiązań międzynarodowych, proponujemy wprowadzenie do opiniowanego projektu ustawy następujących zmian.	
83.	Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-	Uwaga ogólna	Należy zwrócić uwagę, że kryteria na podstawie, których przeprowadzana jest ocena ryzyka dostawcy sprzętu lub oprogramowania są nieprecyzyjne – tym samym pozostawiają dużo swobody do oceny Kolegium. W związku z powyższym rekomendowane jest sprecyzowanie kryteriów – opracowanie skali, na podstawie, której jest przeprowadzana analiza ryzyka dostawcy sprzętu lub oprogramowania. Wskazać należy, że w przypadku określenia ryzyka, jako umiarkowane lub niskie od dokonanej oceny, nie przysługują dostawcy sprzętu lub oprogramowania żadne środki odwoławcze. Biorąc pod uwagę skutki gospodarcze, ekonomiczne, które	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra

	Techniczn ych		poniesienie dostawca sprzętu lub oprogramowania zasadne jest, aby w ustawie wprowadzić zapis przyznający prawo dostawcy do wniesienia odwołania również w przypadku, gdy Kolegium oceni ryzyko jako umiarkowane lub niskie. Zaznaczyć należy, że w przypadku określenia ryzyka jako umiarkowanego, to podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzić do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz mogą jedynie kontynuować używanie dotychczas posiadanego sprzętu, usług lub oprogramowania, wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania. W odniesieniu do dostawcy sprzętu lub oprogramowania w stosunku do którego określono ryzyko jako wysokie, rekomendowane jest, aby termin na wniesienie odwołania wydłużyć do co najmniej 3 miesięcy, 14 -dniowy termin na wniesienie odwołania jest zbyt krótki, biorąc pod uwagę, że wniesienie odwołania oraz jego pełne uzasadnienie może wymagać sporządzenia specjalistycznych opinii, ekspertyz. Podkreślenia wymaga, że Kolegium ma 2 miesiące od otrzymania odwołania na jego rozpatrzenie. W związku z powyższym wskazane jest aby sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania była ogłaszana przez Pełnomocnika w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” dopiero po rozpatrzeniu odwołania, jak również by dopiero po rozpatrzeniu odwołania stosowane były środki wskazane w art. 66b i art. 66c. Ponadto, rekomendowane jest również przyznanie	właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa

			dostawcom sprzętu i oprogramowania prawa do złożenia wniosku o zmianę oceny dokonanej przez Kolegium w przypadku wystąpienia nowych okoliczności – w projektowanym przepisie prawo to zostało przyznane wyłącznie członkowi Kolegium. Wskazać również należy, że skutki publikacji komunikatu przez Pełnomocnika z perspektywy dostawcy oprogramowania lub sprzętu sprowadzają się do zakazu prowadzenia działalności gospodarczej, jak również zawieszenia planowanych projektów, wycofania poczynionych przez dostawcę inwestycji. Z perspektywy podmiotów krajowego systemu cyberbezpieczeństwa, w operatorów usług kluczowych np. Szpitali wycofywanie sprzętu, oprogramowania i usług oraz brak możliwości zakupu sprzętu, oprogramowania i usług danego dostawcy powodować może ogromnie koszty, ponadto może to również naruszać zasady konkurencji.	spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
84.	Fundacja Bezpieczna	Uwaga ogólna do Rozdziału 4	Zakres proponowanego rozdziału 4a w znacznej mierze pokrywa się z treścią, która występuje w rozdziale 5 nowego Prawa Komunikacji Elektronicznej. Nie jest to zgodne z zasadami techniki prawodawczej (rozporządzenie Prezesa Rady Ministrów	Wyjaśnienie Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa

	Cyberprzestrzeń		w sprawie „Zasad techniki prawodawczej” §4 ust. 1 - Ustawa nie może powtarzać przepisów zamieszczonych w innych ustawach.).	sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
85.	Polski Związek Pracodawców	Uwaga ogólna	Przedmiotowy projekt ustawy wprowadza istotne zmiany w trzech strategicznych, z punktu widzenia podmiotu prowadzącego działalność gospodarczą, obszarach: **1. w zakresie obowiązków operatora usługi kluczowej**	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur

	Przemysłu Farmaceutycznego		- obecne rozwiązanie opierające się na wewnętrznych lub zewnętrznych Zespołach zmienia się na zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie (tzw. SOC), nakładając przy tym dodatkowe obowiązki (np. zgłoszeniowe, rejestracyjne w zakresie takiego zespołu); - nałożenie dodatkowych obowiązków na nowe zespoły np. w zakresie wprowadzania nowych zabezpieczeń, przeprowadzania analiz ryzyka **2. w zakresie uznawania, iż sprzęt lub oprogramowanie mają wysokie ryzyko dla cyberbezpieczeństwa państwa** - dotyczy m.in. operatora usługi kluczowej, - ocena bez wyraźnych kryteriów; - obowiązek wycofania sprzętu lub oprogramowania w ciągu 5 lat od komunikatu; - zakaz instalacji nowego sprzętu (zakaz wprowadzania do użycia); - wysoka kara za niedostosowanie się do oceny; - brak odpowiedzialności odszkodowawczej Skarbu Państwa; **3. Ostrzeżenia i polecenia zabezpieczające Pełnomocnika Rządu** - polecenie zabezpieczające ma formę decyzji administracyjnej o rygorze natychmiastowej wykonalności; - ostrzeżenia nie mają ustalonej formy; - nakaz określonego zachowania się, w tym zakaz zaprzestania użytkowania określonego sprzętu lub oprogramowania; - okres obowiązywania to 2 lata (ostrzeżenie może być jednorazowo przedłużone); - brak odpowiedzialności odszkodowawczej Skarbu Państwa; - dotyczy: • operatora usługi kluczowej również	odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej. Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji

			• właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, o których mowa w art. 3 ustawy z dnia z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców.	lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in.

				prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie

				mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało

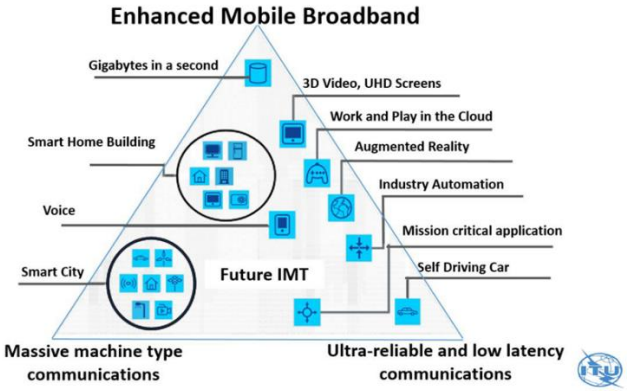
				także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
86.	Polski Związek Pracodawców	Uwaga ogólna	Wprowadzenie powyższych rozwiązań doprowadzi do sytuacji, w której dotychczasowa praktyka dbania o bezpieczeństwo ogólne – Państwa, poprzez opracowanie i wdrożenie rozwiązań gwarantujących bezpieczeństwo na poziomie poszczególnych	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione.

	Przemysłu Farmaceutycznego		podmiotów zastąpione zostanie systemem nakazowym, w którym to organy Państwa będą decydowały o tym jak zadbać o bezpieczeństwo poszczególnych podmiotów. Takie podejście do systemu bezpieczeństwa elektronicznego jest daleko nieefektywne z punktu widzenia rachunku ekonomicznego, a także zarządzania ryzkiem w przedsiębiorstwach. To podmioty stosujące na co dzień rozwiązania w zakresie bezpieczeństwa, dbając o swoje własne bezpieczeństwo poprzez stosowanie najlepszych praktyk i metodologii dostępnych na rynku, są najlepszym gwarantem tego bezpieczeństwa. Dotychczasowe rozwiązania, wypracowane wraz z rozwojem cyberbezpieczeństwa i funkcjonujące już od dłuższego czasu, sprawdzały się w dotychczasowej praktyce i są stosowane powszechnie na całym świecie. Ponadto podnieść należy, iż koszty ekonomiczne proponowanego rozwiązania mogą być niezwykle wysokie i mogą prowadzić do bezpośredniego zagrożenia egzystencji wielu podmiotów. **Szczególnie rozszerzenie zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej może przynieść katastrofalne skutki.** Samodzielne zarządzanie bezpieczeństwem opierające się na wewnętrznej, odzwierciedlającej własną architekturę, analizie i szacowaniu ryzyka spowodowały, iż podmioty zbudowały złożone i powiązane wzajemnymi zależnościami systemy zabezpieczeń. Zabezpieczeń analizowanych pod kątem swej skuteczności i aktualności w sposób ciągły, co jest krytyczne dla reagowania na często pojawiające się nowe zagrożenia. Systemy te, w zaproponowanym rozwiązaniu zawartym w projekcie ustawy, mogą być narażone na ograniczenie swojej funkcjonalności lub w ogóle na likwidację w oparciu o komunikaty bezpieczeństwa	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

			ogłoszone przez odpowiednie organy Państwa. Podkreślić przy tym trzeba, że wszelkie koszty związane z zawieszeniem i wymianą stosowanych rozwiązań zostały przerzucone w całości na podmioty, które już raz poniosły wymierne koszty. W tej sytuacji brak odpowiedzialności odszkodowawczej po stronie Państwa może spowodować, iż podmioty gospodarcze nie będą w stanie udźwignąć nałożonych na nie zobowiązań, nawet w perspektywie 5 letniej, jaka została założona na wymianę sprzętu uznanego za niebezpieczny. Do tego dołożyć należy również astronomiczne kary nałożone na operatorów usługi kluczowej za brak realizacji obowiązków określonych w projektowanej ustawie. Podkreślić również należy, iż brak jest jednoznacznych kryteriów jakimi mają posługiwać się organy administracji publicznej w ocenie dostawców sprzętu i oprogramowania. Nie zostały ustalone również minima czasowe w jakich mogłyby się odbywać oceny poszczególnych dostawców co niesie za sobą ryzyko dodatkowego zaskakiwania przedsiębiorców i brakiem możliwości faktycznej reakcji w sytuacji gdy budżet na zapewnienie dostępu do określonego sprzętu został wyczerpany, a dany dostawca z dnia na dzień został uznany za niebezpiecznego. Brak jest również odniesienia, w jakich systemach dane rozwiązanie jest niebezpieczne, co powoduje konieczność wymiany całości sprzętu lub oprogramowania bez względu na to czy w danym podmiocie faktycznie mogą one prowadzić do naruszenia zasad bezpieczeństwa. Mając na uwadze przedstawioną argumentację należy stwierdzić, iż obiektywny i oparty o przejrzystą metodologie proces oceny ryzyka cybernetycznego dostępnych technologii lub produktów miałby dużo większą korzystną wartość dla poziomu	W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			bezpieczeństwa i kondycji gospodarczej podmiotów niż nakazowo/zakazowy mechanizm dyskwalifikowania określonych producentów. Kolejnym argumentem przemawiającym za odstąpieniem od proponowanych rozwiązań jest fakt, iż większość producentów sprzętu elektronicznego korzysta z poddostawców usytuowanych w państwach azjatyckich, które z automatu spełniają przynajmniej jedno kryterium uznania ich za niebezpieczne (ochrona danych osobowych, ale również prawa człowieka). W tej sytuacji bardzo groźnym może być sytuacja, w której przy braku możliwości zakupu sprzętu uznawanego za bezpieczny, podmioty gospodarcze nie będą w stanie sprostać wymaganiom stawianym przez Organy administracji publicznej i tym samym mogą stać przed dylematem: kończyć swoją działalność czy ryzykować nałożenie absurdalnie wysokich kar. Projekt ustawy nie odpowiada na pytanie co w takiej sytuacji powinien dany podmiot uczynić. Przedstawiając powyższe uwagi obawiamy się sytuacji, w której wskazanie któregoś z wiodących producentów urządzeń elektronicznych, sparaliżuje dostęp do produktów tego producenta, a też pośrednio do innych bazujących na jego podzespołach. Może mieć to szczególny znaczenie dla przemysłu farmaceutycznego, gdzie wyśrubowane wymagania ze strony poszczególnych organów, w tym w szczególności na etapie wytwarzania leków – przez Głównego Inspektora Farmaceutycznego, dodatkowo zawężają już dość wąską niszę producentów automatyki i elektroniki przemysłowej, których urządzenia i podzespoły mogłyby stanowić	

			bazę np. dla linii produkcyjnych. Finalnie może skończyć się to zablokowaniem możliwości technicznych produkowania leków, zachwiania dostępności do tanich i sprawdzonych leków dostępnych na rynku od lat, a w konsekwencji do paraliżu polityki lekowej państwa i gwałtownym wzroście wydatków płatnika publicznego na droższe leki pochodzące z importu. **Mając na uwadze powyższe okoliczności uzasadnionym wydaje się odstąpienie od dalszego procedowania przedmiotowego projektu ustawy.**	
87.	T-Mobile Polska	Uwaga ogólna	Projekt ustawy proponuje uwzględnić w krajowym systemie cyberbezpieczeństwa podmioty działające na rynku telekomunikacyjnym. Warto wskazać, iż rynek telekomunikacyjny obecnie określany jest jako rynek komunikacji elektronicznej, na którym sieci oraz usługi dostarczają nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni ale również inne podmioty funkcjonujące dzisiaj poza rynkiem telekomunikacyjnym.	Wyjaśnienie Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

				administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
88.	T-Mobile Polska	Uwaga Ogólna	Punktem wyjścia jest przyjęcie założenia, iż przyszłe usługi łączności elektronicznej są (lub będą) świadczone w układzie trójkąta charakterystycznego dla modelu funkcjonowania sieci 5G:  Dla tak sformułowanego modelu, trójkąta usług łączności elektronicznej, rozszerza się liczba podmiotów/funkcji	Wyjaśnienie Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

			realizowanych w ramach komunikacji. Usługi łączności elektronicznej to nie tylko połączenie głosowe, szybki dostęp do sieci Internet (Enhanced Mobile Broadband) ale również: • sieci dedykowane dla komunikacji masowej IoT np. LTE-M, NB-IoT (Massive machine type communications), • sieci o wysokich parametrach jakościowych np. campus network's (Ultra-reliable and low latency communications). Dodatkowo, sieci te będą świadczyć usługi w ramach odpowiednich, wydzielonych warstw - tzw. 'network slicing', dedykując odpowiednie parametry jakościowe dla określonych rodzajów/grup usług np. usługi bankowe mogą wymagać wydzielonego zasobu sieciowego o określonych parametrach bezpieczeństwa, tworząc rozwiązanie E2E w ramach network slicing. Każdy podmiot, który bierze udział w realizacji komunikacji/przesyłaniu sygnałów jest podmiotem, który świadczy usługi łączności elektronicznej, czyli: • „*tradycyjni*" przedsiębiorcy telekomunikacyjni-operatorzy; • dostawcy urządzeń końcowych oraz systemów operacyjnych np. Samsung, IOS biorący udział w transmisji; • dostawcy rozwiązań chmurowych (np. Paas, Iaas); • dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0. (np. sieci campus network).	administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			Wszystkie te podmioty (nie tylko tradycyjnie postrzegani przedsiębiorcy telekomunikacyjni) powinny realizować działania w zakresie cyberbezpieczeństwa, w zależności od zakresu świadczonych usług oraz posiadanych możliwości technicznych, operacyjnych. Pominięcie, któregoś z tych podmiotów będzie oznaczało, iż albo część usług komunikacji elektronicznej nie będzie spełniać wymagań w zakresie cyberbezpieczeństwa. W tym zakresie niezbędne jest zweryfikowanie pojęć stosowanych w projekcie prawa komunikacji elektronicznej dotyczących przedsiębiorców świadczących usługi komunikacji elektronicznej oraz dostarczających sieci komunikacji elektronicznej. Przykładowo proponowane przepisy projektu ustawy najprawdopodobniej nie będą dotyczyć: • dostawców urządzeń końcowych oraz oprogramowania, biorących udział w transmisji i świadczeniu usług (np. masowa usługa RCS Google Message). Wynika to z przyjętej definicji sieci telekomunikacyjnej (w projekcie PKE), który wyłącza urządzenia końcowe (w domyśle wraz z oprogramowaniem) z pojęcia sieci telekomunikacyjnej. Jest to odmienne podejście od zastosowane EKŁE, gdzie pojęcie sieci łączności elektronicznej[15] nie wyłącza urządzeń końcowych. • dostawców rozwiązań chmurowych (np. usługi Paas, Iaas), pomimo tego, iż biorą udział w transmisji sygnałów. Wynika to z przyjętej definicji usługi	

			komunikacji elektronicznej (w projekcie PKE), która wyłącza usługi, które głównie nie zajmują się transmisji sygnałów. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie usług łączności elektronicznej obejmuje usługi, które częściowo (nie głównie, jak to jest w PKE), zajmują się transmisją sygnałów. • dostawcy sieci dla sieci prywatnych (niepublicznych) dla klientów B2B w ramach Przemysłu 4.0., pomimo tego, iż realizują sieci oraz usługi, które mają bardzo często charakter kluczowy dla bezpieczeństwa określonych branż. Wydaje się, że wynika to z przyjętej definicji przedsiębiorcy komunikacji elektronicznej (w projekcie PKE), która koncentruje się na dostarczaniu publicznych sieci telekomunikacyjnych. Jest to odmienne podejście od zastosowane w EKŁE, gdzie pojęcie dostarczanie sieci łączności elektronicznejabstrahuje od charakteru sieci, czy ma ona charakter publiczny, bądź niepubliczny oraz obejmuje urządzenia końcowe, które są zainstalowane w maszynach. Prawidłowo skonstruowane obowiązki w zakresie bezpieczeństwa powinny obejmować wszystkie podmioty działające na rynku komunikacji elektronicznej. W przeciwnym wypadku, może okazać się, iż niektóre podmioty będą miały większą swobodę działania w określonych segmentach rynku np. w budowaniu sieci niepublicznych pod rozwiązania IoT np. rozwiązania smart city, czy też sieci campusowych. W ten sposób może powstać pewna nierównowaga konkurencyjności między podmiotami.	

89.	T-Mobile Polska	Uwaga ogólna	Projekt ustawy proponuje wprowadzenie mechanizmu oceny ryzyka dostawcy sprzętu lub oprogramowania, który będzie mógł istotnie ograniczać działalność dostawcy sprzętu i oprogramowania. Jednakże istotne konsekwencje decyzji podjętej przez Kolegium, poza dostawcą, ponosić będą przede wszystkim operatorzy telekomunikacyjni, dostawcy usług, a nawet użytkownicy końcowi, którzy wykorzystują sprzęt lub oprogramowanie dostawcy będącego przedmiotem decyzji. W szczególności należy mieć na uwadze, iż rynek telekomunikacyjny charakteryzuje się bardzo dużym stopniem złożoności i zróżnicowaniem, które wychodzi poza działalność pojedynczych operatorów. Z tego względu decyzje Kolegium muszą mieć charakter bardzo wyjątkowy (incydentalny) i powinny zostać poprzedzone szeroką i wnikliwą analizą skutków regulacji. Z uwagi na wysoką rangę polityczną Kolegium, wszelkie analizy skutków regulacji, scenariuszy rozwiązań alternatywnych, źródeł finansowania kosztów oraz ewentualne rekomendacje dla Kolegium powinny każdorazowo być integralnym i niezbędnym elementem wniosku do Kolegium, aby następnie uzyskać wysoki poziom jakościowy ostatecznej decyzji Kolegium. Oznacza to, iż zdecydowany wysiłek merytoryczny powinien zostać położony na etap przygotowania wniosku o przeprowadzenie ostatecznej oceny przez Kolegium. Z kolei pod decyzję Kolegium powinien zostać poddany w pełni przygotowany wniosek, zawierający pełną informację, która umożliwi Kolegium podjęcie odpowiedzialnej decyzji, niosącej ze sobą wielorakie i długofalowe skutki dla rynku i użytkowników końcowych Z pewnością opinia Kolegium wpływa bezpośrednio na rachunek kosztów po stronie innych podmiotów. Z tego względu regulacja powinna dopuszczać mechanizm rekompensaty finansowej, który będzie mógł być zastosowany w uzasadnionych przypadkach, jak	**Uwaga nieuzwględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			również mechanizm przesunięcia w czasie wdrażania opinii, w celu minimalizacji obciążeń danego sektora. W celu zwiększenia pewności prawnej, projekt opinii Kolegium powinien zostać poddany konsultacji z zainteresowanymi podmiotami (w trybie właściwym, uznanym przez Kolegium).	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

90.	Polska Izba Komunikacji Elektronicznej	Uwaga ogolna	PIKE stanowczo sprzeciwia się rozszerzeniu zakresu przedmiotowego ustawy o KSC na przedsiębiorców z sektora telekomunikacyjnego. Art. 1 ust. 3 dyrektywy z UE/2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: dyrektywa NIS) wprost wyłącza stosowanie ogólnych regulacji dot. cyberbezpieczeństwa wobec przedsiębiorców telekomunikacyjnych w zakresie ich sieci i usług łączności elektronicznej. Pomimo że art. 3 dyrektywy NIS wskazuje poziom harmonizacji minimalnej, czyli umożliwia państwom członkowskim minimalne standardy regulacyjne, to jednak rozszerzenie jakiegokolwiek zakresu stosowania przepisów dyrektywy NIS nie może się odbywać wbrew jej innym bezwzględnie obowiązującym przepisom. Takim przepisem w istocie jest wspomniany art. 1 ust. 3 dyrektywy NIS. Ustawodawca europejski bowiem świadomie rozdzielił kwestie zachowania bezpieczeństwa sieci i usług telekomunikacyjnych od szeroko pojętego cyberbezpieczeństwa i w aktualnym stanie prawnym kompleksowo uregulował je w art. 40 i 41 dyrektywy 2018/1972 ustanawiającej Europejski Kodeks Łączności Elektronicznej (dalej: EKŁE). Ich wdrożenie do prawa polskiego nastąpi pod koniec roku przepisami projektowanej ustawy Prawo komunikacji elektronicznej (dalej: PKE). Tym samym, konsultowana nowelizacja ustawy o KSC niesłusznie oraz niezgodnie z przepisami dyrektywy NIS dubluje regulacje z rozdziału 5 PKE „Bezpieczeństwo sieci i usług oraz zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego” oddział 1 „Bezpieczeństwo sieci i usług”. Odrębność tej regulacji uwarunkowana jest potrzebą zapewnienia bezpieczeństwa w sieciach telekomunikacyjnych w oparciu o współpracę z	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			wyspecjalizowanymi organami telekomunikacyjnymi takimi jak Prezes Urzędu Komunikacji Elektronicznej czy CSIRT TELCO. Wobec powyższego, **PIKE postuluje o <u>zachowanie odrębności regulacyjnej sektora telekomunikacyjnego</u> w zakresie cyberbezpieczeństwa, a tym samym zrezygnowanie z rozszerzenia zakresu przedmiotowego ustawy o KSC na przedsiębiorców telekomunikacyjnych z uwagi na specyfikę prowadzonej przez nich działalności oraz <u>niezgodność takiej regulacji z przepisami unijnymi</u>**.	
91.	Polska Izba Komunikacji Elektronicznej	Uwaga ogólna	**Niezgodność przepisów ustawy o KSC z projektowanymi przepisami PKE oraz EKŁE – uwagi szczegółowe** Jak zostało wskazane powyżej, nie dość, że nowelizacja ustawy o KSC niepotrzebnie powiela regulacje projektowane w PKE, to robi to dodatkowo w sposób niezgodny z unijnymi przepisami EKŁE. Sprzeczności te są uwidocznione już w samych definicjach. W PKE (podobnie jak i w EKŁE) *incydent bezpieczeństwa* zdefiniowano jako „*każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci i usług".* Tymczasem ustawa o KSC określa *incydent telekomunikacyjny* jako „*incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej*". Łatwo dostrzec, że zakresy obu tych definicji są wyraźnie różne – w PKE mowa o rzeczywistym skutku dotyczącym bezpieczeństwa sieci i usług, podczas gdy ustawa o KSC wskazuje na rzeczywisty lub potencjalny skutek w dodatku tylko dla świadczenia usług. Dodatkowo definicja z ustawy o KSC błędnie obejmuje każdą przerwę ciągłości świadczenia usług bez względu na jej ważność, czas trwania czy jej przyczynę. Tym samym, **definicje te powinny zostać uzgodnione w kierunku zmiany definicji *incydentu telekomunikacyjnego* w ustawie o KSC w zgodzie z art. 2 pkt 42 EKŁE i art. 2 pkt 12 PKE.**	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.

			W kontekście precyzyjnego zdefiniowania *incydentu telekomunikacyjnego* na gruncie EKŁE i PKE, tym bardziej **nieuzasadniona jest regulacja art. 20a ust. 4 oraz art. 20b ust. 4 ustawy o KSC, które upoważniają właściwego ministra do dookreślenia w formie aktu wykonawczego – rozporządzenia**, jakie środki będą musieli przedsięwziąć przedsiębiorcy telekomunikacyjni aby takim incydentom zapobiegać, a także progów incydentu telekomunikacyjnego, których przekroczenie spowoduje powstanie obowiązku zgłoszenia incydentu. **W opinii PIKE są to kwestie zasadnicze dla przedmiotu tej ustawy – stanowią element definiujący zakres przedmiotowy regulacji i dlatego powinny być określone w ustawie, a nie w rozporządzeniach**. Forma rozporządzenia pozostawia zbyt duży zakres regulacji w gestii władzy wykonawczej, co może spowodować w skrajnych sytuacjach (w przypadku narzucenia obowiązku wymagającego dużych nakładów finansowych oraz zakresu pracy) konieczność modyfikacji długofalowych strategii konkretnej spółki, zarówno w przypadku określonych zadań kluczowych (poprzez przeniesienie środków), jak i strategii cyberbezpieczeństwa danego operatora telekomunikacyjnego. **Kolejnym przykładem nieuzasadnionego rozszerzenia zakresu regulacji ustawy o KSC** w porównaniu do przepisów PKE i EKŁE, **jest propozycja szczegółowego wyliczenia elementów zgłoszenia incydentu telekomunikacyjnego w art. 20d. Izba ocenia tę regulację jako zbyt szczegółową a także nadmiarową.** Katalog ten zawiera bowiem szereg elementów, których wskazanie w zgłoszeniu incydentu może okazać się niemożliwe, ponieważ przedsiębiorca telekomunikacyjny może nie posiadać na ich temat wiedzy, a co w konsekwencji znacząco utrudni, a czasami nawet uniemożliwi dokonywanie przez przedsiębiorców zgłoszeń.	Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			Dodatkowo, Izba wskazuje na szereg szkodliwych regulacji dotyczących współpracy przedsiębiorców telekomunikacyjnych z różnymi podmiotami i organami w zakresie cyberbezpieczeństwa. W pierwszej kolejności niepokoją nowe prawa CSIRT MON, CSIRT NASK i CSIRT GOV względem sektora telekomunikacyjnego, ponieważ ich przyznanie następuje kosztem uprawnień Prezesa UKE oraz CSIRT TELCO. Taka regulacja jest wadliwa, ponieważ rozdrabnia ona prace nad zapewnieniem bezpieczeństwa sieci i usług telekomunikacyjnych pomiędzy wiele organów niewyspecjalizowanych w kwestiach telekomunikacyjnych. Przykładowo, **art. 26 ustawy o KSC wyraźnie wskazuje na uprawnienia CSIRT MON, CSIRT NASK i CSIRT GOV przy badaniu wszelkiej podatności i incydentów telekomunikacyjnych, pomijając całkowicie przy tej regulacji Prezesa UKE i CSIRT TELCO. Oznaczać to będzie, że przedsiębiorcy telekomunikacyjni przy zwalczaniu incydentów telekomunikacyjnych nie będą wiedzieć z którym CSIRT w danym momencie współpracować, a ponadto część z tych CSIRT przy swoich działaniach będą kierowały się własnymi priorytetami niezwiązanymi z rynkiem telekomunikacyjnym. Dodatkowo taka treść regulacji jest sprzeczna z przepisami PKE i EKŁE.** Następny problem to rozszerzenie katalogu podmiotów współpracujących w zakresie cyberbezpieczeństwa z SOC operatorów usług kluczowych (wśród których są też niektórzy przedsiębiorcy telekomunikacyjni). Powoduje to w szczególności pojawienie się nowego **obowiązku współpracy tych SOC z organami wymiaru sprawiedliwości, co PIKE ocenia jako nieproporcjonalne i nadmiarowe.** Przedsiębiorcy telekomunikacyjni mają już własne procedury współpracy z organami wymiaru sprawiedliwości, uwzgledniające kwestie ochrony tajemnicy telekomunikacyjnej. Zachodzi obawa, ze	

			odrębnie uregulowany w ustawie o KSC obowiązek współpracy z organami wymiaru sprawiedliwości w oderwaniu od regulacji telekomunikacyjnych może grozić naruszeniami przepisów o ochronie tajemnicy telekomunikacyjnej. Jako zbędną należy również ocenić konieczność współpracy przedsiębiorców telekomunikacyjnych z ISAC. Izba wskazuje, że **rola tej instytucji nie dotyczy zwalczania incydentów telekomunikacyjnych, a jedynie dokonywania analizy i wymiany informacji na temat potencjalności zagrożenia incydentami. Tymczasem informacje o incydentach telekomunikacyjnych powinny być gromadzone wyłącznie przez CSRIT TELCO co pozwolili na skoncentrowane działania rządowe do zwalczania tych incydentów we współpracy z rynkiem. Ponadto przepisy PKE ani EKŁE nie przewidują utworzenia takiej instytucji.**	
92.	Polska Izba Komunikacji Elektronicznej	Uwaga ogólna	**Rozszerzenie uprawnień Kolegium oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa** PIKE wskazuje, że projektowana ustawa o KSC istotnie rozszerza kompetencje Kolegium ds. Cyberbezpieczeństwa oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa, **przekształcając je z organów pierwotnie doradczo-opiniujących w organy o uprawnieniach mających fundamentalny wpływ na prowadzoną przez przedsiębiorców działalność gospodarczą**. Chodzi tutaj w szczególności o umożliwienie dokonywania oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa oraz wydawanie ostrzeżenia lub polecenia zabezpieczającego w przypadku możliwości wystąpienia lub realnego wystąpienia incydentu telekomunikacyjnego. Szczegółowa analiza powyższych kompetencji prowadzi do wniosku, że **regulacje te naruszają zasadnicze zasady prawa administracyjnego**. Mianowicie, brakuje informacji o charakterze prawnym ostrzeżenia, o konsekwencjach wydanego ostrzeżenia,	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec

			brakuje określenia obowiązku przeprowadzenia konsultacji z zainteresowanymi podmiotami, określenia mechanizmu odwoławczego od ostrzeżenia i polecenia zabezpieczającego, w sytuacji, w której niezastosowanie się do ich treści zagrożone jest wysokimi karami pieniężnymi. Tym samym, **całość projektowanych regulacji art. 66a-66c oraz 67a-67c ustawy o KSC jest wyjątkowo szkodliwa i naruszające podstawowe zasady prowadzenia działalności gospodarczej przez przedsiębiorców telekomunikacyjnych, pozbawiając ich faktycznego udziału w procesie decyzyjnym, a także realnej kontroli sądowej i administracyjnej wydanych decyzji**. Co się tyczy uwag szczegółowych dotyczących nowych kompetencji organów, PIKE chciałoby się pochylić przede wszystkim nad przepisami dot. wycofania sprzętu z użytku (czyli również sprzętu telekomunikacyjnego) ze względu na aspekty cyberbezpieczeństwa. W konsekwencji, regulacja ta umożliwia narzucenie zakupu czy wdrożenia konkretnego rozwiązania technicznego, określonego producenta, co w swoich skutkach może spowodować ograniczenie konkurencji, wzrost kosztu budowy sieci telekomunikacyjnych oraz wprowadza możliwość prowadzenia lobbingu przez producentów. Racjonalizacja tej regulacji powinna polegać przede wszystkim na jasnym określeniu norm i standardów dla sprzętu, a następnie na stopniowym wygaszeniu produkcji sprzętu niespełniającego wymogów, nie zaś na zakazywaniu używania sprzętu, który został legalnie wyprodukowany i wprowadzony do obrotu zgodnie z przepisami prawa i normami obowiązującymi w chwili produkcji i wprowadzenia do obrotu. Skutki ekonomiczne wycofania urządzeń i oprogramowania są wymierzone w przedsiębiorców telekomunikacyjnych, które nie powinny ponosić odpowiedzialności za zgodność tych urządzeń i	którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa

			oprogramowania z nowymi wymogami bezpieczeństwa ustalone przez organy nie związane nawet z rynkiem telekomunikacyjnym. W efekcie proponowanych regulacji ustawy o KSC przedsiębiorcy telekomunikacyjni poniosą ogromne straty finansowe z przyczyn, za które nie ponoszą odpowiedzialności, oraz których nie mogli nawet przewidzieć ani im zapobiec przy zachowaniu najwyższej staranności. Na uwagę zwraca bowiem fakt, ze kontroli przez Kolegium i Pełnomocnika nie podlegają same urządzenia czy oprogramowanie, ale ich producent. W tym zakresie konieczne byłoby zastosowanie mechanizmu pokrycia strat bądź przyznawania rekompensat dla przedsiębiorców telekomunikacyjnych. Co więcej, regulacja ta uderzy jednakowo w małych jak i dużych przedsiębiorców telekomunikacyjnych używających sprzętu, który może zostać uznany za zakazany. Izba pragnie zwrócić również uwagę na inne aspekty nowego uprawnienia w zakresie nakazania usunięcia urządzeń i oprogramowania z sieci telekomunikacyjnej w ciągu 5 lat. Po pierwsze, termin ten będzie realnie krótszy, dlatego, że przedsiębiorcy telekomunikacyjni będą mieli problemy z serwisowaniem takich urządzeń i oprogramowania. Producent bowiem będzie wycofywał się z polskiego rynku, a ich ilość na rynku będzie się stale zmniejszała co podniesie cenę serwisu. W przypadku uszkodzenia takich urządzeń nie będzie nawet opłacalne ich naprawianie z uwagi na wcześniejszą konieczność ich usunięcia niż wynikałoby to z usługi serwisowej czy gwarancji producenta. Po drugie, nakaz usuwania urządzeń i oprogramowania uderzy w inwestycje telekomunikacyjne realizowane w ramach POPC a także w Ogólnopolską Sieć Edukacyjną. Konieczne będzie modyfikowanie tych sieci jeszcze w okresie ich trwałości, a więc niezgodnie z umowami publiczno-prywatnymi na te inwestycje.	pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania. Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73

			Najważniejszy zarzut Izby związany jest z faktem, że **zaprojektowana w swoim aktualnym brzmieniu regulacja narusza fundamentalne zasady prawa zagwarantowane Konstytucją RP**: 1. w zakresie **zasady praworządności** – nie określa jasnych i konkretnych norm i standardów jakie musi spełniać sprzęt czy też kryteriów, według których sprzęt jest uznawany za zgodny lub niezgodny z wymogami. Nie wskazuje także precyzyjnych procedur postępowania, formy podejmowania rozstrzygnięć itp., 2. w zakresie **zasady *lex retro non agit*** – ustanawia wymagania i reguły postępowania w stosunku do produktów wprowadzonych do obrotu w przeszłości, 3. w zakresie **zasady ochrony praw nabytych** – pozbawia przedsiębiorców prawa do korzystania ze sprzętu i wyposażenia nabytych przed wejściem w życie projektowanych przepisów, 4. w zakresie **zasady dwuinstancyjności postępowania** – projektowane przepisy nie określają niezależnej, obiektywnej, a także znanej przepisom kodeksu postępowania administracyjnego procedury odwoławczej.	zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest

				np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
93.	Polska Izba Komunikacji Elektronicznej	Uwaga ogólna	**Wpływ regulacji na sektor MŚP** Biorąc pod uwagę znaczące zmiany w zakresie cyberbezpieczeństwa dla przedsiębiorców telekomunikacyjnych, nie można zgodzić się z oceną skutków regulacji ustawy o KSC, która stwierdza brak jej wpływu na małe i średnie przedsiębiorstwa. Znaczną część rynku telekomunikacyjnego objętą tą regulacją stanowią bowiem przedsiębiorcy MŚP, a zatem wpływ tej ustawy, wbrew dokonywanym ocenom, na ich działalność gospodarczą będzie znaczący.	**Uwaga nieuwzględniona** Przedsiębiorcy komunikacji elektronicznej zostaną zobowiązani do wdrożenia adekwatnych (proporcjonalnych) do oszacowanego ryzyka środków technicznych lub organizacyjnych mających zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorcy ci będą musieli obsługiwać incydent telekomunikacyjny (co jest w ich dobrym interesie) a zgłaszać do CSIRT Telco i CSIRT

				poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu.
94.	Polska Izba Komunikacji Elektronicznej	Uwaga ogólna	PIKE wyraża poważne wątpliwości co do zasadności projektowanej nowelizacji ustawy o KSC w kontekście jej rozszerzenia na usługi i sieci telekomunikacyjne. Prezentowana regulacja wykazuje szereg niezgodności z przepisami bezwzględnie obowiązującymi prawa UE (dyrektywą NIS oraz dyrektywą EKŁE implementowaną do polskiego prawa projektem PKE). Ponadto, projektowane przepisy w szczegółach naruszają podstawowe zasady prawa administracyjnego oraz zasady prawa zagwarantowane Konstytucją RP. Tym samym całość projektowanej ustawy PIKE ocenia zdecydowanie negatywnie i postuluje o usunięcie regulacji związanych z rynkiem telekomunikacyjnym, w szczególności usunięcie uprawnień Kolegium oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa. Jednocześnie PIKE wnosi o pozostawienie wszystkich regulacji dotyczących sektora telekomunikacyjnego do wyłącznej regulacji aktualnie konsultowanego projektu PKE. Kwestie dotyczące bezpieczeństwa usług i sieci telekomunikacyjnych, ze względu na swoją specyfikę powinny być objęte jednym, kompleksowym aktem prawnym. Biorąc pod uwagę istotność przedmiotowego zagadnienia i jego wpływ na rynek telekomunikacyjny, PIKE wskazuje, że pozostaje do dyspozycji Ministra Cyfryzacji w przypadku potrzeby jakichkolwiek dalszych wyjaśnień i uzupełnień niniejszego stanowiska.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

				incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
95.	Fabryka E-Biznesu	Uwaga ogólna	Ustawa w proponowanym brzmieniu prowadzi do dyskryminacji niektórych z operatorów telefonii komórkowej, co w efekcie może doprowadzić do braku konkurencji na rynku telekomunikacyjnym, wzrostu cen, co bez wątpienia odbije się na konsumentach. Ponadto wejście w życie ustawy w obecnym brzmieniu spowoduje mniej korzystne warunki dla rozwoju sieci 5G w Polsce, czego efektem będzie opóźnienie wprowadzenia 5G w naszym kraju o kilka lat, na czym stracą polskie przedsiębiorstwa. Ponadto warto zaznaczyć, że krajowy system cyberbezpieczeństwa jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatora telekomunikacyjnego, ponieważ prawa i obowiązki operatora telekomunikacyjnego zostały szczegółowo określone w Prawie Komunikacji Elektronicznej (nowe prawo telekomunikacyjne) poprzez przyjęcie kodeksu komunikacji elektronicznej. Przyczyną takiego rozwiązania jest fakt, że dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do którego stosuje się przepisy ustawy o krajowym systemie cyberbezpieczeństwa, spowoduje nakładanie się przepisów i potencjalny konflikt. Zazwyczaj kluczowym dostawcą operatora	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

			infrastruktury krytycznej jest operator telekomunikacyjny i ma to ogromne znaczenie. Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE powoduje konstruktywne i interpretacyjne wątpliwości i zamieszanie. Co za tym idzie pozwolę sobie zasugerować postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC oraz przyjęcie, że KSC nie ma zastosowania do przedsiębiorstw komunikacji elektronicznej. Żywię ogromną nadzieję, że Ministerstwo Cyfryzacji zapozna się z głosem społeczeństwa i wprowadzi niezbędne zmiany w przepisach omawianego projektu ustawy.	incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

96.	Krajowa Izba Gospodarki Cyfrowej DigiCom Krajowa Izba Gospodarki Cyfrowej DigiCom	Uwaga ogólna Uwaga ogólna	Na wstępie trzeba podkreślić, iż zapewnienie bezpieczeństwa sieci i systemów informatycznych jest dziś priorytetowym wyzwaniem, z którym mierzyć się muszą rządy wszystkich rozwiniętych państw, w tym państw członkowskich UE. Nie ulega wątpliwości, że niezbędna jest regulacja tego obszaru, tak aby, w zgodzie z zasadami konkurencji, z jednej strony stworzyć warunki przyjazne do rozwoju tego sektora gospodarki, z drugiej zaś strony zabezpieczyć interesy podmiotów o słabszej pozycji rynkowej, tj. konsumentów. Projektowana ustawa ma niebagatelne znaczenie dla tempa wdrażania sieci 5G i co się z tym wiąże, rozwoju gospodarczego państwa. Stąd też procedowanie przedmiotowego projektu ustawy powinno być oparte o dogłębną analizę sytuacji rynkowej podmiotów na nim funkcjonujących, z uwzględnieniem specyfiki tego rynku. Należy zwrócić uwagę na rozwiązania niejasne i nieprecyzyjne. Regulacja dotyczy sektora zaawansowanego technicznie i technologicznie. Stąd też konieczne jest takie konstruowanie przepisów, by przesłanki, na podstawie których przyznawane są uprawnienia lub nakładane są obowiązki, były obiektywne i jasne, a wydawane w oparciu o nie rozstrzygnięcia poprawne i weryfikowalne. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. Projektowane rozwiązanie w postaci sporządzania przez Kolegium ds. Cyberbezpieczeństwa oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa oparte jest o niejasne kryteria. Jako, że nie są to przesłanki technologiczne, trudno je obiektywnie zweryfikować. Rozwiązanie to powinno raczej zmierzać w kierunku stworzenia mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. Ocena powinna być dokonywana nie tyle w odniesieniu do podmiotu, tj. dostawcy sprzętu, oprogramowania lub usług, co samego sprzętu czy oprogramowania. W przypadku sporządzenia oceny ryzyka określającej ryzyko jako wysokie podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu	**Uwagi częściowo uwzględnione** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa

97.	Install Tech	Uwaga ogólna	Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się się zaniepokojeni Projektem Ustawy, który może mieć negatywny wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT. Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na zatrudnienie i rozwój branży telekomunikacyjnej, co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty, konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
98.	Polska Izba Handlu	Uwaga ogólna	**Potencjalne naruszenia prawa** **1. Naruszenie polskich przepisów** **1)** Naruszenie prawa konstytucyjnego **a) Zasada proporcjonalności** Proponowane kryteria procedury ocennej, której efektem może być zakaz prowadzenia działalności gospodarczej w Polsce zostały określone w sposób **nieprecyzyjny**. Przepisy Projektu przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, bardzo duże uprawnienia i kompetencję do prowadzenia jednostronnego postępowania ocennego. Konsekwencje tego postępowania mogą wywrzeć olbrzymi wpływ na sytuację ekonomiczną danego dostawcy, ale również operatorów telekomunikacyjnych oraz konsumentów. Postępowanie przed Kolegium do spraw cyberbezpieczeństwa ma się w całości odbywać bez udziału ocenianego dostawcy, który dopiero z komunikatu w Monitorze Polskim dowie się, o przeprowadzonej ocenie. Dlatego też przyjęte rozwiązania legislacyjne są **sprzeczne z zasadą proporcjonalności wyprowadzoną z zasady demokratycznego państwa prawnego** (Art. 2 Konstytucji). **b) Niedziałanie prawa wstecz i pewność prawa** Projektowane przepisy w znaczący sposób podważają zaufanie obywateli do Państwa. Projekt zakłada niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy (w tym infrastruktury). W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą *lex retro non agit* (niedziałania prawa wstecz).	**Uwagi częściowo uwzględnione** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji.

			W związku z tym, że demokratyczne państwo prawne oznacza państwo w którym chroni się zaufanie obywatela do państwa i stanowionego przez nie prawa, ustawodawca dokonując kolejnych zmian stanu prawnego **nie może stracić z pola widzenia interesów podmiotów, jakie ukształtowały się przed dokonaniem zmiany stanu prawnego[16].** **c) Naruszenie zasady równości wobec prawa** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa (art. 32 Konstytucji). **d) Brak przeprowadzenia oceny skutków regulacji** Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z	Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o

[16] (wyrok TK z 13.04.1999 r., K 36/98, OTK 1999, Nr 3, poz. 40)

			powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu. **2) Naruszenie pozostałych przepisów polskiego prawa** **a) Naruszenie przepisów procedury administracyjnej** W projektowanych przepisach nie przewidziano prawa strony do udziału w postępowaniu ocennym, prowadzonym przez Kolegium. Proponowane rozwiązania naruszają więc podstawowe zasady postępowania administracyjnego wyrażone w ogólnych przepisach Kodeksu postępowania administracyjnego., m.in. zasadę pogłębiania zaufania obywateli do władzy publicznej (art. 8 kpa), zasadę udzielenia informacji przez organ (art. 9), zasadę wysłuchania stron (art. 10). Wprowadzone przepisy naruszają więc podstawowe prawo jednostki do czynnego udziału w postępowaniu. **b) Naruszenie prawa konkurencji w Polsce** Uregulowanie kwestii wykluczenia dostawców w ustawie KSC narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. nr 50, poz. 331 ze zm. Zgodnie z art. 1 ust. 2 tej ustawy, reguluje ona w szczególności zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu	uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów.	
99.	Polska Izba Handlu	Uwaga ogólna	**2. Niezgodność z prawem europejskim** a) **Brak notyfikacji przepisów Komisji Europejskiej** Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. b) **Naruszenie zasad TFUE** Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, naszym zdaniem, są sprzeczne z podstawowymi zasadami równego traktowania/niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), Art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), Art. 49 (zakaz ograniczeń swobody przedsiębiorczości) TFUE. c) **Naruszenie zasady niedyskryminacji w prawie UE** Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w	**Uwaga nieuwzględniona** Projekt jest zgodny z Traktatami unijnymi, w szczególności są to rozwiązania proporcjonalne i adekwatne do rozwiązywanego problemu.

			sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której "każdy jest równy wobec prawa". Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość". Europejski Trybunał Sprawiedliwości zauważył, że „zakaz dyskryminacji ustanowiony w prawie UE jest szczególnym wyrazem ogólnej zasady równości, która jest jedną z podstawowych zasad prawa wspólnotowego". Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów. d) **Naruszenie zasady proporcjonalności określonej przez ETS** Pkt 13 w sprawie C-331/88 Fedesa odnosi się do zasady proporcjonalności: Po wprowadzeniu środka dyskryminującego Trybunał przyjrzy się proporcjonalności środka w odniesieniu do jego celu. Innymi słowy, środek taki musi być (1) konieczny do osiągnięcia celu i nie może wykraczać poza to, co jest konieczne do osiągnięcia celu, (2) najmniej restrykcyjny środek do osiągnięcia tego celu, oraz (3) spowodowane niedogodności nie mogą być nieproporcjonalne do zamierzonych celów. e) **Naruszenie zasady swobodnego przepływu towarów** Zasada ta może być nadal naruszona, nawet jeśli państwo członkowskie nie ustanawia wyraźnego przepisu zakazującego przywozu produktów od niektórych dostawców. Jak wyjaśnił Europejski Trybunał Sprawiedliwości, każdy zakaz używania produktu na terytorium państwa członkowskiego UE wpłynie na zachowanie nabywców i wpłynie na dostęp tego produktu na rynku tego państwa członkowskiego. Przepisy mające na celu	

			odsunięcie określonego dostawcy od łańcucha dostaw w niektórych państwach członkowskich UE powstrzymają potencjalnych klientów przed kupowaniem produktów/technologii danego dostawcy. f) **Naruszenie dyrektywy o konkurencji** Dyrektywa 2002/77/WE w sprawie konkurencji zakazuje przyznawania wszelkich specjalnych praw w sektorze łączności elektronicznej. Projekt przyznaje jednak unijnym przedsiębiorstwom bezsporne przywileje skutecznego eliminowania konkurencji ze strony dostawców spoza UE, dyskryminując tym samym dostawców spoza UE (nawet tych najbardziej zaawansowanych technologicznie).	
100.	Polska Izba Handlu	Uwaga ogólna	**3. Naruszenie przepisów WTO** a) Układ Ogólny w sprawie Taryf Celnych i Handlu (GATT) zawiera klauzulę o najbardziej uprzywilejowanej pozycji. Członek WTO nie może dyskryminować indywidualnych partnerów handlowych, traktując niektóre kraje bardziej przychylnie niż inne b) Zasada krajowego traktowania GATT zobowiązuje członków WTO do traktowania "podobnych" produktów zagranicznych i krajowych, usług i usługodawców w równym stopniu. W przypadku stosowania krajowego obowiązku podejścia, produkty zagraniczne, usługi lub zagraniczni usługodawcy nie mogą podlegać mniej korzystnym regulacjom niż „podobny" produkt krajowy, usługodawca lub usługodawca krajowy (art. III GATT). c) Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na	**Uwaga nieuwzględniona** **P**orozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.

			bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie. **4. Zobowiązania dwustronne w ramach umów międzynarodowych** Przyjęcie prawodawstwa, które pozwoli na wykluczenie z polskiego rynku z podmiotów reprezentujących kapitał zagraniczny narusza zobowiązania podmiotów na mocy umów dwustronnych z innymi państwami. Na przykład, jeżeli dostawca z państwa trzeciego będzie wykluczony na podstawie niejasnych kryteriów, to może to zostać uznane za naruszenie przez Polskę obowiązku równego i sprawiedliwego traktowania na terytorium Polski na mocy Traktatu o Dwustronnej Inwestycji.	

101.	Polska Izba Handlu	Uwaga ogólna	**Uwagi techniczne dotyczące ryzyka i rozwiązań bezpieczeństwa** **4. Kryteria powinny być neutralne technologicznie, a nie uwzględniać względy polityczne:** 1) Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne a nie charakterystyka dostawcy; 2) Kryteria powinny mieć charakter techniczny, obiektywne, rozsądne i proporcjonalne, oraz zawierać odniesienie do oceny ryzyka zawartej w specyfikacjach technicznych 3) Projekt ustawy musi być zgodny zarówno z wymogami prawnymi dotyczącymi dobrych praktyk legislacyjnych, jak i z obowiązującymi przepisami, takimi jak prawo Unii Europejskiej, międzynarodowe prawo inwestycyjne, prawami człowieka i Konstytucją RP; **OCZEKIWANE DZIAŁANIA** Niezależnie od okoliczności, iż czas na odniesienie się do materii projektu jest niezwykle krótki i zostaliśmy praktycznie pozbawieni prawa przeprowadzenia pogłębionych analiz potencjalnego wpływu przedmiotowego aktu na funkcjonowanie gospodarki, zdecydowaliśmy się przedłożyć powyższe wstępne uwagi oraz propozycje zmian. Jednocześnie zwracamy się z prośbą o przeprowadzenie następujących działań: **POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH, GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI** W zakresie skutków społecznych należy opisać wpływ na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

102.	Krajowy Sekretariat Łączności NSZZ Solidarność	Uwaga ogólna	Po analizie przedstawionego do konsultacji projektu ustawy uważamy, że wymaga on istotnych zmian, a przede wszystkim znacznego ograniczenia swojego zakresu. W swoim aktualnym kształcie zakłada on bardzo daleko idące zmiany dotykające przedsiębiorstw telekomunikacyjnych oraz prowadzonej przez nich działalności gospodarczej. Nie mamy żadnych wątpliwości, że jego ewentualne przyjęcie w obecnym kształcie będzie miało negatywny wpływ na kondycję tego sektora gospodarki, a więc i zatrudnianych w nim pracowników. Projekt nie przewiduje żadnych uproszczeń w zakresie działalności telekomunikacyjnej, o które wielokrotnie wnioskowaliśmy, a wręcz przeciwnie skupia się na nakładaniu nowych obowiązków i ograniczeń, a także bardzo poważnym wzmocnieniu możliwości wpływu instytucji państwowych na nasze bieżące funkcjonowanie. Przedstawiona propozycja zmian prawnych pojawiła się w okresie, w którym potencjał przedsiębiorców telekomunikacyjnych skupiony jest na realizacji inwestycji w nowoczesne sieci, utrzymanie ciągłości działania usług oraz przygotowanie do wdrożenia Prawa komunikacji elektronicznej. Co więcej, w samym obszarze bezpieczeństwa jesteśmy zaangażowani we wdrożenie do 30 grudnia br. postanowień rozporządzenia w sprawie warunków technicznych i organizacyjnych wydanego do art. 175d PT, nad którym prace trwały ponad pół roku, i które wydawało się, że adresuje już kwestie bezpieczeństwa w zakresie sieci 5G. Niestety, ale wraz z kolejnymi propozycjami zmian prawnych, jesteśmy w sytuacji, w której wciąż trwa dyskusja o rozwiązaniu kluczowych problemów zidentyfikowanych przez administrację, ale wciąż jest brak jest samych rozwiązań. Jakkolwiek jesteśmy przeciwnikami zbytniego pośpiechu we wprowadzaniu istotnych dla sektora regulacji, tak	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			musimy skonstatować, że przedłużająca się faza niepewności nie ułatwia prowadzenia działalności gospodarczej. Szczególnie, że trudno nie zauważyć, że rozwiązania już wprowadzone i planowane powodują istotny chaos. Obecnie trudno już nadać właściwe znaczenie wprowadzonym już: (1) zmianom w rozporządzeniu do art. 175d PT (które mimo że musi być wdrażane nie jest utrzymywane w projekcie nowelizacji PKE i jego los jest faktycznie nieznany), (2) możliwym do wydania rekomendacjom Pełnomocnika Rządu ds. Cyberbezpieczeństwa, (3) opracowywanym wymaganiom dla aukcji częstotliwości określanych przez UKE i opiniowanych przez Kolegium, w kontekście planowanych kolejnych potężnych kompetencji organów administracji, tj.: (1) ocen dokonywanych przez Kolegium, (2) ostrzeżeń Pełnomocnika, (3) poleceń zabezpieczających Pełnomocnika. Tymczasem projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zakłada włączenie naszego sektora, już od 21 grudnia br. do zupełnie nowego reżimu prawnego. Niezależnie od oceny takiego działania jako nieuzasadnionego, uważamy, że takie strukturalne zmiany wymagają odpowiedniego przygotowania i czasu na wdrożenie. Tym samym proponowana ustawa stanowi kolejne obciążenie naszego sektora, które jednocześnie jest przedstawione bez wcześniejszej dyskusji i szerszego uzasadnienia. Obciążenie, które będzie wiązało się z dodatkowymi kosztami i wysiłkiem organizacyjnym. Trudno nam zaakceptować taki sposób procedowania szczególnie, że bardzo skromny zakres przedstawionych w uzasadnieniu i OSR informacji skłania nas do konkluzji, że sam projekt ustawy powstawał w pośpiechu i niekoniecznie był przedmiotem wystarczającej refleksji odnośnie swoich skutków. Tym bardziej, że w naszej ocenie wysiłek ten	

			będzie zupełnie nieproporcjonalny wobec potencjalnych pozytywnych skutków. Wręcz przeciwnie, uważamy, że nagłe wprowadzenie omawianej ustawy w znaczącym stopniu utrudni realizację zadań w zakresie bezpieczeństwa i integralności. **Włączenie przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa – koncepcja z której należy zrezygnować.** Za zupełnie niezrozumiałą, szczególnie w kontekście braku przedstawienia uzasadnienia, uważamy koncepcję przeniesienia lub powtórzenia przepisów dot. obowiązków przedsiębiorców telekomunikacyjnych, w tym zakresie zgłaszania naruszeń/incydentów do ustawy o krajowym systemie cyberbezpieczeństwa. Wszystkie wymagania w tym zakresie są już regulowane ustawą – Prawo telekomunikacyjne oraz w sposób zgodny z EKŁE proponowane w projekcie prawa komunikacji elektronicznej. Przedsiębiorcy są obowiązani do zgłaszania wszystkich naruszeń/incydentów według ustalonych w rozporządzeniu progów oraz formularza. Informacje te Prezes UKE może przekazywać do właściwych CSIRT. CSIRT mogą współpracować z innymi podmiotami krajowego systemu cyberbezpieczeństwa. Regulacja ta jest kompletna i daje podmiotom dla których te informacje mogą być istotne możliwość dostępu do nich. Jeśli istnieją w tym zakresie jakiekolwiek deficyty proponujemy, aby zostały one w pierwszej kolejności wyartykułowane, a następnie przedyskutowane. Jesteśmy bowiem przekonani, że zwiększenie wiedzy CSIRT o incydentach w obszarze telekomunikacji nie wymaga włączania tego sektora do krajowego systemu cyberbezpieczeństwa. A szczególnie w tak krótkich jak przewidziane terminach i niejasny także z legislacyjnego punktu widzenia sposób.	

			Na tym etapie uważamy za niezbędne usunięcie z projektu przepisów zakładających włączenie sektora telekomunikacyjnego do krajowego systemu cyberbezpieczeństwa.	

103.	Krajowy Sekretariat Łączności NSZZ Solidarność	Uwaga ogólna	**Ocena bezpieczeństwa dostawców – postulujemy uwzględnienie potencjału narzędzi certyfikacyjnych.** Dyskusja nt. oceny bezpieczeństwa dostawców ma charakter globalny, a w UE i poszczególnych krajach trwają prace nad regulacjami mającymi tę kwestię właściwie zaadresować. Nie jest przedmiotem niniejszego stanowiska ocena zasadności tych działań, gdyż mają one w dużej mierze charakter polityczny, ekonomiczny, a potencjalnie także wywiadowczy. Z perspektywy przedsiębiorców telekomunikacyjnych zaznaczamy jednak, że jakiekolwiek decyzje w tym obszarze muszą uwzględniać ich potencjalny wpływ na koszty, dostępność i jakość usług telekomunikacyjnych w Polsce. W praktyce oznacza to, że należało będzie każdorazowo precyzyjnie określać koszty danego rozwiązania, w tym wskazywać czy dane rozwiązanie faktycznie podniesie poziom bezpieczeństwa narodowego w cyberprzestrzeni i czy koszt jego wprowadzenia jest proporcjonalny wobec tego efektu. Nie można bowiem pominąć faktu, że skutki ewentualnych wykluczeń będą miały swój wpływ finansowy oraz konkurencję zarówno na rynku dostawców, jak i wobec użytkowników ich urządzeń, w tym z sektora telekomunikacyjnego. Finalne obciążenia w tym zakresie mogą więc dotykać przede wszystkim konsumentów usług, co zresztą potwierdzono w samym OSR projektu. Odnosząc się bezpośrednio do zaprezentowanego modelu oceny, w naszej ocenie: • należy uzupełnić go o element technicznej, w tym opartej na certyfikacji. Ponadto jego zakres jest zbyt szeroki i nie odnosi się do z góry ustalonego zakresu kluczowych zasobów, pod kątem których miałaby być dokonywana ocena danego dostawcy;	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			• skutki ewentualnych wykluczeń muszą odnosić się do z góry określonej kategorii zasobów oraz zastosowań o charakterze kluczowym dla bezpieczeństwa, co ogromnie poprawiłoby przejrzystość tej regulacji oraz pozwalało na dostosowanie strategii działania, w tym obszarze; • procedura oceny oraz jej publikacji muszą być precyzyjnie określone i umożliwiać zainteresowanym stronom przynajmniej przedstawienie stanowiska w toku oceny oraz złożenie odwołania do decyzji finalnej;	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
104.	Krajowy Sekretariat Łączności NSZZ Solidarność	Uwaga ogólna	**Kary – zbyt wysoki poziom kar pieniężnych** W naszej ocenie potencjalne kary pieniężne w wys. 3 lub 1% światowego obrotu karanego podmiotu są zdecydowanie zbyt wysokie, szczególnie, że dla podmiotów publicznych mogą wynosić nie więcej niż 100 tys. zł. Stanowi to w naszej ocenie niczym nie uzasadnioną dysproporcję, szczególnie, że w obszarze bezpieczeństwa publicznego to właśnie organy i jednostki państwa mają do realizacji kluczową rolę. Postulujemy redukcję maksymalnego poziomu kar co najmniej 10-krotnie oraz wykreślenie odwołania do obrotu „światowego".	**Uwaga nieuwzględniona** Kary są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego.
105.	MJC	Uwaga ogólna	W związku z zaproszeniem społeczeństwa, przez Ministerstwo Cyfryzacji, do udziału w konsultacjach dotyczących projektu ustawy o cyberbezpieczeństwie, niniejszym wyrażam swoją dezaprobatę w stosunku do proponowanej regulacji. Projekt ustawy w obecnym brzmieniu, w mojej ocenie narusza podstawowe przepisy prawa polskiego. Koliduje z kluczowymi, konstytucyjnymi zasadami prawa. Wejście w życie tegoż projektu ustawy wywoła ryzyko naruszenia polskich przepisów. Poniżej pozwoliłem sobie wymienić największe z moich obaw, czyli naruszenie przepisów konstytucyjnych: 1. **Zasada proporcjonalności** - Przepisy Projektu w art. 66a przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, nieograniczoną i pozbawioną kontroli sądowej kompetencję do prowadzenia jednostronnego postępowania ocennego, bez udziału ocenianego dostawcy, który o przeprowadzonej ocenie ma dowiedzieć się dopiero z komunikatu w Monitorze Polskim. Konsekwencje takiego postępowania mogą wywrzeć olbrzymi wpływ na sytuację	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka

			ekonomiczną danego dostawcy, operatorów telekomunikacyjnych oraz konsumentów. Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania, a ponadto odwołanie nie zawiesza wykonalności decyzji. Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia strony zainteresowanej obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu. 2. **Pewność prawa** - Projekt, w art. 66b zakłada rażąco niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy. W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą lex retro non agit. Ustawodawca dokonując kolejnych zmian stanu prawnego musi mieć na względzie interesy podmiotów, które ukształtowały się przed dokonaniem zmiany stanu prawnego. 3. **Równość wobec prawa -** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa. **Brak przeprowadzenia analizy skutków jakie wywoła wprowadzenie regulacji -** Zmiany zawarte w projekcie nowelizacji ustawy mogą wiązać się z negatywnymi skutkami wśród społeczeństwa tj. likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego,	zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

			gospodarczymi - obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli i politycznymi. Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Przepisów prawa konkurencji: 1. Uregulowanie kwestii wykluczenia dostawców w ustawie narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do podmiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Reguluje ona w szczególności zasady i tryb postępowania w stosunku do podmiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów. Bez wątpienia niniejszy projekt wzbudza więcej kontrowersji i konieczna jest jego dodatkowa analiza oraz naniesienie zmian, tak aby nie wywoływał on negatywnych skutków wśród polskich obywateli.	Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
106.	IAB Polska	Uwaga ogólna	Ustawa o Krajowym Systemie Cyberbezpieczeństwa, implementująca do polskiego porządku prawnego Dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, została uchwalona dwa lata temu. Okres jaki minął od implementacji skutecznie udowodnił, co jest piętą achillesową polskiego systemu cyberbezpieczeństwa tj. brak	**Wyjaśnienie** Projekt ma celu zwiększenie cyberbezpieczeństwa na poziomie krajowym, stąd też przewiduje się powołanie CSIRT sektorowych.

			przewidzianych adekwatnych środków pieniężnych oraz problem z dostępem odpowiednio wykwalifikowanych specjalistów. Do tej pory nie udało się zakończyć procesu wyznaczania operatorów usług kluczowych oraz powołano tylko jeden zespół odpowiadający za obsługę lub wsparcie obsługi incydentów w konkretnym sektorze tj. CSIRT KNF dla sektora finansowego przy Komisji Nadzoru Finansowego. W tych okolicznościach polski rząd planuje powołać dalsze CSIRT-y i SOC-i oraz uzupełnić krajowy system cyberbezpieczeństwa o nową grupę podmiotów, która na gruncie dotychczasowej ustawy o KSC była co do zasady sektorowo wyłączona tj. przedsiębiorców komunikacji elektronicznej.	
107.	IAB Polska	Uwaga ogólna	**I. Zmiany dotyczące przedsiębiorców komunikacji elektronicznej** Jak zostało wskazane w uzasadnieniu Projektu, coraz większe znaczenia dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. W *5G Toolbox*, Państwa członkowskie zobowiązały się m.in. do zaostrzenia wymagań w zakresie bezpieczeństwa infrastruktury i usług telekomunikacyjnych. Zgodnie z uzasadnieniem Projektu, analizowane zmiany do ustawy o KSC są elementem działań na rzecz wdrożenia postanowień tego dokumentu. Projekt wdraża również postanowienia Europejskiego Kodeksu Łączności Elektronicznej. Zgodnie z treścią Projektu, przedsiębiorcy komunikacji elektronicznej staną się częścią krajowego systemu cyberbezpieczeństwa poprzez dodanie w zakresie ustawy o KSC Rozdziału 4a „Obowiązki przedsiębiorców komunikacji elektronicznej”, w którym będą uregulowane kwestie dotyczące obowiązku stosowania przez przedsiębiorców komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów

			usług. IAB Polska pragnie zwrócić uwagę, że miejscem przedmiotowych regulacji dotyczących sektora telekomunikacyjnego nie powinna być ustawa o KSC, która do tej pory zawierała wyłączenie sektorowe w zakresie usług telekomunikacyjnych, ale projekt PKE. Analizowane przepisy posługują się pojęciem przedsiębiorcy komunikacji elektronicznej dla określenia obowiązków tam zawartych. Projektowane brzmienie ustawy o KSC odwołuje się w zakresie definicji pojęcia przedsiębiorcy telekomunikacyjnego do projektu ustawy o PKE. Zgodnie z obecnym brzmieniem art. 2 pkt 41 projektu PKE **przedsiębiorca komunikacji elektronicznej** to przedsiębiorca telekomunikacyjny lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów. Z kolej **usługa komunikacji interpersonalnej niewykorzystująca numerów** oznacza usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej, w tym usługę, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji (art. 2 pkt 77 projektu PKE). Należy zauważyć, że pojęciu „usługi komunikacji interpersonalnej" (art. 2 pkt 77 projektu PKE) odpowiada zawarta w EKŁE definicja „usługi łączności interpersonalnej" (art. 2 pkt 5 EKŁE). Nie ulega wątpliwości, że przepisy krajowe stanowiące implementację konkretnej dyrektywy powinny być interpretowane w zgodzie z jej brzmieniem. W związku z	usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Przedsiębiorcy komunikacji elektronicznej zostaną zobowiązani do wdrożenia adekwatnych (proporcjonalnych) do oszacowanego ryzyka środków technicznych lub organizacyjnych mających zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorcy ci będą musieli obsługiwać incydent telekomunikacyjny (co jest w ich dobrym interesie) a zgłaszać do CSIRT Telco i CSIRT poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu.

			powyższym przy interpretacji projektu PKE warto odwołać się do treści EKŁE. Motyw 17 zd. 1 EKŁE wprost wskazuje, że usługi łączności interpersonalnej obejmują wszystkie rodzaje poczty elektronicznej: „*Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych*”. Dodatkowo, poczta elektroniczna spełnia wszystkie przesłanki powyższych analogicznych definicji. W tym zakresie pewną trudność interpretacyjną może sprawiać jedynie przesłanka interaktywności, która jednak została wyjaśniona w przytoczonym już powyżej motywie 17 zd. 4 i 5 EKŁE – „*Łączność interaktywna oznacza, że usługa umożliwia odbiorcy informacji odpowiedź. Usługi, które nie spełniają tych wymogów, takie jak linearne usługi medialne, wideo na żądanie, strony internetowe, sieci internetowe, serwisy społecznościowe, blogi lub wymiana informacji między urządzeniami, nie powinny być uznawane za usługi łączności interpersonalnej*”. Na marginesie należy zauważyć, że poczta elektroniczna nie może mieścić się również w zakresie wyłączenia zawartego w art. 2 pkt 77 PKE tj. „usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej”. Nie ulega bowiem wątpliwości, że w przypadku poczty elektronicznej interaktywna komunikacja stanowi jej istotę. Z powyższej analizy wynika, że posługiwanie się w propozycji nowelizacji ustawy o KSC pojęciem przedsiębiorcy komunikacji elektronicznej powoduje, że wskazane obowiązki znajdą zastosowanie również do podmiotów takich jak np. dostawcy	

			poczty elektronicznej, co należy uznać za podejście zbyt daleko idące. Projekt nowelizacji ustawy o KSC zakłada nałożenie na podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów analogicznych obowiązków jak na przedsiębiorców telekomunikacyjnych. W ocenie IAB zasadne jest w tym miejscu zaprezentować analogiczne stanowisko jak w przypadku projektu PKE. Przepisy ustawy o KSC uwzględniając regulacje zawarte w EKŁE powinny różnicować obowiązki dostawców usług lub sieci telekomunikacyjnych (nakładać dalej idące obowiązki) oraz dostawców usług łączności interpersonalnej niewykorzystującej numerów (nakładać obowiązki o mniejszym zakresie). Potwierdza to motyw 95 EKŁE, zgodnie z którym: *„Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze. Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli*	

			dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału". W związku z powyższym IAB Polska postuluje, aby regulacje wdrażane do ustawy o KSC nie wychodziły poza ramy regulacyjne wynikające z dyrektywy EKŁE, gdyż **zrównywanie obowiązków w zakresie bezpieczeństwa sieci i usług dla wszystkich przedsiębiorców komunikacji elektronicznej nie znajduje uzasadnienia,** natomiast może prowadzić do zaburzenia zasad konkurencyjności poprzez niepotrzebne obciążanie dodatkowymi obowiązkami przedsiębiorców nie sprawujących rzeczywistej kontroli nad transmisją danych. Należy tutaj zauważyć, że w sposób oczywisty realizacja nowych obowiązków pociąga za sobą konieczność poniesienia dodatkowych i wysokich kosztów w zakresie wdrożenia odpowiednich rozwiązań. Postulujemy zatem, aby dostawcy usług komunikacji elektronicznej, którzy nie sprawują rzeczywistej kontroli nad transmisją sygnału, w tym w szczególności dostawcy usług komunikacji interpersonalnej niewykorzystującej numerów byli zwolnieni z obowiązków w zakresie bezpieczeństwa sieci i usług przewidzianych w projektowanym rozdziale 4a nowelizacji KSC. Obowiązki te są właściwe jedynie dla przedsiębiorców telekomunikacyjnych sprawujących kontrolę nad sygnałem i posiadających właściwe ku takiej kontroli środki lub których podjęcie uzasadnia charakter dostarczanych przez nich usług i znajduje oparcie w EKŁE. Warto zauważyć, że zachowanie ciągłości dostarczania sieci telekomunikacyjnej powinno spoczywać na dostawcy usług telekomunikacyjnych a nie bezpośrednio oddziaływać również na korzystających z takiej sieci dostawców usług OTT. Należy zwrócić uwagę, że o ile operatorzy telekomunikacyjni dysponują całością infrastruktury technicznej, to już np.: operatorzy poczty	

			elektronicznej nie mają na nią wpływu i funkcjonują na „cudzym" sprzęcie lub dostępie. Objęcie tymi samymi obowiązkami co dostawca telekomunikacyjny dostawcy poczty elektronicznej czy czatu wydaje się nie tyle nieuzasadnione co wręcz szkodliwe i niebezpieczne dla zasad prawa konkurencji oraz wolności gospodarczej na rynku usług komunikacji elektronicznej a przede wszystkim nie spełnia intencji stojącej za regulacjami wynikającymi z EKŁE. Dolegliwości finansowe wynikające z konieczności spełnienia nowych obowiązków przez dostawców usług komunikacji interpersonalnej niewykorzystującej numerów mogą prowadzić do tego, że rachunek ekonomiczny dalszego prowadzenia takiej usługi będzie nieopłacalny. Zimniejszy się tym samym katalog oferowanych usług, ich różnorodność oraz próg dostępu dla użytkowników końcowych, co wiąże się nie tylko ze stratą dla nich ale i dla krajowej przedsiębiorczości i konkurencyjności na rynku europejskim. Dodatkowo, Projekt wydaje się być niekompatybilny z przepisami projektu PKE. Przykładowo, projektowany artykuł 20c ustawy o KSC odwołuje się do przedsiębiorcy komunikacji elektronicznej, o którym mowa w art. 47 ust. 1 projektu PKE. Tymczasem wskazany przepis PKE dotyczy wyłącznie przedsiębiorcy telekomunikacyjnego, czyli nie całej kategorii przedsiębiorców komunikacji elektronicznej. Mając na uwadze powyższe należy skonstatować, że przedstawiony do konsultacji projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych z dn. 7 września 2020 r. jest pełen terminologicznych niejasności i nieprzystających do praktyki rynkowej rozwiązań i obowiązków, co pozwala sądzić, że ujęcie w rozdziale 4a usług	

			komunikacji interpersonalnej, w tym poczty elektronicznej czy innych usług OTT, jest oczywistym przeoczeniem	
108.	Federacja Konsumentów	Uwaga ogólna	Z zadowoleniem dostrzegamy inicjatywę zapewnienia bezpieczeństwa świadczonych usług elektronicznych, w tym telekomunikacyjnych, oraz świadomego i odpowiedzialnego korzystania z nowoczesnych technologii. Bezpieczeństwo 5G jest dziś szczególnie ważne, zwłaszcza w kontekście wszechobecnych *fake newsów* dotyczących wpływu 5G na zdrowie i prywatność konsumentów. Jednocześnie apelujemy do Resortu o to, aby skutki wprowadzanych w tym zakresie rozwiązań nie oddziaływały negatywnie na konsumentów. Wiemy z doświadczenia, że za każdy, nawet najbardziej zasadny, obowiązek nałożony na przedsiębiorców, skutkujący koniecznością rozbudowania struktur czy wdrożenia dodatkowych rozwiązań, zawsze finalnie płaci klient w opłacie za otrzymaną usługę. Analiza konsultowanego Projektu, prowadzi do wniosku, że Krajowy System Cyberbezpieczeństwa po noweli będzie przedsięwzięciem kosztownym, którego skutki są trudne do przewidzenia. Równocześnie dostrzegamy, że przedstawiona wraz z Projektem Ocena Skutków Regulacji nie uwzględnia analizy wpływu projektowanych przepisów na dostępność i zwłaszcza koszty usług dla konsumentów w wyniku wprowadzenia przedmiotowych przepisów.	**Wyjaśnienie** OSR został uzupełniony o analizę wpływu projektowanych przepisów na konsumentów. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka. Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od

				dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
109.	Federacja Konsumentów	Uwaga ogólna	Federacja Konsumentów popiera objęcie Krajowym System Cyberbezpieczeństwa podmiotów działających na rynku telekomunikacyjnym z uwagi na przedmiot ich działalności i zakres świadczonych usług, ale jednocześnie dostrzega, że inwestycje związane z realizacją takiej sieci, w tym jej modernizacją i remontem, są kosztowne i długotrwałe. Należy więc mieć na uwadze, że obowiązek zaprzestania w terminie 5 lat od oceny ryzyka korzystania ze sprzętu lub oprogramowania określonego dostawcy będzie skutkował w praktyce wymianą znacznej części funkcjonującej w Polsce infrastruktury, co	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra

			zapewne w naturalny sposób przełoży się na koszty świadczenia usług dla odbiorcy końcowego. Skutki tego typu rozwiązań mogą być podwójnie dotkliwe dla konsumenta, gdyż z jednej strony prawdopodobnie nastąpi wzrost cen usług, a z drugiej może dojść do pogorszenia ich jakości w okresie reorganizacji sieci i opóźnienia we wdrożeniu 5G z powodu konieczności przebudowy sieci LTE. W związku z przedstawionymi powyżej wątpliwościami Federacja Konsumentów stoi na stanowisku, że nowelizacja ustawy nie powinna powodować pogorszenie jakości i wzrost kosztów usług dla konsumentów. Z braku możliwości szczegółowej analizy Projektu ze względu na krótki czas trwania konsultacji, jednocześnie chcąc uniknąć wymienionych powyżej negatywnych konsekwencji, jako minimum wnosimy o rozważenie możliwości wydłużenia terminu na ewentualne wycofanie sprzętu albo oprogramowania dostawców objętych oceną wysokiego ryzyka o 5 lat, czyli łącznie do lat 10, co pozwoli na rozłożenie negatywnych skutków w czasie i mitygację wyżej wspomnianych ryzyk. Akceptowalne ceny usług świadczonych w oparciu o 5G są bowiem warunkiem koniecznym, aby korzyści z wdrożenia były wiodącym przekazem, w miejsce tego, o czym słyszymy i czytamy dzisiaj, a więc wspomnianej wyżej fali niepopartych żadnymi dowodami spekulacji o zagrożeniach. Jednocześnie, zwracamy uwagę, że globalny rynek technologii, opartej o dostawy sprzętu i oprogramowania przez międzynarodowe korporacje, może być trudny do przewidzenia w dłuższym horyzoncie czasowym. Nie można wykluczyć sytuacji, w której dostawca mający obecnie siedzibę na terenie państwa członkowskiego UE lub NATO przejdzie w wyniku zmian właścicielskich w ręce nowych właścicieli spoza tego obszaru, co mogłoby spowodować potrzebę kolejnej rewolucji w już	właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa

			zainstalowanym sprzęcie i oprogramowaniu. Stąd, oprócz kryteriów geograficznych lub geopolitycznych zasadnym wydaje się uwzględnienie w projekcie ustawy również innych kryteriów, takich jak certyfikacja bezpieczeństwa oparta o międzynarodowe standardy, promowanie otwartych interfejsów przy budowaniu sieci 5G oraz dywersyfikacja dostawców na poziomie sieci krajowej i poszczególnych sieci operatorskich na etapie budowy sieci. Deklarujemy wsparcie i dalszą współpracę w analizie i tworzeniu rozwiązań pro-konsumenckich.	spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
110.	Stowarzyszenie „Miasta w Internecie”	Uwaga ogólna	W naszej opinii dynamicznie rozwijające się sektory gospodarki, w tym sektor IT wymagają stałej modernizacji ram instytucjonalno-prawnych, z czego wynika konieczność prowadzenia dyskusji nad kierunkami regulacji obejmującej możliwie szeroką grupę podmiotów. Cyberbezpieczeństwo bowiem dotyczy zarówno wielkich podmiotów takich jak dostawców sprzętu czy operatów, ale także konsumentów, takich m.in. jak samorządy lokalne. Regulacje powinny być wyważone,	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji

			precyzyjne i niedyskryminujące, tak aby zapewnić ochronę interesów podmiotów o słabszej pozycji rynkowej. W tym kontekście na szczególną uwagę i analizę zasługuje projektowane rozwiązanie, w myśl którego szerokie kompetencje zyskuje Kolegium ds. Cyberbezpieczeństwa, będące – w świetle zapisów projektu ustawy - ciałem politycznym, nie zaś eksperckim. Kolegium zyskuje narzędzie do eliminowania z rynku podmiotów w oparciu o niesprecyzowane kryteria. Zakłada np. sporządzenie, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Ocena taka uwzględnić ma m.in. prawdopodobieństwo pozostawania przez dostawcę sprzętu lub oprogramowania pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, a ponadto uwzględnia: • • stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, • • prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka. Nie są to kryteria o charakterze technicznym, ale raczej natury uznaniowej, politycznej. W naszym przekonaniu regulacja winna zawierać kryteria odnoszące się do specyfikacji technicznej weryfikowalne merytorycznie. Dlatego też ocena powinna obejmować normy techniczne oraz właściwe certyfikacje. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania może określić ryzyko: na niezidentyfikowanym poziomie, niskie, umiarkowane lub wysokie. W tym ostatnim wypadku podmioty krajowego systemu cyberbezpieczeństwa nie mogą wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego	lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in.

			dostawcy sprzętu lub oprogramowania oraz zobowiązane są wycofać z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. Rozwiązanie to może pociągać za sobą – jak deklarują operatorzy i eksperci rynku telekomunikacyjnego – nieporównywalnie wysokie koszty dla rynku. Koszt zastąpienia urządzeń dominującego producenta nowymi oznaczać może nawet podwojenie pierwotnych kosztów wdrożenia. A zakaz wprowadzania sprzętu, oprogramowania lub usług, oraz obowiązek ich wycofania, de facto zmniejszy liczbę dostawców, a więc konkurencję na rynku. To z kolei może doprowadzić do obciążenia konsumentów, co nie pozostanie bez negatywnego wpływu na rozwój gospodarki w tym sektorze. Opóźnienia we wdrożeniu infrastruktury 5G mogą natomiast zagrozić zachowaniu ciągłości usług wobec wyczerpywania się zdolności rozwiązań 4G do zaspakajania rosnącego popytu. Warto również zwrócić uwagę na tryb i procedura postępowania odwoławczego od sporządzonej przez Kolegium oceny ryzyka. Wątpliwości budzi przede wszystkim rozwiązanie przewidujące, iż odwołanie wnosi się do Kolegium, zatem ten sam organ, który sporządzał ocenę ryzyka będzie orzekał o słuszności wydanego przez siebie rozstrzygnięcia. Dostawca sprzętu lub oprogramowania będzie mógł odwołać się w ciągu zaledwie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium będzie miało natomiast aż 2 miesiące od otrzymania odwołania na jego rozpatrzenie. Jest to okres relatywnie długi, jednak uwzględniający specyfikę tego sektora gospodarki. Natomiast przy obecnych zapisach projektu ustawy pozycja dostawcy w tym postępowaniu jest	prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie

			słaba. Zgodnie zaś z elementarnymi zasadami postępowania administracyjnego, stronie winno się zagwarantować możliwość czynnego udziału w postępowaniu. Ponadto czas rozpatrywania odwołania może negatywnie oddziaływać na kondycję dostawcy. Funkcjonowanie na rynku jak największej liczby dostawców sprzętu, oprogramowania i usług ma wielkie znaczenie dla tempa wdrażania w Polsce sieci 5G. Dlatego też zmiany powinny być ukierunkowane na stworzenia takich warunków, które zachęcałyby do wejścia na rynek także nowe podmioty, a klimat panujący na rynku pobudzał rozwój sektora. Bez wątpienia analizie należy także poddać kompetencje Pełnomocnika do wydawania ostrzeżeń i poleceń zabezpieczających. Ostrzeżenia wydają się być pozytywnym rozwiązaniem, w ramach którego zabezpieczane są interesy konsumentów. Dają bowiem słabszym rynkowo podmiotom wiedzę o ryzyku wiążącym się z pewnymi podmiotami. Natomiast rozwiązanie w postaci poleceń zabezpieczających wydawanych w oparciu o niejasne kryteria mogą doprowadzić do arbitralnego nakazywania przez Pełnomocnika zachowań takich jak np. zakaz połączeń z określonymi adresami IP lub nazwami URL. Ograniczenie liczby dostawców technologii 5G w połączeniu ze zmianami na rynku telekomunikacyjnym może doprowadzić do opóźnień we wdrożeniu sieci 5G w Polsce, a tym samym do zmniejszenia się konkurencyjności polskiej gospodarki oraz obniżenia jakości życia mieszkańców. Rozwój technologii 5G stymulować będzie z pewnością tworzenie nowych miejsc pracy oraz rozwój innych dziedzin cyfrowych powiązanych z korzystaniem z 5G. Warto również rozważyć kwestię regulacji obowiązków przedsiębiorców komunikacji elektronicznej wyłącznie na gruncie projektowanej ustawy – Prawo Komunikacji Elektronicznej.	mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało

			Projektowana ustawa ma kompleksowy charakter a przewidziane na jej gruncie kompetencje regulatora, jakim jest Prezes Urzędu Komunikacji Elektronicznej, wydają się w sposób efektywny zapewniać bezpieczeństwo infrastruktury telekomunikacyjnej.	także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

111.	Stowarzyszenie Inżynierów Telekomunikacji	Uwaga ogólna	Z przedstawionego projektu ustawy i zaproponowanych rozwiązań wynika, że zostały one przygotowane z pominięciem niektórych ważnych aspektów dotyczących budowy i funkcjonowania sieci telekomunikacyjnej, wykorzystywanej do świadczenia usług mobilnych. Wprowadzanie nowych regulacji, które będą rzutować na strukturę sieci i które będą determinować wybór producentów dostarczających poszczególne elementy tej sieci, musi uwzględniać ryzyko jakie niesie ze sobą tego typu regulacja – nie chodzi tu wyłącznie o ryzyko biznesowe właścicieli infrastruktury, ale przede wszystkim o ryzyko dotyczące zapewnienia stałej, jakościowo najlepszej pracy tych sieci i obsługi użytkowników końcowych. Zwracamy uwagę na fakt, że proponowany, nowy art. 66b w ustawie o cyberbezpieczeństwie, może mieć dalekosiężne skutki dla pracy całej sieci przedsiębiorcy telekomunikacyjnego, których w całości z góry nie można przewidzieć. Konstrukcja i architektura sieci telekomunikacyjnych to skomplikowany organizm, w którym nie można dowolnie i bez	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do
112.	Uniwersytet Jagielloński Collegium Medicum	Uwaga ogólna	Chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby: a) naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów; b) wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży; c) pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko; d) Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być

			oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania **a) Naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów.** Polski rynek jest obecnie jednym z najbardziej atrakcyjnych przestrzeni inwestycyjnych dla branży. Dzisiaj jesteśmy państwem, z którym handluje się w sposób wolny i przejrzysty, mamy przepisy gwarantujące inwestorom uczciwą konkurencję, wolny rynek i sprawiedliwe traktowanie. Proponowany kształt nowych przepisów znacząco wpływa na te atuty, które stanowią podstawowe przymioty w każdym demokratycznym państwie. Zagraniczny kapitał jest bardzo wrażliwy na tego rodzaju regulacje. Jesteśmy pewni, że w przypadku wprowadzenia przepisów w proponowanym kształcie przełożą się one na rozwój zarówno polskiego przemysłu, sektora usług ale także na życie polskich obywateli. **b) Wpływanie przez Kolegium w sposób niejasny oraz bez szczegółowych wytycznych (technicznych) na podmioty w branży.** W myśl projektu Kolegium dostałoby bardzo szerokie, niejasne, niekontrolowane przez żaden zewnętrzny podmiot uprawnienia do wpływania na konkretnego dostawcę. To z kolei w dalszej kolejności przekłada się na inne podmioty gospodarcze, a na samym końcu na konsumenta. Postępowanie które pozbawia prawa do możliwości składania wyjaśnień wydaje się wysoce niesprawiedliwe. Natomiast pozbawienie możliwości odwołania (w niektórych przypadkach) zgodnie z przepisami KPA wyraźnie narusza porządek prawny oraz zasady równego traktowania zagwarantowane w Konstytucji. Proponowane przepisy stworzą potencjalne ryzyko wpływania w sposób	wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu

			nieuczciwy i niezgodny z prawem na podejmujących decyzję w sprawie oceny. Powstanie szczegółowych wytycznych – jasnych, obiektywnych kryteriów oceny powinno zminimalizować to ryzyko. **c)pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko.** Każdy podmiot – zarówno w przypadku oceny określającej wysokie ryzyko, jak i ocen określających średnie i niskie ryzyko - powinien mieć takie same możliwości odwoławcze od oceny. Blokowanie możliwości odwoławczych niektórych z nich wpływa przede wszystkim na równość podmiotów względem innych. Każdy zasługuje na możliwość odwołania od oceny, która w założeniu nowych przepisów ma się odbywać bez udziału zainteresowanego podmiotu. Odwołanie powinno zawieszać postępowanie do czasu wydania prawomocnego wyroku w sprawie przez sąd powszechny w myśl przepisów KPA. Taki stan rzeczy byłby w sposób oczywisty najbardziej sprawiedliwy. **d)Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania.** Pięcioletni termin wycofania z rynku jest bardzo krótkim terminem na wycofanie z rynku całego sprzętu, oprogramowania i usługi z rynku. Proponujemy termin 10–cio letni, który jest dużo bardziej adekwatny do sytuacji. Należy pamiętać o tym, że operatorzy poniosą również gigantyczne koszty związane wprost z nowymi przepisami i w żaden sposób przez siebie nie zawinione. Dlatego też rząd powinien	Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			wprowadzić rekompensaty dla tych podmiotów, które takie koszty będą musiały ponieść. Oczywistym jest, że każdy podmiot który poniesie takie straty będzie szukał możliwości ich odrobienia. To z kolei wprost przełoży się na ceny usług dla końcowego odbiorcy, czyli obywatela. Sam termin 5–cio letni jest tak krótki, że może również wpłynąć na stabilność sieci, która będzie miała również szeroko idące konsekwencje. W związku ze wszystkimi powyżej przytoczonymi argumentami, będziemy ogromnie wdzięczni za uwzględnienie przedstawionych propozycji zmian w treści projektowanych przepisów. Jedynie sprawiedliwe, przejrzyste i obiektywne mechanizmy ustawowe dadzą pozytywny skutek zarówno dla przedsiębiorców, jak i dla obywateli. Wierzymy, że zagadnienia na które zwracamy uwagę będą przyczyną do poddania ponownej analizie oraz weryfikacji tych projektowanych przepisów, które naszym zdaniem mogą wpływać negatywnie na sposób funkcjonowania ustawy w praktyce.	
113.	Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo Sektorowa Rada ds. Kompetencji	Uwaga ogólna	Rolą Sektorowej Rady ds. kompetencji Telekomunikacja i Cyberbezpieczeństwo jest przede wszystkim działanie na styku edukacji i praktyki w obu wskazanych dziedzinach. Obejmuje to m. in. rekomendowanie rozwiązań legislacyjnych w obszarze edukacji i dostosowanie do potrzeb rynku pracy oraz formułowanie rekomendacji dotyczących zapotrzebowania na kompetencje w danym sektorze. Z powyższych względów, w kręgu zainteresowania Rady są wszelkie rozwiązania legislacyjne, które mają wpływ na kształt rynku pracy oraz potrzeby edukacyjne w dziedzinie telekomunikacji i cyberbezpieczeństwa. Sektorowa Rada do spraw Kompetencji Telekomunikacja i Cyberbezpieczeństwo uczestniczy w konsultacjach i wypracowuje	**Uwaga częściowo uwzględniona** Definicje cyberbezpieczeństwa i bezpieczeństwa sieci i systemów informatycznych zostaną poprawione.

	Telekomunikacja i Cyberbezpieczeństwo		rekomendacje zmian regulacji m.in. organizując konferencje naukowe ekspertów z administracji, biznesu i edukacji. Debaty skupiają się na problemach kompetencji w ich podwójnym znaczeniu: „wiedzy i umiejętności" oraz „uprawnień i obowiązków" a także na elementach „siatki pojęciowej" w regulacjach, które dotyczą obu dziedzin. Rada była głównym organizatorem konferencji „Leksykon cyberbezpieczeństwa" (31.07.2020), „Działalność w zakresie cyberbezpieczeństwa. Aspekty prawne, organizacyjne i techniczne", 7.08.2020 oraz „Potrzeby kompetencyjne w zakresie cyberbezpieczeństwa i łączności elektronicznej w świetle planowanych zmian w przepisach" (2.10.2020), podczas których omawiano m. in. kwestie związane z kwalifikacjami i kompetencjami w związku z projektem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Rezultatem konferencji są poniższe uwagi i propozycje do ww. projektu. Problemy definicyjne W pierwszej kolejności, Rada pragnie zwrócić uwagę na problemy związane z definiowaniem cyberbezpieczeństwa w różnych aktach prawnych. 2 W ustawie o krajowym systemie cyberbezpieczeństwa (UKSC) cyberbezpieczeństwo jest definiowane jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy (art. 2 pkt 4). Definicja ta jest zbliżona do definicji „bezpieczeństwa sieci i systemów informatycznych" zawartej w art. 4 ust. 2 Dyrektywy NIS, które „oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające	

			dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne". Pomimo, że UKSC to implementacja Dyrektywy NIS to jednak powyższe, zasadnicze pojęcia są określane i definiowane w różny sposób. W akcie o cyberbezpieczeństwie (Rozporządzenie 2019/881), „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami (art. 2 ust. 1). „Cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych [information system], użytkowników takich systemów oraz innych osób. Z kolei projekcie nowelizacji UKSC z 7.09.2020 r. proponuje się nowy termin – „bezpieczeństwo sieci i usług" i definiuje się go jako zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług, b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy [art. 2 pkt 8f projektu]. Jednocześnie, pozostawia się dotychczasową definicję cyberbezpieczeństwa. Rada zwraca uwagę na niejednoznaczność terminu „cyberbezpieczeństwo". Termin ten jest również wadliwie tłumaczony z języka angielskiego, często jako „bezpieczeństwo	

			cybernetyczne”, i „bezpieczeństwo systemów informatycznych” – co, zdaniem Rady wymaga korekty. Wymagałoby pogłębionej analizy ustalenie czy i w jaki sposób do różnic pomiędzy polską ustawą a unijnym rozporządzeniem odnoszą się reguły kolizyjne, ponieważ przyjęcie poglądu o krzyżowaniu się zakresów ustawy o ksc i rozporządzenia UE 2019/881 pociągałoby za sobą konieczność uchylenia dotychczasowej definicji cyberbezpieczeństwa. Niewątpliwie potrzebne jest wdrożenie procedury corrigendum nieodpowiednich spolszczeń w Dz. Urz. UE Pl. [m.in. cybersecurity jako „bezpieczeństwa cybernetycznego” zamiast cyberbezpieczeństwa, a information systems jako systemów informatycznych zamiast systemów informacyjnych] a także zestawienie i adekwatnie objaśnienie innych elementów leksykonu cyberbezpieczeństwa. Rada rekomenduje uzgodnienie znaczenia terminu cyberbezpieczeństwo jako zbiorczego określenia o rosnącej wadze w różnych kontekstach, dla uzyskania spójności wielopoziomowej regulacji oraz zestawienie i adekwatne objaśnienie innych elementów siatki pojęciowej. Ułatwi to jasne określenie uprawnień i obowiązków podmiotów krajowego systemu cyberbezpieczeństwa. Jednocześnie Rada zwraca uwagę na brak cyberbezpieczeństwa w klasyfikacjach rodzajów działalności. Dotyczy to zarówno Międzynarodowej Standardowej Klasyfikacji Rodzajów Działalności (ISIC), Statystycznej Klasyfikacji Rodzajów Działalności Gospodarczej w Unii Europejskiej (NACE), jak i Polskiej Klasyfikacji Działalności (PKD). Działalność ma miejsce wówczas, gdy czynniki takie jak: wyposażenie, siła robocza, technologia produkcji, sieci informacyjne lub produkty są powiązane w celu wytworzenia określonego wyrobu lub	

			wykonania usługi. Działalność charakteryzowana jest przez produkty wejściowe (wyroby lub usługi), proces technologiczny oraz przez produkty wyjściowe. Wyróżnia się działalność: przeważającą, drugorzędną i pomocniczą. Cyberbezpieczeństwo nie jest wyodrębniane jako rodzaj działalności. Klasyfikacja PKD 2007 stosowana jest do podmiotów gospodarczych dla potrzeb: Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG), Krajowego Rejestru Sądowego (KRS), Krajowego Urzędowego Rejestru Podmiotów Gospodarki Narodowej (REGON), Krajowej Ewidencji Podatników (KEP). Niewyodrębnienie w PKD cyberbezpieczeństwa utrudnia realizację zadań publicznych wyznaczonych podmiotom krajowego systemu cyberbezpieczeństwa i rozwój działalności gospodarczej. Uwaga powyższa dotyczy wprawdzie tylko pośrednio projektu nowelizacji UKSC, ale Rada stoi na stanowisku, że minister właściwy do spraw informatyzacji powinien zainicjować kompleksowe uporządkowanie kwestii związanych z terminologią oraz klasyfikacją działalności związaną z tematyką cyberbezpieczeństwa.	
114.	Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo	Uwaga ogólna	*Kwalifikacje i umiejętności związane z cyberbezpieczeństwem* Rada zwraca uwagę, że w UKSC brak wyraźnych wymogów w zakresie kwalifikacji, wiedzy i umiejętności. Art. 14 stanowi, że operator usługi kluczowej w celu realizacji niektórych zadań powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (po nowelizacji ma to być SOC) Według § 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z 4.12.2019. podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest obowiązany w zakresie realizowanych obowiązków, o których mowa w art. 8 pkt 4 i 6, art. 11 ust. 1 pkt	**Uwaga nieuwzględniona** Kwestie związane z zobowiązaniem podmiotów krajowego systemu cyberbezpieczeństwa do podnoszenia kwalifikacji kadr wykracza poza zakres przedmiotowy nowelizacji. Operatorzy usług kluczowych, jak słusznie zauważył autor opinii mają obowiązek zapewnić dysponowanie odpowiednio wykwalifikowanym personelem.

			1–5, art. 12 i art. 13 UKSC, dysponować personelem posiadającym umiejętności szczegółowo określone w punktach a-d. Pojawiają się wątpliwości dotyczące dokumentowania faktu dysponowania odpowiednim personelem [czy ma on posiadać stosowne certyfikaty, szkolenia, itp.] oraz braku wymogów w odniesieniu do personelu wewnętrznych struktur. 4 Rada zdaje sobie sprawę z różnicy w podejściu do wymogów kwalifikacyjnych w sferze prywatnej i publicznej. Sfera prywatna jest z jednej strony często lepiej motywowana do podnoszenia kwalifikacji, z drugiej – wszelkie ustawowe wymogi tego typu traktuje jako dodatkowe, kosztowne obowiązki nakładane na sektor gospodarczy. W sferze publicznej z kolei, brak ustawowych wymogów co do posiadania określonych kwalifikacji powoduje niechęć do wydawania publicznych pieniędzy na te cele, a tym samym brak motywacji do podnoszenia poziomu umiejętności. W raporcie NIK z 2019 r. dotyczącym zapewniania bezpieczeństwa e-usług oceniono krytycznie 70% badanych podmiotów publicznych. Pewnym wzorem mogą być przepisy dotyczące ochrony danych osobowych dotyczące inspektorów ochrony danych. W art. 37 ust. 5 RODO stanowi, że Inspektor ochrony danych wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk ochrony danych oraz umiejętności wypełniania swoich zadań. Do szkolenia innych osób upoważnianych do przetwarzania, mobilizują administratorów zasada rozliczalności i dolegliwe sankcje. Rada stoi na stanowisku, że efektywność nowych regulacji cyberbezpieczeństwa może być ograniczona ze względu na niewystarczający potencjał kadrowy, zwłaszcza SOC i CSIRT	

			sektorowych. W związku z tym Rada rekomenduje, aby w UKSC umieścić przepisy skłaniające do podnoszenia kwalifikacji.	
115.	Polskie Towarzystwo Informatyczne	Uwaga ogólna	Z zadowoleniem witamy projekt ustawy o zmianie ustawy o Krajowym Systemie Cyberbezpieczeństwa, który zgodnie z uzasadnieniem, ma zrealizować to co już wielokrotnie nasza organizacja podnosiła w toku prac nad innymi projektami aktów prawnych tj. konieczność dostosowywania RP do zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G UE (zwanego dalej "5G Toolbox") w opracowaniu którego Polska brała udział, i w którym zawarto środki na poziomie strategicznym i technicznym oraz wskazano działania wspierające stosowanie tych środków dla ograniczenia ryzyk cyberbezpieczeństwa europejskich sieci 5G. Nie jest prawdziwa teza że ustawa ta jest wymierzona przeciwko jakiejkolwiek firmie na świecie, co sugeruje prasa choć nie oznacza to wcale ze nie może być użyta przeciwko jakiejkolwiek firmie rodem z Chin czy Rosji lub Korei Północnej, z której pochodzą pierwsze podmioty objęte sankcjami UE za cyberataki, choć jak słusznie zauważa p. Izabela Albrycht w https://ik.org.pl/publikacje/5g-made-by-america/: „Całkowicie swoje sieci telekomunikacyjne na komponenty z ChRL zamknęły Australia, Nowa Zelandia i Japonia, a zapowiedziała – Wielka Brytania. Wiele krajów podpisało natomiast z USA deklaracje polityczne wyrażające wolę współpracy w zakresie zapewnienia bezpieczeństwa sieci 5G w tym Polska, Łotwa, Rumunia, Polska, Czechy, Estonia, Słowenia". W tej ogólnoświatowej debacie na pewno firmie Huawei nie służy postawa macierzystego państwa, oskarżanego o cyberataki na szpitale w Unii Europejskiej w okresie pandemii COVID 19, co spotkało się ze zdecydowanym sprzeciwem Komisji Europejskiej:	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania

			https://www.cyberdefence24.pl/szefowa-ke-oskarza-chiny-o-ataki-na-szpitale Projektowana nowelizacja wprowadza kolejne zmiany systemowe, które pozwolą zwiększyć poziom bezpieczeństwa w sektorze komunikacji elektronicznej i telekomunikacji. Uważamy za słuszny postulat włączenia telekomunikacji do ogólnego systemu prawnego cyberbezpieczeństwa przy ograniczaniu obowiązków informacyjnych, które i tak są liczne na tym bardzo dziś regulowanym rynku. Nie da się jednak współcześnie tworzyć rozwiązań systemowych w skali państw wyłączając z niego telekomunikację. Opiniowany projekt ustawy projektuje narzędzia do realizacji wyżej wymienionych celów zwłaszcza w nowo tworzonych art. 66 „a”- 67 „c” które przyznają nowe szerokie kompetencje Kolegium ds. Cyberbezpieczeństwa oraz Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa. Możliwość przeprowadzenia oceny ryzyka przez Kolegium ds. Cyberbezpieczeństwa oraz ostrzeżenia i polecenia wydawane przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa, z wiążącymi skutkami , co proponuje ustawa , to absolutnie krok w dobrym kierunku. Zwracamy uwagę że ,ryzyka opisane w 5G Toolbox są szersze i bardziej różnorodne np „R4. Dependency on a single supplier”. W Polsce że sprzęt i oprogramowanie od jednego dostawcy stanowią większość całej infrastruktury LTE (4G) i 5G a w przypadku niektórych operatorów jest to ponad 80% ich zasobów . Jest to zjawisko głęboko niepożądane, gdyż problem z jednym tylko dostawcą stawia pod znakiem zapytania cyberbezpieczeństwo całego kraju. Na przykład w przypadku zakłócenia łańcucha dostaw tak z powodów np. pandemii jak i ew. regionalnych czy światowych.	poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący

			Zgodnie z 5GToolbox środkami zaradczymi (Measures) niwelującymi to ryzyko są: - Dywersyfikacja dostawców. - Zrównoważony i zróżnicowany łańcuch dostaw i wartości 5G. Skuteczność tych środków zaradczych w opracowanym 5GToolbox określono jako „bardzo wysoką" (Very High) i są to jedyne środki zaradcze. Ustawa powinna wprowadzać zarówno środki dywersyfikacji ze względu na kraje pochodzenia jak i kategorie produktów i wykorzystywać technologie otwarte takie jak np. oparte na OPEN RAN. Zwracamy uwagę że należy zmienić drobną nieścisłość w obecnie obowiązującej ustawie która nakazuje by Pełnomocnikiem rządu ds. cyberbezpieczeństwa była osoba w randze podsekretarza lub sekretarza stanu (art.61 ust.3 obecnie obowiązującej ustawy). Nie obejmuje to Ministra, a obecnie Pan Minister Marek Zagórski pełni tę ważną rolę. Nie można wykluczyć iż w przyszłości tę funkcję także będzie pełnił Minister. Można naprawić przy okazji nowelizacji tę niezręczność, która może prowadzić jednak do podważania decyzji pełnomocnika. W ocenie PTI projektowana nowelizacja wprowadza kolejne poziom zmiany systemowe, które pozwolą zwiększyć bezpieczeństwa w sektorze komunikacji elektronicznej i telekomunikacji a niedoskonałości projektu można usunąć na kolejnych etapach prac legislacyjnych.	w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
116.	ISSA Polska	Uwaga ogólna	Naszym celem statutowym jest m.in. dostarczanie wiedzy związanej z tematyką szeroko pojętego bezpieczeństwa, jak również edukacja i promowanie standardów oraz opiniowanie wydarzeń i rozwiązań z zakresu cyberbezpieczeństwa uznaliśmy za istotne wskazanie najistotniejszych problemów związanych z	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy

			projektowanymi rozwiązaniami. Projekt zmian w naszej ocenie jest niezwykle potrzebny, jednakże wprowadza pewne dyskusyjne zagadnienia. Niektóre zawarte w projekcie zapisy (w tym, co najmniej Art. 66 i 66a) w naszej ocenie wykraczają poza merytorykę zagrożeń cyberbezpieczeństwa w perspektywie technicznej i dziedzinowo uznawanej za merytoryczną.	Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji

				na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
117.	ISSA Polska	Uwaga ogólna	**Definicje**	**Wyjaśnienie**

			Wprowadzając do ustawy o Krajowym Systemie Cyberbezpieczeństwa Art. 8f), projekt wprowadza kolejną definicję z zakresu bezpieczeństwa a mianowicie „bezpieczeństwo sieci i usług". Uważamy, że nowelizację warto wykorzystać do uporządkowania istniejących definicji dotyczących szeroko pojętego bezpieczeństwa telekomunikacyjnego, a nie wprowadzania kolejnej definicji - szczególnie, że obecna propozycja rodzi pytania czym są te „sieci" oraz „usługi", których bezpieczeństwo należy zapewnić. Doprecyzowania wymaga definicja incydentu telekomunikacyjnego w Art. 8b). W większych firmach telekomunikacyjnych każdego dnia rejestrowane są nawet miliony zdarzeń typu skanowanie portów atak DDOS. Teoretycznie każdy z nich „może" - np. w sposób pośredni doprowadzić do obniżenia jakości usługi komunikacji elektronicznej. W tym momencie brak jest jakichkolwiek dalszych informacji w tym zakresie. Dodatkowo przekazywanie zgodnie z art 20b pkt 2 (oraz 20c ust 3 pkt 3) informacji o incydentach w takiej ilości powinno być wykonywane jedynie w sposób automatyczny a systemy ku temu potrzebne powinny być dostarczone przez CSIRTy.	Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.

118.	ISSA Polska	Uwaga ogólna	**Zadania SOC** Zespoły SOC funkcjonują na polskim rynku od ponad 15 lat – działają zatem w dobrze opisanej roli w organizacjach, jak również w konkretnej rzeczywistości rynkowej, zarówno w zakresie usług zlecanych, jak i dostarczanych klientom. W związku z powyższym proponujemy uwzględnienie dotychczasowych doświadczeń w dotyczących zespołów SOC propozycjach zapisów: Częstym modelem realizacji SOC jest wariant, w którym jedynie część zadań SOC jest realizowana przez podmiot zewnętrzny – brzmienie proponowanego Art. 14 ust 2) do Ustawy o Krajowym Systemie Cyberbezpieczeństwa powinno zapewniać taką możliwość.	**Wyjaśnienie** Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.
119.	ISSA Polska	Uwaga ogólna	**Postulat rzetelnych konsultacji społecznych** Ponieważ nowe regulacje, będą oddziaływały na szeroki zakres odbiorców, dlatego też Ministerstwo Cyfryzacji powinno przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców, organizacje konsumentów, instytucje odpowiedzialne za ochronę konkurencji i konsumenta, Radę Dialogu Społecznego. 2. Postulat zorganizowania konferencji uzgodnieniowej oraz wcześniejszego wysłuchania publicznego Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy.	**Wyjaśnienie** Umożliwiono wypowiedzenie się wszystkim interesariuszom w trakcie konsultacji publicznych.

			Z uwagi na szeroki wpływ projektowanych zmian na kwestie dotykające wszystkich obywateli, uznajemy także za celowe przeprowadzenie wysłuchania publicznego, już na etapie prac rządowych. 3. Postulat dokonania notyfikacji projektu Zwracamy uwagę na równoległe prace Komisji Europejskiej w zakresie rewizji dyrektywy NIS1, która jak dotąd jest głównym źródłem regulacji z zakresu cyberbezpieczeństwa. Tym samym sugerowalibyśmy, aby zmiany naszego prawa krajowego nie wyprzedzały regulacji UE, tym bardziej jeśli kierunek obranych zmian może pójść w przeciwnym kierunku niż regulacje europejskie. 4. Postulowane kluczowe zmiany projektu Przyjęta w projekcie nowelizacji koncepcja powstania CSIRT Telko i SOC'ów jest godna poparcia w zakresie, w jakim służy zapewnieniu koordynacji działań i wymiany informacji podmiotami należącymi do KSC a dostawcami sieci i usług komunikacji elektronicznej. Zwracamy przy tym uwagę, że skuteczne wymiana informacji o incydentach wymaga nie tworzenia osobnych organizacji a zniesienia prawnych ograniczeń dotyczących dzielenia się informacjami, które mogą być klasyfikowane jako tajemnica w firmach telekomunikacyjnych oraz finansach i bankowości. Proponujemy więc przede wszystkim stworzyć mechanizmy, które pozwolą tym podmiotom dzielić się informacjami o incydentach i oszustwach – również tych jedynie podejrzewanych.	

			Uważamy również, że implementacja dyrektywy NIS poprzez przyjęcie i uchwalenie ustawy o KSC na terenie RP powinna w sposób bardziej świadomy rzutować na istotność ochrony kluczowych elementów infrastruktury w sieciach industrialnych, przemysłowych – OT. Istotność zagrożeń dla całej infrastruktury krytycznej od strony sieci przemysłowych OT podkreśla fakt złożoności infrastruktury sieci IT, ICT oraz OT oraz ich wzajemnej korelacji, zależności fizyczno -logicznych od siebie i wymienianych danych. Naszym zdaniem rekomendacje i wymagania w obszarze urządzeń automatyki przemysłowej oraz urządzeń aktywnych infrastruktury powinny nawiązywać do szeregu dobrych praktyk i uznanych standardów branżowych IEC62443, NIST SP 800-82, wytycznych Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) przedstawionych np. w publikacji "Communication network dependencies for ICS-SCADA Systems".	
120.	ISSA Polska	Uwaga ogólna	Całość zagadnienia powinna zostać opracowana w odrębnej sektorowej i branżowej publikacji zawierającej wymagania i wytyczne wyczerpującą tematykę: - metodyki przeprowadzania audytów systemów ICS, sieci przemysłowych oraz zasobów bezpośrednio sklasyfikowanych jako urządzenia czynne i aktywne pod kątem wytwarzania dóbr, zarządzania i nadzorowania procesem produkcyjnym, - szacowania ryzyka w oparciu przeprowadzony audyt z opracowaniem metod zmniejszenia ryzyka utraty ciągłości produkcyjnej, podania rekomendacji związanych z zarządzaniem ryzykiem,	**Wyjaśnienie** Dziękujemy ISSA Polska za przedstawioną propozycję. Mając na uwadze naszą dotychczasową współpracę z ekspertami z ISSA Polska m.in. przy przygotowaniu szablonu sprawozdania z audytu bezpieczeństwa u operatorów usług kluczowych DC KPRM wyraża gotowość do kontynuowania współpracy.

			▯ sposobu określenia istniejących podatności urządzeń sieci produkcyjnej i systemów automatyki przemysłowej ICS/OT, urządzeń sieciowych, ▯ określenia wytycznych służących zwiększeniu niezawodności systemów produkcyjnych zmniejszających potencjalne następstwa w przerwaniu ciągłości świadczonych usług komunikacji tychże urządzeń ▯ określeniu metod prewencji poprzez ciągłe monitorowanie zasobów sieciowych oraz urządzeń automatyki przemysłowej, komunikacji tychże urządzeń z uwzględnieniem specyfiki protokołów przemysłowych ▯ nadaniu wytycznych sektorowych służących zbudowaniu wielowarstwowego systemu ochrony kluczowych zasobów, urządzeń, instalacji i systemów wytwórczych. ▯ wytycznych do projektantów co do projektowania systemów bezpieczeństwa systemów komputerowych dla otoczenia OT/ICS oraz komponentów systemów sterowania, doboru elementów systemu Jednocześnie jako ISSA Polska pozostajemy do dyspozycji Ministerstwa Cyfryzacji w zakresie wsparcia eksperckiego i wiedzy związanej z tematyką szeroko pojętego bezpieczeństwa systemów informacyjnych.	
121.	ISSA Polska	Uwaga ogólna	Proponujemy dodanie proaktywnej funkcji CSIRT sektorowego w zakresie obowiązku wysyłania cotygodniowej uproszczonej informacji o aktualnym stanie dynamicznej analizy ryzyka, skali zarejestrowanych incydentów z ich priorytetami, trendem dla wszystkich zarejestrowanych uczestników systemu cyberbezpieczeństwa. W związku tym proponujemy dodanie ust. 1.c w brzmieniu:	**Wyjaśnienie** CSIRT sektorowy zapewnia wymianę informacji o podatnościach i zagrożeniach w sektorze. Jest to wskazane w art. 44 w ust 1 pkt 3 i 4.

			1.c CSIRT sektorowy zapewnia co tygodniowy raport sytuacyjny w zakresie cyberbezpieczeństwa sektora, zawierający co najmniej informacje o: 1) Poziomie stanu dynamicznej analizy ryzyka dla sektora; 2) ilości otrzymanych incydentów od uczestników sektora; 3) Istotnych zidentyfikowanych podatnościach	
122.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Bez wątpienia istotnym wyzwaniem pozostaje zapewnienie cyberbezpieczeństwa. Wraz ze wzrostem znaczenia sieci telekomunikacyjnych i wykorzystywaniem jej do realizacji coraz szerszego katalogu usług publicznych, niekiedy krytycznych, wprowadzenie regulacji minimalizujących ryzyko występowania incydentów zakłócających świadczenie usług wydaje się być oczywiste. Przedstawiony projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa rozumiemy jako próbę odpowiedzi na to wyzwanie, sformułowaną po dwuletnim okresie obowiązywania zmienianego aktu. W tym sensie zrozumiałe wydaje się być zaproponowanie przepisów wprowadzających centra wymiany informacji między podmiotami krajowego systemu cyberbezpieczeństwa oraz wprowadzających obowiązek ustanawiania sektorowych CSIRT (zamiast dotychczasowego trybu fakultatywnego). Niemniej jednak niektóre z przepisów budzą kontrowersje. Dotyczy to przede wszystkim przepisów zaproponowanych w odniesieniu do możliwości weryfikowania dostawców sprzętu lub oprogramowania. Uwzględnione w projekcie regulacje zakładają, że możliwe będzie wyłączenie podmiotów zidentyfikowanych jako źródło zagrożenia z systemu zamówień publicznych w Polsce, czy zobowiązanie podmiotów krajowego systemu cyberbezpieczeństwa do ograniczenia korzystania z produktów, oprogramowania i usług takich dostawców. Tego rodzaju oceny	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			ryzyka może, zgodnie z art. 66a projektu, dokonać Kolegium ds. Cyberbezpieczeństwa. Jednym z bardziej wrażliwych elementów sporządzania oceny w projekcie ustawy, są kryteria brane pod uwagę w toku procesu. Zgodnie z projektem, przy sporządzaniu oceny przeprowadzać ma się analizy dotyczące w szczególności m.in.: - zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania; - prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza UE bądź NATO (analiza ta ma uwzględniać m.in. stopień i rodzaj powiązań między dostawcą a tym państwem, prawodawstwo państwa w zakresie ochrony praw obywatelskich i praw człowieka, czy strukturę własnościową dostawcy). Przedstawione kryteria mają charakter nieostry i podmiotowy, a nie przedmiotowy, co umożliwia uznanie takiego samego sprzętu lub oprogramowania za stanowiące zagrożenie albo nie, w zależności wyłącznie od jego dostawcy. Kryteria (*de facto*) doboru dostawców sprzętu i oprogramowania uznajemy zatem za przejaw chęci pozostawienia otwartego pola gry i możliwości podjęcia każdej decyzji, w zależności od rozwoju sytuacji geopolitycznej, jak i dynamiki wydarzeń w innych państwach. W tym sensie – polityki międzynarodowej, a niekoniecznie bezpośredniego interesu gospodarczego – przyjęte przez projektodawcę podejście pozwala na dostosowanie aktywności Polski do uwarunkowań międzynarodowych i podjęcie dowolnej decyzji. Należy jednak pamiętać o konieczności zapewnienia pewnej przewidywalności otoczenia regulacyjnego dla działających w Polsce przedsiębiorców	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

			Zwracamy również uwagę na specyfikę niektórych sektorów – sparaliżowanie dostępu do produktów niektórych producentów urządzeń elektronicznych może spowodować np. istotne trudności w zakresie technicznych możliwości produkowania leków.	musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
123.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Ponadto, pragniemy poddać pod rozwagę ustawodawcy możliwość zastosowania uzupełniających rozwiązań w zakresie cyberbezpieczeństwa, które zminimalizują negatywne skutki finansowe dla przedsiębiorców telekomunikacyjnych, przy równoczesnym zapewnieniu najwyższych standardów cyberbezpieczeństwa. W szczególności zwracamy uwagę na zbyt krótki przewidziany 5-cio letni okres na eliminację sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka. Użytkownicy tego sprzętu lub oprogramowania nabywali go w dobrej wierze i z założeniem pełnego wykorzystania biznesowego przez okres zdecydowanie dłuższy, niż 5 lat. Realny czas na amortyzację sprzętu wykorzystywanego w sieciach telekomunikacyjnych stanowi minimum 7-8 lat. W tym okresie zasadne byłoby również dopuszczenie dokonywania dalszych niezbędnych zakupów i wdrożeń, w tym np. aktualizacji oprogramowania kluczowego dla bezpieczeństwa. Dodatkowo, zwracamy uwagę na ewentualną możliwość uzależnienia zasad eliminacji sprzętu dostawcy określonego jako dostawcy wysokiego ryzyka od poziomu wrażliwości danego obszaru dla krajowego systemu cyberbezpieczeństwa, na którym sprzęt jest wykorzystywany. Ustawodawca może wskazać regiony, w których	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za

			należy zastosować najbardziej rygorystyczne podejście ze względu na ich krytyczną i strategiczną rolę w krajowym systemie cyberbezpieczeństwa.	wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę

				wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
124.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Istotnym wątkiem jest również kwestia rozszerzenia zakresu ustawy na podmioty spoza tych uznanych za operatora usługi kluczowej. Należy podkreślić, że autonomiczne zarządzanie bezpieczeństwem przez te podmioty doprowadziło do zbudowania złożonych i wzajemnie powiązanych systemów zabezpieczeń, w trybie ciągłym analizowanych pod kątem skuteczności i aktualności. Omawiana regulacja może spowodować, że funkcjonalność tych systemów zostanie ograniczona z uwagi na komunikaty bezpieczeństwa ogłaszane przez organy administracji. Tym samym, podmioty gospodarcze poniosą niejako podwójne koszty.	**Wyjaśnienie** Katalog podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa jest bardzo szeroki i wskazany w art. 4.
125.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Należy ponadto zwrócić uwagę na regulacje dot. ostrzeżeń oraz poleceń zabezpieczających, wydawanych przez Pełnomocnika ds. Cyberbezpieczeństwa. Zarówno ostrzeżenia jak i polecenia zabezpieczające w swojej treści wskazują określone zachowanie, które należy podjąć i które ma w swoim założeniu zmniejszyć ryzyko incydentu. Jednym ze wskazanych w ustawie zachowań zmniejszających ryzyko incydentu jest nakaz wprowadzenia	**Wyjaśnienie** Projektowane przepisy dot. ostrzeżenia i polecenia zabezpieczającego nie mają na celu ograniczenie wolności słowa i dostępu do internetu. . Ich stosowanie jest ograniczone tylko do niektórych grup podmiotów z

			reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL (art. 67b ust. 3 pkt 7 uksc), czyli działanie polegające na ograniczaniu (blokowaniu) dostępu do niektórych stron lub usług. Zgodnie z regulacją Rozporządzenia EU dot. otwartego internetu, użytkownicy końcowi mają prawo do uzyskania za pomocą internetu dostępu do informacji i treści oraz do ich rozpowszechniania, a także do korzystania z wybranych aplikacji i usług oraz ich udostępniania, jak również do korzystania z wybranych urządzeń końcowych, niezależnie od lokalizacji użytkownika końcowego lub dostawcy usług czy też od lokalizacji, miejsca pochodzenia lub miejsca docelowego informacji, treści lub usługi. Zasada otwartego internetu może podlegać ograniczeniu tylko wyjątkowo i przy zachowaniu proporcjonalnych środków – należałoby zatem uzupełnić projekt ustawy o regulacje gwarantujące wyjątkowość i proporcjonalność radykalnego środka, jakim jest zablokowanie dostępu do niektórych stron lub usług	sektorów gospodarki kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa m.in. do operatorów usług kluczowych, administracji publicznej, czy przedsiębiorców telekomunikacyjnych. Co więcej, środki te mogą być aktywowane w sytuacji zagrażającej wystąpieniu incydentu krytycznego7 (ostrzeżenie) lub w trakcie jego trwania, w związku z potrzebą zapewnienia koordynacji i odpowiednio szybkiej reakcji na zażeganie sytuacji kryzysowej wywołanej cyberatakiem (polecenie zabezpieczające).
126.	Związek Przedsiębiorców i Pracodawców	Uwaga ogólna	Niezależnie od potrzeby ujednolicenia i skoordynowania prawodawstwa w zakresie obowiązków ciążących na przedsiębiorcach komunikacji elektronicznej, ważne jest aby na etapie projektowania aktów wykonawczych pamiętać o konieczności zachowania zasady proporcjonalności i nieobciążania przedsiębiorców dodatkowymi obowiązkami w stopniu wyższym, niż jest to konieczne dla zrealizowania celów ustawy. Jednocześnie, wszelkie mechanizmy ocenne należy umocować w istniejących już przepisach, takich jak te zawarte w ustawie Prawo przedsiębiorców oraz ustawie Kodeks postępowania administracyjnego. Gwarantują one przejrzystość procedur i ich zasad, umożliwiają udział dostawcy w postępowaniu oraz zapewniają niedyskryminującą procedurę odwoławczą.	**Wyjaśnienie** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.

			Mając na uwadze wszelkie powyższe aspekty, postulujemy o dalsze prace nad przedstawionym projektem ustawy i kontynuowanie szerokich konsultacji tego aktu, tak aby każdy zainteresowany podmiot miał możliwość skutecznego przekazania swojej opinii na jego temat. Nie ulega wątpliwości, że projekt będzie miał bezpośredni wpływ na wiele podmiotów obecnych na polskim rynku, dlatego szczególnie istotne jest, by wysłuchać wszystkich racji i rozważyć np. możliwość przeprowadzenia konferencji uzgodnieniowej, zgodnie z bardzo dobrą praktyką obecną w niektórych procesach legislacyjnych.	
127.	EXATEL	Uwaga ogólna	W pierwszej kolejności należy wyrazić uznanie dla większości zmian zaproponowanych w przedmiotowym projekcie, ponieważ bez wątpienia wpłyną one pozytywnie na system cyberbezpieczeństwa w Polsce. Dodanie do krajowego systemu cyberbezpieczeństwa ISAC, utworzenie CSIRT Telco czy też poddanie dostawców sprzętu lub oprogramowania procedurze sprawdzającej pod kątem zagrożeń dla społeczno-ekonomicznego bezpieczeństwa państwa to kroki zwiększające cyberbezpieczeństwo Polski. Projekt przewiduje również obowiązek powoływania CSIRT sektorowych, które zastąpić mają dotychczasowe sektorowe zespoły do spraw cyberbezpieczeństwa. Do ich zadań ma należeć: 1) przyjmowanie zgłoszeń o incydentach; 2) reagowanie na incydenty; 3) gromadzenie informacji o podatnościach i zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo; 4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;	**Wyjaśnienie** CSIRT sektorowy nie może prowadzić działalności komercyjnej, dlatego zastosowano katalog podmiotów z art. 4 PZP.

			5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach; 6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie w podnoszeniu świadomości zagrożeń cyberbezpieczeństwa (opcjonalnie); 7) koordynowanie w uzgodnieniu z operatorami usług kluczowych obsługi incydentów, które dotyczą różnych podmiotów w danym sektorze lub podsektorze (opcjonalnie). Należy zauważyć, że organami właściwymi są: minister właściwy do spraw energii; minister właściwy do spraw transportu; minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; Komisja Nadzoru Finansowego (ma być to zgodnie z projektem Urząd KNF); minister właściwy do spraw zdrowia; Minister Obrony Narodowej; minister właściwy do spraw gospodarki wodnej; minister właściwy do spraw informatyzacji. Co do zasady organ właściwy będzie musiał zbudować strukturę CSIRT w urzędzie go obsługującym lub powierzyć realizację zadań CSIRT sektorowego jednostkom mu podległym lub przez niego nadzorowanym. W przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5, organ właściwy może, po zasięgnięciu opinii Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, powierzyć realizację zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), oraz określić szczegółowy zakres realizowanych przez niego zadań. Do tych podmiotów z art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019) zaliczamy:	

			1) jednostki sektora finansów publicznych w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, 1622 i 1649); 2) inne, niż określone w pkt 1, państwowe jednostki organizacyjne nieposiadające osobowości prawnej; 3) inne, niż określone w pkt 1, osoby prawne, utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego, jeżeli podmioty, o których mowa w tym przepisie oraz w pkt 1 i 2, pojedynczo lub wspólnie, bezpośrednio lub pośrednio przez inny podmiot: a) finansują je w ponad 50% lub b) posiadają ponad połowę udziałów albo akcji, lub c) sprawują nadzór nad organem zarządzającym, lub d) mają prawo do powoływania ponad połowy składu organu nadzorczego lub zarządzającego; 4) związki podmiotów, o których mowa w pkt 1 lub 2, lub podmiotów, o których mowa w pkt 3. Podsumowując powyższy wyciąg z przepisów trzeba wskazać, że nie ma możliwości zlecenia pełnienia funkcji CSIRT sektorowego „na zewnątrz” – krąg podmiotów mogących pełnić tą funkcję został ściśle ograniczony i w ograniczeniu pominięto również spółki Skarbu Państwa działające na rynku komercyjnym. Tylko nieliczne z organów właściwych mają jednostki podległe lub nadzorowane, które mają zbudowaną podstawową bazę umiejętności w zakresie cyberbezpieczeństwa. Wskazać tutaj można jednostki podległe Ministrowi Obrony Narodowej oraz ministrowi właściwemu do spraw cyfryzacji. W tym miejscu jednak trzeba wskazać, że jednostki te pełnią już rolę CSIRT na poziomie krajowym i nie powinny one dublować swojej funkcji,	

			pełniąc jednocześnie rolę CSIRT na poziomie sektorowym. Efektem przyjętego rozwiązania jest więc konieczność stworzenia przez 8 organów właściwych CSIRT sektorowych od podstaw, na co ustawodawca przewiduje 18 miesięcy od dnia wejścia w życie projektowanej ustawy. Tymczasem należy wskazać, że budowanie, szkolenie i utrzymanie zespołu do spraw cyberbezpieczeństwa wraz z pozyskaniem lub przygotowaniem odpowiednio skutecznego zestawu wykorzystywanych przez zespół narzędzi jest skomplikowanym i długotrwałym procesem. Jego przeprowadzenie wiąże się często ze sporymi komplikacjami, tymczasem zgodnie z projektem taki proces będzie musiał zostać przeprowadzony w urzędach nie mających doświadczenia w takiej działalności.	
128.	EXATEL	Uwaga ogólna	Wskazać można następujące zagrożenia, które w znaczny sposób utrudnią samodzielną budowę CSIRT sektorowych przez organy właściwe: **1. Deficyt wyspecjalizowanej kadry na rynku niezbędnej do powołania CSIRT** Nawet pomimo proponowania rynkowych stawek wynagrodzeń (chociaż z wyliczeń zawartych w OSR nie do końca wiadomo, czy przyjęte koszty uwzględniają też koszty zatrudnienia po stronie pracodawcy) nie ma gwarancji, że uda się zrekrutować zespół odpowiednich specjalistów. W szczególności należy wskazać na niedobór specjalistów z obszaru cyberbezpieczeństwa na rynku, co dotyczy zarówno kadry technicznej mającej doświadczenie w pracy w SOC/CSIRT, jak i kadry posiadającej doświadczenie w budowie i organizacji pracy zespołów SOC/CSIRT. Ponadto nagłe	**Wyjaśnienie** Termin 18 miesięcy na powołanie CSIRT sektorowych jest realny. Niezależnie od zmian legislacyjnych KPRM prowadzi działania mające na celu zaadresowanie problemów o których mówi autor uwagi m. in. w obszarze podnoszenia kompetencji i kwalifikacji kadr, pozyskania finansowania ze źródeł europejskich na działania wzmacniający krajowy system cyberbezpieczeństwa.

			ogłoszenie naborów do kilku nowych organizacji zajmujących się cyberbezpieczeństwem doprowadzi do powstania na rynku takich specjalistów nadmiernego popytu, co z kolei przełoży się na dodatkową presję płacową i w konsekwencji może zdestabilizować działanie aktualnie funkcjonujących zespołów (w tym np. migrację kadry eksperckiej z CSIRT MON, CSIRT NASK i CSIRT GOV do innych podmiotów). 2. **Dostosowanie kultury organizacyjnej do warunków rynkowych istniejących w sektorze IT** Specjaliści IT zajmujący się cyberbezpieczeństwem preferują elastyczne formy zatrudnienia, które obecnie nie są proponowane ani stosowane w polskiej administracji. Ponadto często interesuje ich praca projektowa. Dodatkowo, rekrutując tego typu specjalistów trzeba często stosować nieszablonowe strategie rekrutacji, nieznane w administracji publicznej. 3. **Konieczność pozyskania doświadczeń organów właściwych co do sposobu utworzenia i funkcjonowania CSIRT** Samo przygotowanie koncepcji funkcjonowania CSIRT jest procesem długotrwałym i skomplikowanym. W jego trakcie trzeba podejmować szereg kluczowych decyzji dotyczących sposobu działania poszczególnych linii, wyboru platformy sprzętowej na której CSIRT będzie działać, zasad prowadzenia rekrutacji na poszczególne stanowiska. Samo opracowanie takiej rzetelnej koncepcji jest wyceniane na kwoty od kilkuset tysięcy do ponad miliona złotych. 4. **Krótki czas przewidziany na powołanie i osiągnięcie pełnej sprawności operacyjnej CSIRT**	

			Wskazać należy, że rekrutacje na stanowiska związane z cyberbezpieczeństwem mogą trwać nawet kilka miesięcy, gdzie przy pozyskiwaniu kompetentnych, doświadczonych pracowników standardem jest minimum 6-9 miesięcy od momentu rozpoczęcia rekrutacji, przy założeniu dysponowania odpowiednio wysokiego budżetu na wynagrodzenia. Czas pozyskiwania pracowników może ulec wydłużeniu lub wręcz uniemożliwić realizacje założeń projektu (istnieje wysokie ryzyko braku osiągnięcia zamierzonego celu gotowości operacyjnej). Należy zauważyć, że zrekrutowanie odpowiednich kandydatów jest pierwszym, ale nie jedynym wyzwaniem z perspektywy zasobów ludzkich – najważniejszym jest utrzymanie zrekrutowanej kadry. Ponadto, w przypadku zlecenia przygotowania samej koncepcji budowy CSIRT na zewnątrz w ramach zamówienia publicznego, doliczyć należy czas niezbędny na przeprowadzenie stosownego postepowania i zawarcie umowy, a następnie jej realizację. W końcu, już po pomyślnym zrekrutowaniu wszystkich pracowników i zakupie niezbędnego sprzętu i licencji konieczny będzie okres przygotowawczy pozwalający na budowę i wdrożenie jednolitych procedur i instrukcji pozwalających obsługę klientów CSIRT. W przewidzianym w ustawie okresie 18 miesięcy wykonanie wszystkich wyżej wymienionych zadań wydaje się być bardzo trudne.	
129.	S4IT Michał Podgórski	Uwaga ogólna	Uważam, że projekt może w pewnym stopniu zagrozić rzeczywistym interesom naszych obywateli wpływając negatywnie na koszty oraz dostępność do usług telekomunikacyjnych, zatrudnienie i przyszłe możliwości. Zgłaszam niniejszym następujące uwagi do projektu ustawy:	**Uwaga częściowo uwzględniona** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł.

			1. Projekt wymaga wycofania całego sprzętu danego dostawcy w ciągu 5 lat, co spowoduje, że rząd/dany sektor będzie potrzebował dużej ilości dodatkowych nakładów finansowych, a tym samym wpłynie negatywnie na proces kształtowania społeczeństwa cyfrowego i może spowodować podwyższenie cen u dostawców, którzy zostali zweryfikowani i zatwierdzeni przez specjalistów. 2. Projekt doprowadzi do wzrostu kosztów po stronie operatorów, co spowoduje konieczność wprowadzenia wyższych taryf telekomunikacyjnych i wpłynie negatywnie na i doprowadzi do podwyższenia abonamentu, co bezpośrednio uderzy w klientów końcowych. 3. Wykluczenie poszczególnych producentów doprowadzi do zmniejszenia konkurencji na rynku, co negatywnie wpłynie na koszty operatorów, a tym samym zaszkodzi interesom konsumentów. 4. Projektowane przepisy faktycznie zmierzają do wykluczenia dostawców przez wzgląd na ich kraj pochodzenia, co doprowadzi do stawiania barier handlowych i wpłynie negatywnie na zaufanie inwestorów zagranicznych oraz na rozwój gospodarczy Polski. 5. Projekt spowolni rozwój cyfrowy oraz wpłynie negatywnie na modernizację przemysłu i tworzenie nowych możliwych miejsc pracy. 6. Brak technicznych kryteriów oceny: Rząd ingeruje w wybór dostawcy zamiast ustanowić jednolite standardy techniczne. Nie określa również sprzętu objętego zakresem nowych obowiązków. Operatorzy są zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego/ średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat.	ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane

			7. Projekt doprowadzi do opóźnienia rozwoju sieci 5G, co negatywnie wpłynie na wygodę i łatwość obywateli w korzystaniu z zaawansowanej technologii cyfrowej, np. praca zdalna, telemedycyna, zdalna edukacja, inteligentny przemysł oraz inteligentne rolnictwo.	ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
130.	S4IT Michał Podgórski	Uwaga ogólna	Z punktu widzenia rzeczywistych interesów polskich obywateli oraz przedsiębiorców, sugerujemy przeprowadzenie szerokich konsultacji społecznych, pełne wysłuchanie opinii publicznej oraz dokonanie wyczerpującej analizy skutków regulacji.	**Uwaga częściowo uwzględniona** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane

			• Przyniesienie realnych korzyści dla konsumentów przez obniżenie kosztów po stronie operatorów utrzymując uczciwość równą konkurencję na rynku telekomunikacyjnym. • Uwzględniając zmniejszenie kosztów po stronie operatorów, sugerujemy przedłużyć termin usunięcia sprzętów wymienionych w art. 66b ust. 1 pkt 2 do 10 lat od daty publikacji oceny w przypadku konieczności zmiany dostawcy. • W celu umocnienia zaufania inwestycyjnego, sugerujemy ustalać jasne, wymierne i wykonalne kryteria w art. 66a ust. 4 pkt 2 i 5 i pozwolić operatorom na wybór dostawców na podstawie przejrzystych kryteriów, np. zgodnie z rozwiązaniem stosowanym w Niemczech. • Przyspieszenie rozwoju sieci 5G, aby zapewnić polskim obywatelom wygodę w korzystaniu z bardziej zaawansowanych technologii cyfrowych oraz utworzyć więcej miejsc pracy.	w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy,

				czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

131.	Orange	Uwaga ogólna	P*rojekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych* (dalej „Projekt") jest bardzo rozległy, a jego treść trudna w interpretacji, co potęguje skromna treść uzasadnienia, zaskoczenie przedsiębiorców telekomunikacyjnych kształtem planowanych zmian oraz nakładanie się przepisów na projektowane nowe Prawo Komunikacji Elektronicznej, i to na 3 miesiące przed planowanym jego wejściem w życie. Krajowy system cyberbezpieczeństwa jest w porównaniu do	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania
132.	Orange	Uwaga ogólna	**Ocena bezpieczeństwa dostawców** W pierwszej kolejności podkreślamy, że dotychczasowe stosowanie urządzeń różnych dostawców, w tym z krajów spoza UE nie skutkowało w naszej ocenie zwiększeniem poziomu ryzyka w sieciach telekomunikacyjnych, ani istotnymi incydentami w tym zakresie. Jako kluczowe przedsiębiorstwa branży telekomunikacyjnej w sposób stały i dogłębny analizujemy funkcjonowanie naszych sieci pod kątem możliwych naruszeń i incydentów. Nasze stanowisko wynika przede wszystkim z oceny technicznych i organizacyjnych aspektów takiej współpracy z dostawcami. Ryzyka jakie faktycznie miały wpływ na funkcjonowanie naszych sieci dobrze oddaje statystyka zgłaszanych do UKE naruszeń, przywołana również w uzasadnieniu do przyjętego ostatnio rozporządzenia do art. 175d PT gdzie wskazano: *Najczęstszymi przyczynami naruszeń były awarie sprzętu i oprogramowania (168 przypadków). Dewastacja infrastruktury spowodowała 16 naruszeń, przerwa w zasilaniu – 6, a błąd ludzki – 5. Marginalne były przyczyny spowodowane klęską żywiołową icyberatakiem.* Taki stan rzeczy wynika w dużej mierze również z bardzo wysokiego poziomu zabezpieczenia sieci przed cyberatakami. W tym kontekście uważamy jednocześnie, że	**Uwaga częściowo uwzględniona** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również

			bardzo istotny nacisk należy położyć przede wszystkim na bezpieczeństwo aplikacji i urządzeń końcowych, które z naszej perspektywy stanowią kluczowe wektory ataków i zagrożeń. Podkreślamy również wagę i potrzebę kontynuowania pogłębionej dyskusji nt. bezpieczeństwa sieci i usług telekomunikacyjnych dla procesu dystrybucji częstotliwości z pasma C. W tym kontekście, szczególnej wagi nabiera konieczność określenia zrozumiałych, racjonalnych i akceptowalnych warunków dotyczących bezpieczeństwa sieci i usług telekomunikacyjnych, jakie będą stawiane uczestnikom postępowania w sprawie rezerwacji częstotliwości z pasma C.. Jest to kluczowe dla perspektywy rozwoju sieci 5G w Polsce. Z perspektywy operatorów telekomunikacyjnych planowany do wprowadzenia mechanizm oceny bezpieczeństwa dostawców stanowi jednocześnie rozwiązanie, które wymaga bardzo dobrego przygotowania, zarówno w warstwie konstrukcji przepisów prawnych, jak i sfery organizacyjnej i merytorycznej do dokonywania takich ocen przez instytucje państwowe. Szczególnie, że jak zauważamy nie dotyczy on wyłączenie sieci 5G, ale co uznajemy za zasadniczo słuszne także wszystkich podmiotów krajowego systemu cyberbezpieczeństwa. Nie widzimy bowiem żadnych powodów, aby sprzęt lub oprogramowanie danego dostawcy nie mogło być stosowane w sieci 5G, ale mogło być stosowane przez operatorów usług kluczowych czy podmioty publiczne, co jak wiadomo nie jest wyłącznie konstrukcją teoretyczną, ale stanem faktycznym. Zastosowanie mechanizmu oceny będzie miało bardzo poważne konsekwencje w wielu sferach dotyczących użytkowników sprzętu i oprogramowania dostawcy ocenionego jako stwarzającego ryzyko wysokie lub umiarkowane, konkurencji na rynku,	zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na

			użytkowników usług czy wreszcie relacji międzynarodowych. Skala konsekwencji, których w tym stanowisku nie przedstawiamy już szczegółowo, jest tak znacząca, że uzasadnia przynajmniej pogłębioną refleksję nad przedłożoną propozycją. Stąd uważamy, że w pierwszej kolejności należy rozważyć czy sam mechanizm oceny funkcjonującego już na rynku dostawcy w zaproponowanej formie jest najbardziej efektywny, właściwie rozkłada akcenty i czy przede wszystkim nie przenosi zbyt dużej odpowiedzialności za dokonane oceny na samą administrację publiczną i to w jej najwyższych rangach. Należy bowiem zakładać, że kluczowe decyzje będą przedmiotem wnikliwych analiz i będą mogły być w różnych formach kontestowane. Uwzględniając zaś przedstawione w projekcie ustawy kryteria oceny, wydaje się, że zarzuty mogą okazywać się zasadne narażając na niepotrzebne ryzyko i koszty zarówno podmioty wydające ocenę, jak i podmioty nią objęte. Zanim przedstawimy nasze kluczowe postulaty odnoszące się do zaprezentowanego w projekcie ustawy modelu oceny, chcielibyśmy poddać pod rozwagę alternatywne i możliwe do równoległego stosowania sposoby działania, których wdrożenie pozwoliłoby osiągnąć podobne efekty, ale z ograniczeniem kluczowych ryzyk: • Włączenie dostawców sprzętu lub oprogramowania do krajowego systemu cyberbezpieczeństwa i wprowadzenie odpowiednich wymagań dot. bezpieczeństwa oraz wdrożenia środków technicznych i organizacyjnych mających ograniczać poziom ryzyka. • Stworzenie mechanizmu generalnego dopuszczenia dostawców do rynku w określonych z góry sektorach	Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

			krajowego systemu cyberbezpieczeństwa oraz spoza niego, jak np. w zakresie telekomunikacji, a także obszarów tych sektorów, tj. zdefiniowanie listy kluczowych zasobów/zastosowań, pod których kątem powinna być prowadzona ocena dopuszczająca dostawcę. Rozwiązanie to dawałoby możliwość instytucjom stworzenia warunków dostępu oraz przeniesienie przynajmniej części ciężaru dowodowego na dostawcę. Mechanizm ten, jako powszechny pozwalałby też na ograniczenie zarzutu stronniczości. • Oparcie się na schematach certyfikacji, które istnieją już w poszczególnych sektorach lub które są opracowywane w ramach wdrożenia „Cybersecurity Act". Uzyskanie takiej certyfikacji powinno zostać wprowadzone jako obowiązkowe dla kluczowych zasobów/zastosowań dostawców. Ten sposób weryfikacji zapewniałby niezależną i trudną do podważenia ocenę czynników technicznych. Uwzględniając jednocześnie zalecenia wskazane w 5G Toolbox mógłby być, szczególnie dla kluczowych ryzyk, uzupełniany przez ocenę kwestii pozostających poza sferą techniki, o ile identyfikowany jest ich istotny wpływ na poziom bezpieczeństwa narodowego. • Opracowanie listy kluczowych zasobów/zastosowań oraz określenie konkretnych wymagań wobec dostawców, które takie zasoby dostarczają dla określonych sektorów. Weryfikacja ich spełnienia byłaby niezbędna dla	

			dopuszczenia nowego sprzętu lub oprogramowania do obrotu. • Niezależnie od powyższych rozwiązań alternatywnych, w każdym przypadku jakiekolwiek decyzje skutkujące wykluczeniem muszą w pełni uwzględniać istniejącą sytuację rynkową, skutki rekomendacji, a przede wszystkim być ograniczone do kluczowych zasobów danego dostawcy oraz zapewniać użytkownikom sprzętu lub oprogramowania odpowiedni czas na dostosowanie. Generalną zasadą powinna być skuteczność oceny jedynie dla przyszłych stanów prawnych i faktycznych, a jedynie w ograniczonych przypadkach skuteczność wobec istniejących już, zakupionych lub użytkowanych urządzeń lub oprogramowania. Z tych względów jakiekolwiek wykluczenia mogące mieć skutki retroaktywne muszą posiadać odpowiednio długie okresy na wycofanie stosowania danych urządzeń lub oprogramowania, określone jako minimum 8-10 lat, co pozwoli na ograniczenie negatywnych skutków finansowych i organizacyjnych procesu wycofania. • Jednocześnie uważamy, że takie rozwiązania powinny być wprowadzane w sposób zharmonizowany na poziomie UE. Odnosząc się natomiast wprost do zaproponowanego w projekcie mechanizmu oceny dostawców postulujemy przede wszystkim: • Ocena dostawców nie powinna być oparta tylko o kryteria nietechniczne, które przedstawiono w projekcie ustawy.	

			Każda ocena tego typu musi również uwzględniać kwestie techniczne w odniesieniu do zidentyfikowanych kluczowych zasobów dostarczanych przez danego dostawcę. Brak takiego elementu może skutkować zarzutami dot. zbytniej uznaniowości dokonanej oceny. Najlepszą natomiast metodą oceny kwestii technicznych jest wykorzystanie mechanizmów certyfikacji, które poza efektem w obszarze bezpieczeństwa, mają również potencjał do pobudzenia rynku, w tym budowy narodowych kompetencji w tym zakresie. • Jakiekolwiek restrykcje wprowadzane w wyniku oceny, muszą zgodnie z 5G Toolbox odnosić się wyłącznie do zdefiniowanych uprzednio kluczowych zasobów. Jednocześnie ich skutek w zakresie istniejących już stanów prawnych i faktycznych musi uwzględniać co najmniej 8-10 letni okres na wycofanie danych urządzeń lub oprogramowania, co odpowiada okresom amortyzacji oraz daje szanse na ograniczenie negatywnych skutków finansowych i organizacyjnych. Jednocześnie, niezbędne jest aby w zakresie w jakim dopuszczone jest stosowanie określonego sprzętu lub oprogramowania istniała możliwość dokonywania zakupów i wdrożeń służących zabezpieczeniu jakości i ciągłości świadczenia użytkownikom usług, w tym w przypadku sieci ruchomych w zakresie zapewniania adekwatnej do zapotrzebowania pojemności sieci.	

			• Kryteria oceny nie mogą abstrahować zupełnie od konkretnych zastosowań danego sprzętu lub oprogramowania. Wszak, niektóre zastosowania kluczowych zasobów mogą uzasadniać nałożenie restrykcji, a inne zupełnie nie. W tym sensie inny będzie ciężar stosowania danego sprzętu lub oprogramowania w określonych systemach lub strategicznych lokalizacjach, a inny w usługach masowych. • Wniosek o sporządzenie oceny musi zostać doprecyzowany tak, aby wyraźnie określał przynajmniej kluczowe zasoby danego dostawcy pod kątem, których ma zostać dokonana ocena, identyfikować aktualnych i potencjalnych użytkowników tych zasobów oraz szczegółowo oceniać skutki ewentualnej oceny negatywnej. • Ocena dokonywana przez Kolegium powinna mieć formę decyzji administracyjnej, a ścieżkę odwoławczą należy zapewnić wszystkim zainteresowanym stronom, w tym użytkownikom sprzętu lub oprogramowania niezależnie czy poziom oceny to ryzyko wysokie, umiarkowane czy niskie. Sposób określenia poziomów ryzyk posługuje się obecnie pojęciami nieprecyzyjnymi, jak poważne, niewielkie, znikome. W naszej ocenie wymaga to istotnego doprecyzowania.	
133.	Orange	Uwaga ogólna	**Ostrzeżenia i polecenia zabezpieczające** W naszej ocenie proponowane środki są zbyt daleko idące i dają Pełnomocnikowi uprawnienia, które mogą faktycznie wpływać na	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu

			sposób prowadzenia działalności gospodarczej także przez podmioty prywatne. W szczególności takie obawy budzi instytucja ostrzeżenia, która jedynie w wyniku identyfikacji zagrożenia wystąpieniem jakiegokolwiek incydentu krytycznego może skutkować nałożeniem konkretnych obowiązków, w tym w zakresie wycofania urządzeń lub oprogramowania danych dostawców (co zasadniczo powinno być przedmiotem oceny Kolegium) i to na długi 2-letni okres. Planowane do wprowadzenia rozwiązania stanowią bardzo poważne oręże w rękach Pełnomocnika, którego stosowanie w obecnym kształcie będzie wymagało bardzo wysokiego poziomu wstrzemięźliwości i dopuszczalne jedynie jako rozwiązanie zupełnie ostateczne. W innym przypadku istnieje znaczące ryzyko, że ostrzeżenia i polecenia będą wykorzystywane zbyt często, zapobiegawczo, nieproporcjonalnie i bez uwzględniania skutków finansowych po stronie podmiotów, których będą dotyczyły skutki wydania ostrzeżeń lub poleceń. W tym obszarze przedstawiamy następujące postulaty kluczowe: • Instytucja ostrzeżenia powinna zostać zmodyfikowana w sposób odpowiadający jej nazwie. Oznacza to, że należy usunąć odwołania do jej skutków jako poleceń, nakazów lub zakazów. W tym ujęciu ostrzeżenie powinno być wydawane jako sygnalizacja określonego ryzyka wraz ze szczegółowym uzasadnieniem oraz przedstawieniem możliwości przeciwdziałania. • W przypadku utrzymania obecnego kształtu ostrzeżenia powinno ono być wydawane w formie decyzji	cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania

			administracyjnej oraz ograniczone do podmiotów publicznych. • Okres na jaki mają być wydawane ostrzeżenia lub polecenia zabezpieczający musi zostać dostosowany do każdej indywidualnej sytuacji i być liczony w dniach/tygodniach, a nie wynosić, aż 2 lata. Tak długi okres wskazuje, że intencją może być stosowanie tych instrumentów nie jako reakcji na konkretne wydarzenia, ale jako instrument realizacji długoterminowej polityki. • Adresowanie ostrzeżeń lub poleceń zabezpieczających, szczególnie w ich obecnym kształcie, do podmiotów prywatnych powinno wiązać się rekompensatą kosztów i strat. • Przed wydaniem ostrzeżenia lub polecenia niezbędne jest przeprowadzenie konsultacji z podmiotem, który ma zostać nim objęty, w celu ustalenia okoliczności, stanu faktycznego oraz potencjalnych działań alternatywnych. W ramach wskazywania oczekiwanych działań od podmiotu do którego adresowane jest polecenie lub ostrzeżenie należy każdorazowo dokonać wnikliwej analizy technicznej możliwości wdrożenia danej rekomendacji.	może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

134.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Uwaga ogólna	Ustawa w oczywisty sposób narusza zasady niedyskryminacji i uczciwej konkurencji pomiędzy przedsiębiorcami oraz międzynarodowe umowy handlowe zawarte przez Polskę z innymi państwami. Projekt ustawy może doprowadzić do sytuacji , w której rynek będzie podlegał wpływom politycznym, co nie sprzyja wolnej konkurencji. Będzie to miało istotny negatywny wpływ na otoczenie biznesowe i całą branżę ICT w Polsce. **Projekt narusza również zasadę niedyskryminacji opracowaną przez UE i zasadę uczciwej konkurencji zgodnie z wytycznymi Światowej Organizacji Handlu (WTO).** Jeśli Projekt zostanie przyjęty, wpłynie to na inwestycje UE w Polsce i rozwój polskiej branży ICT. Co więcej, projekt negatywnie wpłynie na wolny handel z członkami WTO i zaufanie inwestorów zagranicznych do Polski. **Naruszenie zasad uczciwej konkurencji:** Jeśli nowe przepisy zostaną przyjęte, Kolegium uzyska de facto prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie sprzyja konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie do tylko jednego z nich spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży **Wbrew podstawowej zasadzie wolnego handlu w gospodarce rynkowej, dyskryminacja niszczy ekosystem branży ICT i zwiększa koszty dostaw i obsługi** sprzedaży produktów z innych krajów wydaje się pomagać niekonkurencyjnym branżom i przedsiębiorstwom. W przypadku polskiej branży ICT pozbawi to branżę ICT i przedsiębiorstwa motywacji do większych inwestycji i ulepszania technologii, prowadząc do spadku konkurencyjności produktów. Z drugiej strony branża i przedsiębiorstwa w innych krajach podejmą więcej kroków w celu poprawy konkurencyjności. W rezultacie	**Wyjaśnienie** Projekt nowelizacji jest zgodny z prawem europejskim i międzynarodowym. Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT. Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej

			międzynarodowa konkurencyjność polskiej branży ICT i przedsiębiorstw będzie ulegać dalszemu osłabieniu.	generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.

135.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Uwaga ogólna	Jako podmiot odpowiedzialny społecznie, mamy za zadanie aktywnie rozpowszechniać racjonalne rozwiązania. Mając na uwadze utrzymanie dobrych relacji środowiska biznesowego z Rządem Polski i apelujemy o rozważenie i podjęcie następujących działań 1. Ministerstwo Cyfryzacji powinno zorganizować otwartą debatę i zaprosić odpowiednie ministerstwa, izby gospodarcze, operatorów i inne zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w projekcie. 2. Rząd powinien w pełni ocenić wpływ projektu, w tym koszty i straty, na konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. 3. Zasadniczo, zablokowanie niektórych dostawców nie może rozwiązać problemów związanych z bezpieczeństwem cybernetycznym. Wnosimy o przyjęcie spójnej strategii w ramach UE, w celu zarządzania za pomocą jasnych specyfikacji technicznych i zharmonizowanych norm, zamiast wykluczania dostawców z określonych krajów. Postulujemy odwołanie się do modelu niemieckiego i równe traktowanie wszystkich dostawców, nie tylko z powodów nietechnicznych. Z punktu widzenia racjonalności ekonomicznej, rząd musi promować dwustronny wolny handel i zmniejszać bariery w swobodnym przepływie towarów i usług. Rząd powinien ogłosić przepisy ustawowe i wykonawcze oraz środki, które sformułował i wdrożył, a także ich zmiany, jak również powinien informować o nich Światową Organizację Handlu	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

136.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Uwaga ogólna	Operatorzy telekomunikacyjni powinni otrzymać rekompensatę za koszty poniesione w związku z wymianą sprzętu lub oprogramowania, a rekompensatę powinno obliczać się na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE.	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
137.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Uwaga ogólna	Wprowadzenie wspólnego unijnego mechanizmu certyfikacji krytycznego sprzętu i oprogramowania wykorzystywanego do weryfikacji bezpieczeństwa. **Uzasadnienie:** 1) Ustalenie obiektywnych i jasnych kryteriów, upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. 2) Skuteczniejszym będzie zmotywowanie dostawców do samokontroli i złożenia oświadczenia o wiarygodności. 3) Nietechnologiczne kryteria są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.	

138.	Aberit	Uwaga ogólna	Działając w imieniu spółki Aberit sp. z o. o. działającej w branży IT, chciałbym wyrazić swoje obawy związane bezpośrednio z planem wprowadzenia projektu cytowanej ustawy. Po zapoznaniu się z przepisami sądzę, że spółka w imieniu, której występuje może zostać dotknięta nowymi regulacjami. Co za tym idzie zwracam się do Państwa z prośbą o zapoznanie się z poniższymi wątpliwościami oraz rozważeniem ich w ramach prowadzonych konsultacji społecznych. Celem naszego Państwa jest dążenie do ciągłego rozwoju, poprawy infrastruktury, ochrony praw i interesów obywateli. Niemniej jednak proponowany projekt ustawy w moim odczuciu może zaszkodzić rzeczywistym interesom obywateli Polski. Przepisy w proponowanej formie mogą wpłynąć negatywnie na ceny, wygodę i dostępność korzystania z usług komunikacyjnych, a także na zatrudnienie i przyszłe możliwości przedsiębiorców działających w objętej regulacjami branży. 1, Wprowadzenie art, 66b ust. 1 w proponowanej formie doprowadzi do powstania istotnych, wysokich kosztów dla operatorów telekomunikacyjnych, których nie powinni oni ponosić. Koszty spowodowane wprowadzeniem nowych regulacji, powinny zostać pokryte przez Skarb Państwa. Jeżeli Państwo wymaga od operatorów wymiany sprzętu i oprogramowania, narzucając im to poprzez zmiany w ustawie, powinni oni otrzymać odszkodowanie za koszty poniesione w związku z przeprowadzoną wymianą. W przeciwnym razie wysokie koszty po stronie operatorów doprowadzą do podniesienia cen usług telekomunikacyjnych, co odbije się bezpośrednio na obywatelach korzystających z usług i ich jakości życia.	Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			1. Projekt zakłada także wykluczenie dostawców infrastruktury ze względu na ich kraj pochodzenia. Wykluczenie części dostawców doprowadzi do braku konkurencyjności na rynku telekomunikacyjnym, co ponownie odbije się na konsumentach i bez wątpienie zaszkodzi ich interesom. Ponadto tego rodzaju ograniczenie wywoła negatywne nastawienie zagranicznych inwestorów, przyczyniając się tym samym do zahamowania rozwoju gospodarczego Polski. 3, Projekt prowadzi także do opóźnienia rozwoju sieci 5G w Polsce. Warto podkreślić, że sieć ta jest już wysoce rozwinięta i sprawnie działa w krajach zachodnich UE. Tego rodzaju zabieg przyczyni się do poszerzenia przepaści pomiędzy Polską, a innymi, rozwiniętymi technologicznie krajami Europy. Opóźnienie rozwoju sieci 5G wpłynie również negatywnie na wygodę i łatwość obywateli w korzystaniu z zaawansowanej technologii cyfrowej, np. praca zdalna, telemedycyna, zdalna edukacja, inteligentny przemysł oraz inteligentne rolnictwo. Biorąc pod uwagę powyższe argumenty, wyrażam swoje obawy i niezadowolenie względem przepisów ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych. Mając na względzie dobro obywateli i rozwój gospodarczy naszego kraju żywię nadzieję, że Ministerstwo Cyfryzacjl weźmie pod uwagę opinię publiczną i podda przepisy niniejszej ustawy dodatkowym konsultacjom.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

139.	Osoba fizyczna	Uwaga ogólna	Przedmiotem oceny ryzyka zakładanym w projekcie nie powinien być dostawca. Ocena ryzyka powinna dotyczyć sprzętu i oprogramowania. Uważamy, że elementem stosunkowo najmniej istotnym jest podmiot, który sprzedaje oprogramowanie i sprzęt, zaś zdecydowanie najważniejszą rzeczą jest sposób korzystania z nich. Narzędzia Unii Europejskiej - toolbox zabezpieczyły już sposób ograniczenia w odniesieniu do kluczowych aktywów. Nie widzimy potrzeby, aby polskie regulacje wykraczały poza system zabezpieczający UE. Natomiast jeżeli przepisy te wejdą w życie w proponowanym kształcie, to wpłynie w niekorzystny sposób na polskie podmioty utrudniając im poruszanie się po wolnym rynku i sprawiając, że będziemy odstawać od zachodnioeuropejskich podmiotów z branży IT. Jednocześnie poważnie Zachwieje to równowagą rynkową, konkurencyjnością polskich firm, a także atrakcyjnością Polski jako miejsca do inwestycji kapitału. Wprost wynikającym z tego problemem będzie zas wolniejszy rozwój gospodarczy Polski (np. w zakresie rozwoju firm, modernizacji przemysłu, tworzenia nowych miejsc pracy etc.} a także - co oczywiste - spowoduje to podwyższenie cen usług telekomunikacyjnych.	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
140.	Osoba fizyczna	Uwaga ogólna	Operatorzy telekomunikacyjni w myśl proponowanych przepisów zostaną obciążeni gigantycznymi kosztami wymiany sprzętu i oprogramowania, co Zachwieje wolnym rynkiem i konkurencyjnością w branży. Uważamy, że podmioty zmuszone do w/w wymian powinny uzyskać rekompensaty od Skarbu Państwa za poniesione straty. Ponieważ koszty, które powstaną wynikają bezpośrednio ze zmiany przepisów wprowadzanych przez Państwo Polskie. Prawie oczywistym wydaje się, że koszty poniesione przez operatorów zostaną przełożone na polskiego obywatela w postaci podniesionych cen abonamentów i usług telekomunikacyjnych, a co za tym idzie odbiją się wprost na polskiej gospodarce.	**Uwaga nieuwzględniona** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

141.	Osoba fizyczna	Uwaga ogólna	Projekt zakłada również wyraźną dyskryminację poszczególnych dostawców. Zakładane kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne np. powiązania dostawcy a polityką rządu kraju macierzystego. Dostawcy nie mają wpływu na politykę swojego kraju a są za to w myśl zaproponowanych przepisów dyskryminowani. Jest to sprzeczne z zasadami wolnego rynku i wolnego handlu. Zakazanie działań dostawców ze względu na w/w kryteria doprowadzi do zlikwidowania lub znacznego ograniczenia konkurencji rynkowej, co nigdy nie przynosi pozytywnych rezultatów. Tylko zdrowa konkurencja może nas uchronić przed ponoszeniem niepotrzebnych kosztów związanych np. z budową i renowacją infrastruktury 1T Kolejnym szczególnie istotnym problemem, który zauważamy w projekcie jest ocena ryzyka dostawcy sprzętu lub oprogramowania ważnego z punktu państwowego systemu cyberbezpieczeństwa. Rozpoczęcie oceny ryzyka powinno być możliwe jedynie w przypadkach określonych w ustawie, aby skupić analizę ryzyka jedynie na kluczowych aktywach, nie zaś na wszystkich aktywach. Postulujemy zatem, aby kontroli podlegało wyłącznie realnie zidentyfikowane ryzyko, a ocena ryzyka była przeprowadzana w stosunku do sprzętu krytycznego z punktu widzenia bezpieczeństwa lub wówczas, gdy miały miejsce poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

142.	Osoba fizyczna	Uwaga ogólna	Dyskryminującym jest również pozbawienie możliwości zmiany wyniku oceny dokonanej przez kolegium. Dostawca powinien mieć prawo do złożenia wniosku o zmianę oceny zarówno w przypadku sprzętu i oprogramowania wysokiego, średniego jak i niskiego ryzyka. Każdy z dostawców powinien mieć takie samo - równe prawo do zaproponowania wprowadzenia planu naprawczego i środków zaradczych. Kolegium powinno posiadać możliwość zaakceptowania programu naprawy podmiotu, a co za tym idzie zmianę oceny. Tylko taka regulacja pozwoli na równe traktowanie wszystkich podmiotów	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
143. 144.	Osoba fizyczna Pan Filip Walczak Młodzieżowy Delegat RP do NATO	Uwaga ogólna Uwaga ogólna	Projekt zmian, jakkolwiek konieczny w zmieniającej się rzeczywistości, budzi pewne konkretne obawy. Wierzę, że społeczny głos w tej sprawie zostanie wzięty pod uwagę i pozwoli uniknąć stworzenia niekorzystnych bądź nieefektywnych przepisów. Z projektu w obecnym kształcie wynikną niepokojące różnice w traktowaniu poszczególnych dostawców. Proponowane kryteria oceny to wyłącznie kryteria nietechniczne, które w tak specjalistycznej branży powinny mieć możliwie najmniejsze znaczenie. Tylko jasne, szczegółowo sprecyzowane kryteria techniczne są w stanie ocenić ryzyko wiążące się z danym dostawcą i jego sprzętem bądź usługami. Kryterium decydującym nie może być np. polityka rządu kraju pochodzenia dostawcy lub sprzętu. W obecnej globalnej sytuacji rynkowej, w której największe podmioty w branży są w skomplikowany sposób powiązane z całym szeregiem państw, tak szerokie, nietechniczne kryteria oceny mogą prowadzić do paraliżu całej branży. Jest to w sposób oczywisty sprzeczne z zasadami wolnego rynku i wolnego handlu zagwarantowanego w wielu przepisach i umowach międzynarodowych. Jawna dyskryminacja będzie zaś prowadziła do znacznego ograniczenia konkurencji rynkowej, co zawsze okazuje się ostatecznie niekorzystne dla wszystkich, w szczególności zaś dla końcowego odbiorcy usługi. Pokrewnym elementem, istotnym z gospodarczego punktu widzenia, jest konieczność zmiany przedmiotu oceny ryzyka: zamiast charakterystyki dostawcy, w pierwszej kolejności winien być oceniany sam sprzęt i jego oprogramowanie. W ramach Unii	Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania

			Europejskiej wypracowano już w tym zakresie odpowiednie zabezpieczenia, potocznie określane jako EU Toolbox, i nie ma podstaw, dla których polskie normy powinny być bardziej restrykcyjne niż wspólnotowe. Proponowane przepisy sprawią, że poruszanie się na rynku IT będzie znacznie utrudnione w porównaniu do naszych zachodnioeuropejskich partnerów, i w wyraźny sposób wpłynie na naszą atrakcyjność inwestycyjną. Polska jako miejsce do inwestycji kapitału jest dzisiaj wyjątkowo atrakcyjna, a wprowadzenie niepotrzebnych ograniczeń prawnych może tę atrakcyjność zmniejszyć. Dynamiczny rozwój gospodarczy Polski jest w interesie wszystkich podmiotów, ale przede wszystkim w leży on w interesie nas - obywateli, którzy mogą korzystać z rozwijającej się rzeczywistości gospodarczej i ekonomicznej, w której żyjemy. Obciążanie operatorów komunikacyjnych znacznymi kosztami wymian sprzętu i oprogramowania, niczym niezawinionych przez podmiot, a wynikających wprost z proponowanych przepisów, jest wysoce niesprawiedliwe. Koszty te powinny być przynajmniej częściowo rekompensowane przez państwo. W przypadku wejścia w życie ustawy w obecnym kształcie, bardzo realnym wydaje się być scenariusz, w którym to operatorzy przeniosą swoje koszty na abonentów, co z kolei wpłynie niekorzystnie na rozwój gospodarczy Polski i na odbiorców końcowych. Pozbawienie niektórych podmiotów możliwości zmiany oceny dokonanej przez Kolegium prowadzi do nierówności poszczególnych podmiotów z branży wobec prawa. Projekt odmawia prawa do złożenia wniosku o zmianę oceny ryzyka przez podmioty najsurowiej ocenione przez Kolegium. Wydaje się to wysoce niesprawiedliwe, gdyż każdy z dostawców powinien mieć	poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący

			zagwarantowane takie same uprawnienia, niezależnie od przypisywanego mu ryzyka. Kolegium nie może być uznane za organ nieomylny. Każdy z podmiotów powinien mieć również równe prawo do wprowadzenia programu naprawczego i środków zaradczych, a samo Kolegium powinno mieć możliwość zmiany decyzji	w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
145.	Pan Filip Walczak Młodzieżowy Delegat RP do NATO	Uwaga ogólna	Projektowany Art. 67b ust. 3 Ustawy ustanawia zamknięty katalog określonych zachowań, jakie mogą zostać wskazane przez Pełnomocnika w ostrzeżeniu. Dynamiczny rozwój nowych technologii i stale zmieniająca się natura cyberzagrożeń powodują, że katalog ten winien być otwarty poprzez dodanie określenia „w szczególności". Pozwoli on Pełnomocnikowi na bardziej elastyczne i skuteczne reagowanie na potencjalne zagrożenia, bez niepotrzebnego związania wąskimi normami kompetencyjnymi. W tym miejscu należy nadmienią iż *a contrario* Art. 67c ust. 4 słusznie zawiera zamknięty katalog określonych zachowań możliwych do nakazania przez Pełnomocnika. Potrzeba pewności prawa wymaga, aby polecenia podlegające natychmiastowemu wykonaniu były ściśle i jasno umocowane w prawie. Odmienny, mniej rygorystyczny charakter ostrzeżeń, zasługuje na odmienne podejście i przyznanie większej swobody Pełnomocnikowi.	Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w

				celu ustalenia czy spełniają ustawową przesłankę ich wydania.
146.	ERSTAR	Uwaga ogólna	Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się zaniepokojeni Projektem Ustawy, który może mieć negatywny wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT. Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na zatrudnienie i rozwój branży telekomunikacyjnej, co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty,	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.

			konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę.	Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o

				uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
147.	ETOB-RES	Uwaga ogólna	Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne. Ważniejszym pytaniem powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje. Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE. Zaproponowane w art. 66a ust. 4 kryteria oceny ryzyka nie są jasne. Powinny one zostać ustalone w sposób obiektywny, pozbawiony wątpliwości, co zagwarantowało by, że ich zastosowanie da rzetelne wyniki oceny ryzyka. W chwili obecnej kryteria nietechnologiczne wykorzystują niejasne pojęcia, które są trudne do zweryfikowania i oceny. Wycofanie i wymiana sprzętu z krytycznym oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci, zajmie to dużo czasu, w przeciwnym razie wpłynie to na stabilność sieci. Również koszty będą bardzo wysokie. Narzucony okres 5 lat jest zbyt krótki aby przeprowadzić tego typu zmiany. Celowym jest wydłużenie okresu do co najmniej 10 lat. Ponadto okres 3 miesięcy dla przygotowania i przedstawienia planu i	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

			harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania jest praktycznie niemożliwy do wdrożenia i powinien zostać wydłużony co jednego roku.	sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast

				przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
148.	Fundacja Alatum	Uwaga ogólna	Proponowany termin wycofywania z rynku sprzętu, usług i oprogramowania w przypadku wydania niekorzystnej oceny przez Kolegium jest bardzo niepokojący. W branży IT proponowany 5-cio letni termin jest okresem wyjątkowo krótkim, który niewątpliwie wpłynie na stabilność całej sieci. Oczywistym wydaje się, że stabilność sieci leży w interesie wszystkich - zarówno rządzących, jak i przedsiębiorców. Dlatego też dużo bardziej adekwatnym i mniej niepokojącym byłby termin 10-cio letni. Musimy pamiętać, że wycofanie z rynku sprzętu, usługi i oprogramowania niesie za sobą gigantyczne koszty i jest to bardzo skomplikowany proces. Rozsądnym byłoby również wprowadzenie rekompensat rządowych dla podmiotów zmuszonych nowymi przepisami do poniesienia tych kosztów. Podmiot nie ma wpływu na nowo tworzone przepisy, które mogą w konsekwencji zmuszać go do poniesienia gigantycznych nakładów finansowych. Pamiętajmy również o tym, że podmioty będą starały się zrekompensować sobie takie straty przenosząc ten koszt bezpośrednio na beneficjentów usług czyli	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania.

			przedsiębiorców i obywateli, co będzie skutkowało znaczącym wzrostem cen usług abonamentowych.	Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

				Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

149.	Fundacja Alatum	Uwaga ogólna	Nowe przepisy zakładają możliwość wpływania przez Kolegium w sposób bardzo niejasny na niektóre podmioty. W branży cybernetycznej można stworzyć szczegółowe wytyczne techniczne, które zablokują możliwość niejasnych i niczym niekontrolowanych możliwości oceny przez Kolegium. Takie techniczne przepisy odsuną od nas widma niejasnego, niesprawiedliwego i nierównego traktowania. Ograniczą też potencjalną korupcję i patologiczne możliwości wpływania na werdykt Komisji. Zasadnym wydaje się też włączenie w postępowanie oceniające samego podmiotu ocenianego np. poprzez możliwość złożenia wyjaśnień. Uważamy również, że jedynie możliwość odwołania od decyzji równa dla wszystkich podmiotów oraz zgodna z przepisami KPA będzie gwarantowała równe traktowanie zagwarantowane nam w Konstytucji. W projekcie zauważamy również niesprawiedliwość społeczną związaną z zakładanymi kryteriami ryzyka. Wszystkie te kryteria to wyłącznie czynniki nietechniczne, które w branży IT powinny mieć drugorzędne znaczenie. Proponowane przepisy zakładają, że dostawcy mają jakikolwiek wpływ na politykę rządu państwa z którego się wywodzą, podczas gdy doskonale wiadomo, że nie odpowiada do rzeczywistości. Wykluczanie w ten sposób podmiotów za nieswojej winy znacząco wpływa natomiast na wolny rynek i ograniczenie konkurencji. Sztuczne zmniejszanie ilości podmiotów na rynku wpłynie zdecydowanie na wzrost kosztów związanych np. z budową i renowacją infrastruktury technicznej. W naszej ocenie proponowany projekt zmian przyniesie wiele opóźnień we wprowadzaniu najnowszych technologii na polski rynek, a tylko szybka budowa sieci 5G może zmniejszyć przepaść między naszym krajem a zachodnią Europą. Perspektywa nowoczesnej gospodarki jest bliska każdemu z nas i tylko ona	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			zagwarantuje nam konkurencyjność w starciu z bogatszymi i lepiej rozwiniętymi państwami UE. Nowe przepisy powinny wspierać innowację i technologię, która w bezpośredni sposób przekłada się na szybki rozwój polskiej gospodarki. Ostatnią rzeczą na którą pragniemy zwrócić uwagę jest umieszczanie w ustawie przepisów dotyczących przedsiębiorstw komunikacji elektronicznej. Przedsiębiorstwa te objęte są szczegółowymi przepisami Prawa Komunikacji Elektronicznej, a nakładanie się tych przepisów niewątpliwie wprowadzi chaos interpretacyjny i konflikty prawne. Sytuacja taka - podobnie jak wcześniejsze przez nas wymienione - zdecydowanie nie będzie korzystnie wpływać na szybki rozwój branży IT. Przepisy dotyczą bardzo specyficznej części gospodarki, w której każde opóźnienie znacząco wpływa na rynek, a przepaść która będzie się tworzyć będzie za chwilę niemożliwa do nadrobienia. Polska powinna dbać o zmniejszanie dystansu miedzy naszym krajem a krajami wysokorozwiniętymi, bo jest to w sposób oczywisty korzystne dla każdego polskiego obywatela. Konsultacje społeczne mają na celu zwrócenie rządzącym uwagi na problemy, których dotykają proponowane zmiany przepisów tak, aby stworzone przepisy dawały zarówno rządowi jak i obywatelowi korzystne, jasne, sprawiedliwe i równe prawo. Wierzymy, że również i te konsultacje doprowadzą do pozytywnych rezultatów dla wszystkich stron. Dziękujemy za możliwość zabrania głosu i za potencjalny wkład w powstanie jak najlepszych regulacji prawnych.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

150.	GBX Soft	Uwaga ogólna	Z uwagi na fakt, że Ustawa dotyczy bezpośrednio mojej osoby oraz działalności jaką prowadzę, szczegółowo zapoznałem się z projektem, który wydaje się być w pewnym zakresie niekorzystny. Moją szczególną uwagę przykuły przepisy, dotyczące oceny ryzyka, które pozwoliłem sobie wskazać w dalszej treści pisma.	

151.	Instytut Lema	Uwaga ogólna	Na wstępie należy wskazać na potrzebę publicznej dyskusji nad kwestią cyberbezpieczeństwa i jej regulacji. Jest to temat niezwykle aktualny i istotny dla społeczeństwa. Projekt ustawy to regulacja o szerokim zakresie przedmiotowym, mająca duże znaczenie dla rynków regulowanych oraz procesu wdrażania sieci 5G, dostawców infrastruktury i oprogramowania a także użytkowników. Z tych też powodów konieczna jest precyzja i spójność regulacji. W pierwszej kolejności, należy zwrócić uwagę na zaproponowane w projekcie rozwiązanie, w ramach którego Kolegium ds. Cyberbeczpieczeństwa zyskuje uprawnienie do możliwość oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Kryteria dokonywania oceny nie zostały w projekcie dostatecznie jasno sprecyzowane i mogą budzić wątpliwości. Jeżeli ocena danego dostawcy sprzętu lub oprogramowania określi ryzyko jako umiarkowane lub niskie, to dostawca może przedstawić środki zaradcze i plan naprawczy. Jeżeli Kolegium zaakceptuje tę propozycję, to ocena ryzyka tego dostawcy może być zmieniona. W przypadku oceny ryzyka określającej wysokie ryzyko, podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły wprowadzać do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania. Z kolei dotychczas używany sprzęt, oprogramowanie i usługi określone także oddziaływać na rynek pracy, bowiem rozwój sieci 5G, z pewnością wiązać się będzie ze zwiększeniem zatrudnienia w branży. Dlatego też niezbędne jest zaprojektowanie takiej regulacji, która tworzyłaby przyjazne warunki dla podmiotów, m.in. dostawców sprzętu i oprogramowania, które poprzez swoją działalność będą napędzać także rozwój gospodarczy kraju.	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			Podsumowując, należy wskazać, iż procedowana regulacja wymaga szerszego spojrzenia na kontekst gospodarczy. Projektowane przepisy powinny w sposób maksymalnie precyzyjny i jasny wskazywać kryteria wyboru dostawców sprzętu, oprogramowania oraz usług, oparte o wymogi techniczne i specjalistyczne. Taki kierunek regulacji jest niezbędny dla utrzymania na rynku konkurencyjności, która pozytywnie będzie wpływać na rozwój gospodarczy kraju, nowych technologii a także sieci 5G. Przepisy powinny w najwyższym stopniu zabezpieczać pluralizm podmiotów funkcjonujących na rynku. Takie rozwiązanie daje gwarancje ochrony interesów podmiotów słabszych, a więc konsumentów, z drugiej zaś strony ma przełożenie na konkurencyjność i stan gospodarki. Niewątpliwie, z uwagi na wagę regulacji, powinno się jak najszerzej rozpatrywać skutki jakie może ona nieść dla rynku. Wybór dostawców oparty o niejasne kryteria, jak wskazano wyżej, może spowodować nie tylko ograniczenie konkurencyjności i co się z tym wiąże opóźnienia we wdrożeniu sieci 5G, ale także, w przypadku wydania wobec dostawcy oceny określającej wysokie ryzyko oraz idący za tym zakaz wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania przez podmioty krajowego systemu cyberbezpieczeństwa, kosztów związanych z wycofaniem. Dlatego też projektowane przepisy powinny być redagowane w sposób jasny i precyzyjny po dokonaniu wnikliwej i wszechstronnej analizy skutków regulacji. Liczymy, iż nasze uwagi zostaną wzięte pod rozwagę i będą pomocne dla dalszego procedowania projektu.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

152.	Mobile Logic	Uwaga ogólna	Niestety proponowane przepisy wydają nam się być nie do przyjęcia. Ich wdrożenie wywoła negatywne skutki zarówno dla gospodarki kraju jak i samych obywateli. Spowoduje to zahamowanie rozwoju sieci 5G, która dobrze działa w rozwiniętych technologicznie krajach zachodnich. Polska chcąc być partnerem biznesowym na arenie międzynarodowej powinna nadążać za digitalowym rozwojem Europy i nadążać za wprowadzanymi trendami. Przyjęcie przepisów w aktualnym brzmienie wywoła opóźnienie wprowadzenia i rozwoju sieci 5G o co najmniej kilka lat, co w dobie technologicznego pędu będzie nie do nadrobienia. Ponadto bez wątpienia polska gospodarka straci w oczach zagranicznych inwestorów, którzy zostaną bezpośrednio dotknięci niniejszą regulacją oraz stracą zaufanie, być może poczują się także dyskryminowani, a samo ograniczenie wywoła w Polsce brak konkurencji co może powodować wzrost kosztów dla usług telekomunikacyjnych, co odbije się także na konsumentach.	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

153.	Mobile Logic	Uwaga ogólna	Przepisy ustawy nie są jasne, chociażby w zakresie kryteriów oceny ryzyka, co powodować będzie w przyszłości wiele zamieszania, sporów i niedomówień o wysoce kosztownych skutkach Niezapewnienie stronom zainteresowanym możliwości wniesienia odwołania od oceny ryzyka jest niezgodne z przepisami konstytucji oraz postępowania administracyjnego i wymagają bezwzględnej zmiany. Terminy jakie projekt ustawy nakłada na przedsiębiorców są przez nich niemożliwe do dochowania. Działania jakich się od nich wymaga są długoterminowe oraz niezwykle kosztowne. Niemożliwym jest całkowite przeorganizowanie sieci w terminie pięciu lat z jednoczesnym zachowaniem jej stabilnego funkcjonowania Ponadto w ustawie nie ma słowa o tym kto pokryje związane z ww. zmianami koszty. Jeśli zrobić będą to mieli sami operatorzy związane to będzie zapewne z podniesieniem ceny oferowanych przez nich usług. Zapłacą więc konsumenci. Zasadnym jest zatem aby operatorzy dotknięci obowiązkiem wprowadzenia zmian w związku z wejściem w życie nowych przepisów otrzymali odszkodowanie pokryte z budżetu państwa Projekt ustawy jak mam nadzieję Państwo zauważą spotyka się z wieloma kontrowersjami, a co za tym idzie wymagane jest jego poprawienie i dostosowanie do realiów oraz gospodarki. Na chwilę obecną wywołać on może wiele szkodliwych i trudnych w usunięciu skutków	Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

154.	Mobilne Miasto	Uwaga ogólna	**POSTULAT RZETELNYCH KONSULTACJI SPOŁECZNYCH** Termin konsultacji społecznych należy zdecydowanie przedłużyć, z uwagi na wskazaną wyżej, a także w naszym piśmie z dnia 15.09.2020 r. wagę dokumentu, do 45 dni. Należałoby przy tym przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców, organizacje konsumentów, instytucje odpowiedzialne za ochronę konkurencji i konsumenta, Radę Dialogu Społecznego. **POSTULAT ZORGANIZOWANIA KONFERENCJI UZGODNIENIOWEJ ORAZ WCZEŚNIEJSZEGO WYSŁUCHANIA PUBLICZNEGO** Zgodnie z § 44 Regulamin pracy Rady Ministrów, zwracamy się z uprzejmą prośbą o zorganizowanie przez Ministerstwo Cyfryzacji konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi, gdyż z pewnością przyczyniłaby się ona do właściwego prowadzenia uzgodnień i zaopiniowania projektu ustawy. **POSTULAT RZETELNEJ ANALIZY SKUTKÓW SPOŁECZNYCH, GOSPODARCZYCH I POLITYCZNYCH ORAZ POKAZANIA W OCENIE SKUTKÓW REGULACJI WYNIKAJĄCYCH Z TEGO PEŁNYCH KOSZTÓW REGULACJI** W zakresie skutków społecznych należałoby opisać wpływ projektowanych przepisów na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług (w tym usług mobilności, do których zarejestrowanych jest ok. 4 milionów Polaków), wzrost	**Uwwaga nieuwzględnioana** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: nie tylko w obszarze, transportu i mobilności, ale także w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce. **PROPONOWANY KIERUNEK ZMIAN** Rynek usług łączności elektronicznej powinien wg nas nadal pozostać kompleksowo regulowany sektorowe, ze względu na jego szczególne cechy. Dlatego uważamy, że docelowym miejscem uregulowania kwestii obowiązków operatorów telekomunikacyjnych w zakresie bezpieczeństwa sieci i usług jest projektowana ustawa Prawo Komunikacji Elektronicznej (PKE),. Należałoby więc pozostawić kompetencje Prezesa UKE uregulowane w art. 39-49 projektu PKE. Model przedstawiony w PKE zapewnia bowiem szereg narzędzi pozwalających zapewnić cyberbezpieczeństwo infrastruktury telekomunikacyjnej	

155.	Nanocoder	Uwaga ogólna	Niniejszym pismem chciałbym wyrazić swoją opinię względem projektu o krajowym systemie cyberbezpieczeństwa. Nie ukrywam, że proponowany projekt wywołuje we mnie ogromne oburzenie i moim zdaniem jest nie do zaakceptowania w proponowanej formie. Nie dość, że koliduje on z przepisami prawa polskiego, prawa unijnego to także jest niezwykle niekorzystny dla przedsiębiorców działających na terenie naszego kraju oraz dla pozostałych obywateli, występujących w roli konsumentów. Przede wszystkim warto zaznaczyć, że KSC jest transpozycją dyrektywy NIS w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, która nie ma zastosowania do operatorów telekomunikacyjnych. Ich prawa i obowiązki zostały szczegółowo określone w prawie telekomunikacyjnym poprzez przyjęcie kodeksu komunikacji elektronicznej. W związku z tym dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do którego stosuje się KSC, powoduje nakładanie się i potencjalny konflikt w przepisach. Przepisy komunikacji elektronicznej zawierają już kompleksowe wymagania wobec operatorów telekomunikacyjnych. Przyjęcie przepisów ustawy w takiej formie spotka się bez wątpienia z ogromnym niezadowoleniem społeczeństwa oraz wywrze negatywne skutki w branży telekomunikacyjnej, które odczują także konsumenci. W związku z powyższym liczę, że Ministerstwo Cyfryzacji szczegółowo zapozna się z wyrażoną opinią społeczeństwa i zdecyduje o naniesieniu niezbędnych zmian do projektu ustawy.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

156.	NeuroGames Lab	Uwaga ogólna	Odbieram ze znacznym niepokojem planowaną nowelizację przepisów ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych i w związku z tym chcę skorzystać z możliwości związanych z prowadzonymi konsultacjami społecznymi projektu ustawy. Propozycje umieszczone w projekcie odbieram jako bezpośredni atak na operatorów telekomunikacyjnych w Polsce, który pośrednio odbije się także na sytuacji wszystkich ich abonentów. Po pierwsze olbrzymie koszty po stronie operatorów telekomunikacyjnych zostaną wygenerowane wprowadzeniem przepisów art. 66b, zakazujących użytkowania sprzętu lub oprogramowania pochodzącego od dostawców obarczonych oceną średniego i wysokiego ryzyka oraz w przypadku wysokiego ryzyka także nakazujących ich wycofanie w ciągu 5 lat od ogłoszenia komunikatu o takiej ocenie. Koszty wymiany sprzętu ostatecznie poniosą oczywiście abonenci. Przyjęcie rozwiązań proponowanych w nowelizacji ustawy przez operatorów spowoduje ich zmuszenie do wymiany posiadanej infrastruktury, pomimo że nie ponoszą przecież żadnej winy za podejmowane na etapie zakupu wynagrodzenia decyzje biznesowe dotyczące wyboru dostawców. Koszty te powinny zostać poniesione przez Skarb Państwa. W innym wypadku mówimy o jawnym pogwałceniu prawa własności i niejako wywłaszczeniu wcześniej zakupionego przez tych operatorów sprzętu. Poniosą oni nie tylko koszty zakupu nowego sprzętu, które nie byłyby konieczne w dotychczasowym stanie prawnym, ale także dodatkowe koszty związane z wycofaniem starego sprzętu. Dlatego konieczne jest wprowadzenie mechanizmu rekompensującego operatorom koszty poniesione w związku z wymianą sprzętu lub oprogramowania obarczonego wysokim ryzykiem. Rekompensata	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			ta powinna być wypłacona w wysokości, która pokryje wydatki poniesione w związku z zakupem odpowiedniego sprzętu lub oprogramowana, koszty amortyzacji i wydatków związanych z wycofaniem z użycia dotychczasowego wyposażenia	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
157.	NeuroGames Lab	Uwaga ogólna	Po drugie zdecydowanie za krótki jest przewidziany w art. 66b ustawy 5-letni okres na wycofanie z użytkowania sprzętu, oprogramowania i usług świadczonych przez dostawcę, którego ryzyko oceniono jako wysokie. Decyzje o inwestycji w sprzęt i oprogramowanie są podejmowane w wieloletniej perspektywie i aby umożliwić amortyzację poniesionych kosztów. Projektowany obowiązek wycofania sprzętu z użytkowania mniej dotkliwie dotknie operatorów komunikacyjnych, którzy zakupili sprzęt wiele lat wcześniej, niż tych, którzy dokonali inwestycji krótko	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W

			przed ogłoszeniem komunikatu o wysokim ryzyku danego dostawcy. Te różnice z jednej strony powinny zostać uwzględnione przy udzielaniu rekompensat (których aktualnie projekt ustawy w ogóle nie przewiduje, o czym mowa powyżej), a z drugiej powinny wpłynąć na wydłużenie okresu na wycofanie z użytkowania sprzętu, oprogramowania i usług świadczonych przez dostawcę do lat 10. Z tych samym względów powinien również zostać wydłużony (do 1 roku) jeszcze bardziej nierealistyczny zakładany przez art. 66c ustawy 3-miesięczy termin na sporządzenie i dostarczenie planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Mam nadzieję, że Ministerstwo ponownie rozważy potencjalny wpływ projektowanych rozwiązań na koszty prowadzenia działalności gospodarczej w Polsce oraz dodatkowe koszty, którymi w ich rezultacie zostaną obarczeni abonenci i wypracuje modeł, który nie będzie za sobą niósł tak szkodliwych gospodarczo konsekwencji.	ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub

				oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
158.	SmartWeb Media	Uwaga ogólna	Szczególne wątpliwości budzi przedstawiony w Projekcie mechanizm dokonywania oceny ryzyka dostawcy sprzętu lub	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione.

			oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Zgodnie z dodawanym Projektem art. 66a ustawy o krajowym systemie cyberbezpieczeństwa, ocena ta dokonywana jest przez Kolegium w oparciu o otwarty katalog kryteriów przedstawionych w ust. 4 projektowanego art. 66a tejże ustawy. Kryteria te opierają się o kryteria, które można podzielić na: 1) zewnętrzne - tj. analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, jego powiązania z państwami spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, a także zdolność ingerencji w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania oraz ich prawodawstwo tych państw w zakresie ochrony danych osobowych, 2) wewnętrzne - związane ze strukturą własnościową dostawcy sprzętu lub oprogramowania oraz stopniem sprawowanego nadzoru nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania 3)administracyjne — związane z liczbą i rodzajem oraz sposobem i czasem eliminowania wykrytych podatności i incydentów oraz treścią wydanych wcześniej rekomendacji, dotyczących sprzętu lub oprogramowania danego dostawcy. Analiza przedstawionych kryteriów prowadzi do wniosku, że kryteria te trudno określić jako przejrzyste i wymierne. Opierają się one m.in. o czynniki nietechniczne, zewnętrzne, związane z zależnościami politycznymi między dostawcą a jego krajem pochodzenia oraz otoczeniem regulacyjnym, w którym dany	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

			dostawca funkcjonuje, co stanowi jawną dyskryminację dostawców ze względu na pochodzenie. Kryteria te nie przedstawiają jednolitych standardów technicznych, lecz subiektywne przesłanki, które mają decydować o wyborze dostawcy. Rozwiązanie to zdecydowanie odbiega od standardów przyjętych w innych państwach Unii Europejskiej stosujących transparentne i techniczne standardy cyberbezpieczeństwa oraz systemy certyfikacji sprzętu oraz oprogramowania. W związku z powyższym, sugerujemy zastąpienie projektowanych kryteriów oceny zobiektywizowanymi przesłankami technicznymi, opierającymi się o przestrzeganie międzynarodowych lub uznawanych w UE standardów cyberbezpieczeństwa, np. IS027001, Wspólne Kryteria, Network Equipment Security Scheme, EU Cybersecurity Certification Scheme, certyfikację sprzętu oraz monitoring bezpieczeństwa. Niezależnie od przedstawionych powyżej wątpliwości związanych z metodologią oceny ryzyka, dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, niepokój wzbudza już sama procedura administracyjna związana z procesem dokonywania tejże oceny, sprzeczna z fundamentalnymi zasadami postępowania administracyjnego wyrażonymi w ustawie z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego **(„k.p.a.”),** w szczególności z art. 10 k.p.a. wprowadzającym zasadę czynnego udziału strony w postępowaniu. Projektowane regulacje nie przewidują możliwości udziału poddawanego ocenie dostawcy w postępowaniu, który (zgodnie z obecnym brzmieniem projektowanych przepisów) dowiaduje się o sporządzonej przez	W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			Kolegium ocenie ryzyka za pośrednictwem ogłoszonego przez Pełnomocnika komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Należy zatem zapewnić poddawanemu ocenie dostawcy aktywny udział w postępowaniu ocennym na każdym jego etapie. Co więcej, zgodnie z art. 15 k.p.a., postępowanie administracyjne jest dwuinstancyjne, chyba że przepis szczególny stanowi inaczej. W tym kontekście uzasadnione wątpliwości budzi projektowany art. 66a ust. 8 zd. pierwsze ustawy o krajowym systemie cyberbezpieczeństwa, który zawęża możliwość odwołania się od oceny sporządzonej przez Kolegium wyłącznie w przypadku uzyskania oceny określającej ryzyko jako wysokie. W świetle konstytucyjnej zasady równości wobec prawa, ocena określająca ryzyko jako średnie i niskie również powinna upoważniać dostawcę do wniesienia odwołania. Przepisy dotyczące wniesienia sprzeciwu do sądu administracyjnego powinny być stosowane odpowiednio.	
159.	TELDATA	Uwaga ogólna	Jako firma będąca w pełni zaangażowana w rozwój branży ICT oraz mająca swój wkład w rozwój technologiczny Polski, czujemy się się zaniepokojeni Projektem Ustawy, który może mieć negatywny wpływ zarówno na naszą firmę, jak i pokrewne branże związane z rynkiem ICT. Zdajemy sobie sprawę, że Rząd dokłada wszelkich starań, aby poprawić cyberbezpieczeństwo kraju, jednak Projekt Ustawy zawiera kryteria, które z pewnością nie będą sprzyjały konkurencyjności na rynku, ze względu na możliwość wpływu na przedsiębiorców poprzez ograniczanie zakresu prowadzenia ich działalności. Zapisy proponowane w Projekcie wpłyną zatem negatywnie na zatrudnienie i rozwój branży telekomunikacyjnej,	**Wyjasnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę

			co w konsekwencji może opóźnić proces cyfryzacji w Polsce. Naszym zdaniem, aby poprawić cyberbezpieczeństwo polskich sieci, warto wziąć pod uwagę ustalenie obiektywnych i jasnych kryteriów oceny ryzyka, opierając się na zasadzie transparentności oraz upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe. Warto rozważyć ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, który obowiązywałby dla wszystkich, niezależnie od kraju pochodzenia. Wierzymy, że takie podejście wpłynęłoby na zwiększenie poziomu cyberbezpieczeństwa w Polsce. Proponujemy, aby Ministerstwo Cyfryzacji zorganizowało otwartą debatę i zaprosiło zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w Projekcie. Rząd powinien w pełni ocenić wpływ Projektu, w tym koszty i straty, konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce. Wyrażamy nadzieję, że nasza opinia zostanie wzięta pod uwagę	wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność

				ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

160.	TEP Doradztwo Biznesowe	Uwaga ogólna	Jako jeden z podmiotów szczególnie zainteresowanych nowymi regulacjami chcieliśmy wyrazić swoje obawy w kilku kwestiach, takich jak choćby: **1.** naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów; **2.** wpływanie przez Kolegium w sposób niejasny i bez szczegółowych wytycznych (technicznych) na podmioty w branży; **3.** pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko; **4.** Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania **Naruszanie przez projekt zasad uczciwej konkurencji i równego traktowania podmiotów.** Polski rynek jest obecnie jednym z najbardziej atrakcyjnych przestrzeni inwestycyjnych dla branży. Dzisiaj jesteśmy państwem, z którym handluje się w sposób wolny i przejrzysty, mamy przepisy gwarantujące inwestorom uczciwą konkurencję, wolny rynek i sprawiedliwe traktowanie. Proponowany kształt nowych przepisów znacząco wpływa na te atuty, które stanowią podstawowe przymioty w każdym demokratycznym państwie. Zagraniczny kapitał jest bardzo wrażliwy na tego rodzaju regulacje. Jesteśmy pewni, że w przypadku wprowadzenia przepisów w proponowanym kształcie przełożą się	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			one na rozwój zarówno polskiego przemysłu, sektora usług ale także na życie polskich obywateli **Wpływanie przez Kolegium** w sposób niejasny oraz bez szczegółowych wytycznych (technicznych) na podmioty w branży. W myśl projektu Kolegium dostałoby bardzo szerokie, niejasne, niekontrolowane przez żaden zewnętrzny podmiot uprawnienia do wpływania na konkretnego dostawcę. To z kolei w dalszej kolejności przekłada się na inne podmioty gospodarcze, a na samym końcu na konsumenta. Postępowanie które pozbawia prawa do możliwości składania wyjaśnień wydaje się wysoce niesprawiedliwe. Natomiast pozbawienie możliwości odwołania (w niektórych przypadkach) zgodnie z przepisami KPA wyraźnie narusza porządek prawny oraz zasady równego traktowania zagwarantowane w Konstytucji. Proponowane przepisy stworzą potencjalne ryzyko wpływania w sposób nieuczciwy i niezgodny z prawem na podejmujących decyzję w sprawie oceny. Powstanie szczegółowych wytycznych-jasnych, obiektywnych kryteriów oceny powinno zminimalizować to ryzyko. **Pozbawienie prawa do odwołania od decyzji Kolegium w przypadku ocen określających średnie i niskie ryzyko.** Każdy podmiot - zarówno w przypadku oceny określającej wysokie ryzyko, jak i ocen określających średnie i niskie ryzyko - powinien mieć takie same możliwości odwoławcze od oceny. Blokowanie możliwości odwoławczych niektórych z nich wpływa przede wszystkim na równość podmiotów względem innych. Każdy zasługuje na możliwość odwołania od oceny, która w założeniu nowych przepisów ma się odbywać bez udziału zainteresowanego podmiotu. Odwołanie powinno zawieszać postępowanie do czasu wydania prawomocnego wyroku w sprawie przez sąd powszechny w myśl przepisów KPA. Taki stan rzeczy byłby w sposób oczywisty najbardziej sprawiedliwy.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

			Relatywnie krótki termin wycofania z rynku sprzętu, oprogramowania i usług w przypadku wydania niekorzystnej oceny przez Kolegium oraz wysokie koszty wycofywania z rynku sprzętu i oprogramowania. Pięcioletni termin wycofania z rynku jest bardzo krótkim terminem na wycofanie z rynku całego sprzętu, oprogramowania i usługi z rynku. Proponujemy termin 10-cio letni, który jest dużo bardziej adekwatny do sytuacji. Należy pamiętać o tym, że operatorzy poniosą również gigantyczne koszty związane wprost z nowymi przepisami i w żaden sposób przez siebie nie zawinione. Dlatego też rząd powinien wprowadzić rekompensaty dla tych podmiotów, które takie koszty będą musiały ponieść. Oczywistym jest, że każdy podmiot który poniesie takie straty będzie szukał możliwości ich odrobienia. To z kolei wprost przełoży się na ceny usług dla końcowego odbiorcy, czyli obywatela. Sam termin 5-cio letni jest tak krótki, że może również wpłynąć na stabilność sieci, która będzie miała również szeroko idące konsekwencje.	do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

161.	TILT	Uwaga ogólna	Martwimy się, że ocenianie dostawców na podstawie nietechnicznych czynników nie zapewni zwiększenia poziomu cyberbezpieczeństwa w Polsce, a co więcej, wpłynie negatywnie na zatrudnienie i rozwój branży ICT. W związku z powyższym, w celu zapewnienia obiektywnych standardów, sugerujemy wprowadzenie ściśle określonych wymogów technicznych dotyczących sprzętu w kluczowych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju pochodzenia. Uważamy, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa w Polsce. Sugerujemy przeprowadzić pełną analizę skutków płynących z Projektu nowelizacji ustawy oraz konsultacji społecznych, co pozwoliłoby obywatelom brać aktywny udział w debatach dotyczących ich rzeczywistych interesów, a także pozwoliłoby Ministerstwu na opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną i bezpośrednio na społeczeństwo. Dziękujemy za wysłuchanie naszych opinii.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

162.	Związek Cyfrowa Polska	Uwaga ogólna Uwaga ogólna	Jako Związek Cyfrowa Polska wyrażamy poparcie dla nowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa (dalej: projekt UKSC). Jest ona potrzebna i wyczekiwana przez rynek cyfrowy i nowoczesnych technologii. Cyberbezpieczeństwo musi stać się najważniejszym elementem cyfrowej gospodarki, a bez jednoznacznych, jasno sprecyzowanych regulacji prawnych byłoby to niemożliwe. Niewątpliwie należy pamiętać, że mówiąc o cyberbezpieczeństwie nie wskazujemy interesu jednego czy innego dostawcy usług, ale całościowo określamy bezpieczeństwo narodowe. I właśnie z tej perspektywy należy ocenić narzędzia, jakie daje nowelizacja ustawy dla cyberbezpieczeństwa kraju. Jest to dziś tym bardziej istotne, że w perspektywie czeka nas wdrożenie sieci piątej generacji, która zmieni funkcjonowanie całego rynku nowoczesnych technologii i która da nowe możliwości do rozwoju innowacji. Jednak by w pełni wykorzystać dobrodziejstwa, jakie przyniesie sieć 5G, trzeba przede wszystkim zadbać o jej właściwą cyfrową ochronę, które przełoży się na bezpieczeństwo i konkurencyjność polskiej gospodarki. **Mając na uwadze cyberbezpieczeństwo oraz szeroki rozwój sieci 5G w Polsce Związek Cyfrowa Polska za najbardziej pożądany model budowy sieci uznaje ten, w którym w maksymalnym stopniu wykorzystany zostanie potencjał polskich firm i działających w Polsce firm światowych vendorów, ośrodków B&R, fabryk, zatrudnionych inżynierów, w tym opowiada się za szerokim wykorzystaniem technologii Open RAN -** rozwiązanie to jest bardziej efektywne, które może obniżyć koszty wykorzystania technologii przez przedsiębiorców i administrację publiczną we wdrażaniu sieci 5G. **Popieramy również to, że projekt UKSC uwzględnia unijne narzędzia 5G Toolbox, które mają za zadanie ograniczenie cyber-ryzyk dla europejskich sieci 5G.** Rozumiemy, że dla utrzymania cyberbezpieczeństwa dla rynku telekomunikacyjnego i komunikacji elektronicznej, Ustawa musi dawać instrumenty, które pozwalają państwu na eliminowanie z obrotu rozwiązań zarówno sprzętowych jak i oprogramowania stanowiące zagrożenia dla bezpieczeństwa państwa, przedsiębiorców, jak i obywateli. Uważamy, że metoda regulacji oparta na analizie ryzyk i wykorzystująca wspólne instrumenty Unii Europejskiej z tzw. Toolbox 5 G jest właściwa - projektowane w art. 66 a-c rozwiązanie bazuje na podmiotowej ocenie ryzyka, która odbywa się przez pryzmat dostawcy sprzętu lub	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność

163.	Signum Edward Kuś Marcin Kuś	Uwaga ogólna	Po zapoznaniu się z tym projektem stwierdzamy, że proponowane zmiany nie przyniosą pozytywnych skutków dla bezpieczeństwa cybernetycznego w Polsce. Poniżej wskazujemy na braki zaproponowanych w Projekcie przepisów: 1. **Naruszenie zasad uczciwej konkurencji:, Jeśli** zostanie przyjęty, Projekt nada Kolegium prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie będzie sprzyjać konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie ich liczby do jednego, spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży. 2. **Wyraźna dyskryminacja:** Kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne, takie jak relacje między dostawcą a ich krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i możliwości kraju macierzystego dotyczące ingerencji w działania dostawców. 3. **Projekt wyraźnie dyskryminuje dostawców z niektórych regionów:** Kryteria oceny ryzyka dostawcy to jedynie czynniki nietechniczne, w tym związek między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystego, struktura własności dostawcy i możliwości kraju macierzystego w ingerowanie w działania dostawców. **4. Brak technicznych kryteriów oceny:** Rząd będzie podejmował interwencje w zakresie wyboru dostawcy, wskazując na dostawców wysokiego/ średniego ryzyka, zamiast ustanowić jednolite standardy techniczne i wskazać sprzęt objęty nowymi	**Wyjasnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			regulacjami. Operatorzy będą zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego / średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat. 5. **Brak metod weryfikacji bezpieczeństwa cybernetycznego:** Projekt nic zawiera wystarczających środków do weryfikacji bezpieczeństwa cybernetycznego, aby zapewnić bezpieczeństwo i niezawodność sieci w czasie rzeczywistym. 6 **Opóźnienie we wdrożeniu 5G wpłynie na wyniki gospodarcze i zatrudnienie:** Według badania przeprowadzonego przez Komisję Europejską szacuje się, że ie5G zapewni łącznie 141 miliardów euro i 2,3 miliona miejsc pracy w 27 państwach członkowskich Unii Europejskiej. 7. **Projekt ogranicza dywersyfikację technologii i przyszły rozwój:** Każdy sprzedawca samodzielnie ocenia rynek i wyznacza własny kierunek rozwoju. Daje to nieograniczony potencjał dywersyfikacji technologicznej i przyczynia się do przyszłego rozwoju branży. =Wykluczenie jednego z najważniejszych dostawców będzie miało negatywny wpływ na badania naukowe w Polsce, różnorodność technologii i przyszły rozwój. Podsumowując, przyjęcie Projektu nie wpłynie pozytywnie na bezpieczeństwo cybernetyczne w Polsce.	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
164.	Signum Edward Kuś Marcin Kuś	Uwaga ogólna	W odpowiedzi na problemy wkazane powyżej, proponujemy, co następuje: 1. Należy przestrzegać unijnego zestawu narzędzi 5G (5G EU toolbox), nieskierowanego do określonych krajów lub dostawców oraz przyjąć ujednolicone standardy techniczne i weryfikacyjne. 2. Cyberbezpieczeństwem w zakresie 5G należy zarządzać za pomocą jasnych specyfikacji technicznych i ujednoliconych standardów, a niewykluczać dostawców z określonych krajów. Model większości krajów UE, takich jak Niemcy, na którym można się z powodzeniem wzorować, to standard bezpieczeństwa cybernetycznego opracowany przez Federalną Agencję Bezpieczeństwa Informacji (BSI) oraz plan zapewnienia bezpieczeństwa sprzętu sieciowego (NESAS) opracowany przez GSMA, zgodnie, z którymi wszyscy dostawcy są traktowani jednakowo. 3. Należy przyjąć kompromisowe (hierarchiczne) rozwiązanie w kwestii zarządzania bezpieczeństwem cybernetycznym i ograniczenie do elementów krytycznych (sieć rdzeniowa), odwołując się do definicji unijnego zestawu narzędzi 5G. Stacje bazowe 5G nie są komponentami podstawowymi, więc nie wymagają żadnych ograniczeń. a)Model niemiecki: Przyjęcie NESAS, opracowanego przez GSMA, jako standard bezpieczeństwa cybernetycznego; certyfikowanie sprzętu wszystkich dostawców oraz przyjęcie strategii wielu dostawców. b) Model w Szwecji i Finlandii: operatorzy zarządzają bezpieczeństwem cybernetycznym, przyjmują strategię wielu	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji.

			dostawców i dokonują przeglądu podstawowych komponentów sieci. 4. Należy przeprowadzić pełną analizę skutków płynących z projektu nowelizacji ustawy oraz konsultacji publicznych. 5. Należy wysłuchać zdecydowanego sprzeciwu ze strony branży teleinformatycznej i opinii publicznej wobec projektu, zaangażować ekspertów w celu pełnego przedstawienia Projektu, zorganizować debatę i wysłuchać opinii wszystkich stron. 6. Należy zmienić przepisy dyskryminujące ze względu na kraj pochodzenia danego dostawcy na przepisy, które będą zgodne z prawem konkurencji UE i zasadami WTO. Należy ustanowić prawa i regulacje sprzyjające cyfrowej przyszłości kraju, wolnej konkurencji operatorów i wysokiej, jakości usług sieciowych dla obywateli kraju.	Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub

				oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
165.	PKN Orlen	Uwaga ogólna	1.1 W pierwszej kolejności PKN wskazuje na potrzebę przyznania organowi właściwemu do spraw cyberbezpieczeństwa w rozumieniu *Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 2018r. poz. 1560 - dalej jako **„Ustawa o KSC")** prawa do ustanowienia *„CSIRT grupy kapitałowej"* czyli *„Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego w **ramach oraz na poziomie** grupy kapitałowej ustanowionego przez organ właściwy do spraw cyberbezpieczeństwa."* 1.2 Powyższe prawo w/w organu do ustanowienia *„CSIRT grupy kapitałowej"* dotyczyłoby takich grup kapitałowych, do których należy **więcej niż jeden operator usługi kluczowej** z określonego sektora. W konsekwencji *„CSIRT grupy kapitałowej"* zachowałby swój sektorowy charakter z tym jednak zastrzeżeniem, że posiadałby **status równorzędny** wobec *„CSIRT-ów sektorowych"* w rozumieniu Projektu. Szczegółowe propozycje wybranych zmian w Projekcie dotyczące powyższego zagadnienia zawarto w **Tabeli numer 1 poniżej.** 1.3 Uzasadnieniem powyższego jest sposób funkcjonowania dużych i strategicznych Grup Kapitałowych:	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.

			1.3.1 wspólna infrastruktura wymuszająca efektywne zarządzanie incydentami, możliwe wyłącznie dzięki scentralizowanemu zarządzaniu cyberbezpieczeństwem, 1.3.2 posiadanie niezbędnych zasobów ludzkich i technicznych do skutecznego, centralnego zarządzania cyberbezpieczeństwem Grupy Kapitałowej, w tym realizacji zadań CSIRT 1.4 W myśl powyższej koncepcji organ właściwy do spraw cyberbezpieczeństwa zapewniałby funkcjonowanie *„CSIRT sektorowego”* dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do Ustawy o KSC (zgodnie z Projektem), a dodatkowo byłby uprawniony ustanowić *„CSIRT grupy kapitałowej*". Organ właściwy do spraw cyberbezpieczeństwa mógłby powierzyć realizację zadań: 1.4.1 *„CSIRT sektorowego”* m.in. jednostkom podległym lub nadzorowanym (zgodnie z Projektem), a także 1.4.2 *„CSIRT grupy kapitałowej*" temu podmiotowi danej grupy kapitałowej, który spełnia warunki, o których mowa w projektowanym art. 44 ust. 6 Projektu, a także po zasięgnięciu opinii Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. 1.5 Ponadto, w myśl preambuły do *Dyrektywy NIS: „(...) Państwa członkowskie* ***powinny zatem zapewnić dobrze funkcjonujące*** *CSIRT, zwane również zespołami reagowania na*	

			incydenty komputerowe (zwane dalej „CERT"), które spełniają zasadnicze wymogi w celu zagwarantowania efektywnych i kompatybilnych zdolności w zakresie postępowania z incydentami i ryzykiem oraz zapewnienia skutecznej współpracy na poziomie Unii (...)" **(motyw 34)** oraz *„Odpowiedzialność za zapewnienie bezpieczeństwa sieci i systemów informatycznych* ***w dużym stopniu spoczywa na operatorach usług kluczowych*** **(motyw 44).**	
166.	Skandynawsko-Polska Izba Gospodarcza	Uwaga ogólna	Wyrażamy poparcie dla wprowadzenia do polskiego prawodawstwa opracowanego przez państwa członkowskie EU unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G ("5G Toolbox"), zgodnie z propozycją zawartą w projekcie ustawy z dnia 7. września 2020 roku o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Wraz ze zmianami technologicznymi będącymi konsekwencjami wprowadzenia sieci 5G i możliwościami rozwoju tej technologii w szerokim obszarze zastosowań, jak przemysł ochrona zdrowia, telekomunikacja, transport, wzrosną zagrożenia i poszerzy się pole do ataków cybernetycznych. Naszym zdaniem proponowana zmiana ustawy o krajowym systemie cyberbezpieczeństwa i wdrożenie unijnego zestawu narzędzi 5G jest krokiem we właściwym kierunku, co pozwoli na zapewnienie ochrony przedsiębiorstwom i pozwoli za zabezpieczenie ich praw własności intelektualnej. Proponowana zmiana stanowi dobrą odpowiedz na wymóg identyfikacji potencjalnych luk w istniejących ramach legislacyjnych i mechanizmach egzekwowania prawa, w tym roli nadzorczej organów publicznych w zakresie krajowego systemu cyberbezpieczeństwa przed pełnym wprowadzeniem 5G w Polsce.	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

			Oczekując na dalsze procedowanie proponowanego projektu, pragniemy jeszcze raz zaznaczyć, ze projekt w obecnej formie jest krokiem we właściwym kierunku, pozwalającym na zapewnienie bezpiecznego i przewidywalnego środowiska biznesowego przedsiębiorcom stowarzyszonych w naszej organizacji	sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast

				przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
167.	Liquid Systems	Uwaga ogólna	Wiele planowanych zmian narusza zasadę niedyskryminacji i uczciwej konkurencji przedsiębiorstw, co wpłynie negatywnie na branżę ICT. Przyjęcie Projektu w aktualnym brzmieniu oznacza: 1. Naruszenie zasad uczciwej konkurencji: Jeśli nowe przepisy zostaną przyjęte, Kolegium uzyska de facto prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie sprzyja konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie do tylko jednego z nich spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży. 2. Wyraźna dyskryminacja: Kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne, w tym relacje między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i możliwości kraju macierzystego dotyczące ingerencji w działania dostawców. 3. Brak technicznych kryteriów oceny: Rząd ingeruje w wybór dostawcy zamiast ustanowić jednolite standardy techniczne. Nie	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania.

			określa również sprzętu objętego zakresem nowych przepisów. Operatorzy zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego / średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat. 4. Wzrost kosztów budowy sieci zostanie ostatecznie przeniesiony na konsumentów, prowadząc do zastosowania wyższych cen dla usług telekomunikacyjnych. Wyłączanie dostawców doprowadzi do zniesienia konkurencji, zwiększając koszty zaopatrzenia operatorów, co z kolei będzie prowadzi to do wyższych cen usług telefonii komórkowej dla użytkowników. Koszty budowy infrastruktury IT dla rządów i przedsiębiorstw mogą znacznie wzrosnąć. Na przykład, brytyjskie media podały, ze po wykluczeniu Huawei koszt budowy sieci w Wielkiej Brytanii wzrósł o 30%.Taryfy w Polsce są obecnie jednymi unijnego zestawu narzędzi 5G. Stacje bazowe 5G nie są komponentami podstawowymi, więc nie wymagają żadnych ograniczeń. a) Model niemiecki: Przyjcie NESAS, opracowanego przez GSMA jako standard bezpieczeństwa cybernetycznego; certyfikowanie sprzętu wszystkich dostawców oraz przyjęcie strategii wielu dostawców. b) Model w Szwecji i Finlandii: operatorzy zarządzają bezpieczeństwem cybernetycznym, przyjmują strategię wielu dostawców i dokonują przeglądu podstawowych komponentów sieci. 5. Należy przeprowadzić pełną analizę skutków płynących z projektu nowelizacji ustawy oraz konsultacji publicznych.	Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

			6. Należy wysłuchać zdecydowanego sprzeciwu ze strony branży teleinformatycznej i opinii publicznej wobec Projektu, zaangażować ekspertów w celu pełnego przedstawienia Projektu, zorganizować debaty i wysłuchać opinii wszystkich stron. 7. Należy zmienić przepisy dyskryminujące kraj pochodzenia danego dostawcy na klauzule 0 niedyskryminacji, zgodnie z prawem konkurencji UE i zasadami WTO. Należy ustanowić prawa i regulacje sprzyjające cyfrowej przyszłości kraju, wolnej konkurencji operatorów i wysokiej jakości usług sieciowych dla obywateli kraju.	Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

168.	Instytut Staszica	Uwaga ogólna	Projekt może naruszać istotne regulacje unijne, a co za tym idzie – być powodem do kolejnego sporu między polskim rządem a Komisją Europejską. Jest kwestią oczywistą, która nie powinna budzić sporów niezależnie od partyjnych barw, że priorytetem jest budowa w naszym kraju możliwie najnowocześniejszego systemu komunikacji na możliwie najbardziej dogodnych warunkach. Te warunki to nie tylko kwestie finansowe, ale także szczegóły związane z obsługą systemu, dostępem do kolejnych, nowych rozwiązań, które pojawią się w następnych latach, możliwość rozwijania przez polskie firmy współpracy z dostawcą technologii. Telekomunikacja, a zwłaszcza technologia 5G, stanowią fundament cyfrowej transformacji oraz ścieżkę powrotu do ożywienia gospodarczego, w szczególności w kontekście aktualnej sytuacji epidemicznej. Sprawne wdrożenie sieci 5G w Polsce może stanowić istotny potencjał gospodarczy w ciągu najbliższych kilku lat. Bez wątpienia jest to czynnik napędzający konkurencyjność i innowacyjność państwa na arenie międzynarodowej, zrównoważony rozwój i transformację cyfrową. Niezależnie od tego, czy jest to transport, energetyka, opieka zdrowotna czy rolnictwo, technologia 5G położy podwaliny pod zieloną i cyfrową transformację gospodarki Rzeczypospolitej Nie można udawać, że całe przedsięwzięcie nie ma kontekstu geopolitycznego. Budowa sieci 5G w krajach europejskich odbywa się w cieniu rywalizacji amerykańsko-chińskiej. Sytuacja ta pokazuje, niestety, słabość Europy, która nie jest już podmiotem w takiej rywalizacji, a jedynie przedmiotem zabiegów pozaeuropejskich koncernów. Polska, podejmując kierunkową decyzję w sprawie budowy sieci 5G, musi znaleźć równowagę między interesami gospodarczymi, politycznymi i pozycja w Unii Europejskiej. Jest to niezwykle	**Uwaga nieuwzględniona** Projekt nie narusza przepisów unijnych oraz innych przepisów międzynarodowych. Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie

169.	Transition Software	Uwaga ogólna do PZP	Należy zmodyfikować poniższe artykuły, tj. umieścić w nim jasne i rozwiewające wszelkie wątpliwości zapisy, że postępowania zakupowe prowadzone przez podmioty IK, a dotyczące szczególnie infrastruktury ICT, w tym zwłaszcza systemów bezpieczeństwa, są wyłączone z przepisów Ustawy Pzp. Z jednej strony są napisane wyraźnie, z drugiej strony, praktyka i pragmatyka zamówień publicznych prowadzonych przez ostatnie lata przez instytucje w naszym kraju, pokazują co innego (pełne stosowanie zakupów w formie przetargu nieograniczonego, nadmierna otwartość i informacyjność, nadmiernie szeroka pula potencjalnych wykonawców, nieuzasadniona, nadmierna obawa przed potencjalnymi zarzutami z powodu naruszenia dyscypliny finansów publicznych, etc. etc.). Jest zrozumiałe, że procesy zakupowe IT w dużych jednostkach budżetowych powinny być należycie kontrolowane, gdyż ryzyka zarówno: - zakupu niewłaściwych rozwiązań, niespełniających kryteriów (ustawianie przetargów), - marnotrawstwa środków publicznych, - korupcji, nie są pomijalne, to jednak chęć nadmiernej otwartości wprost powoduje ryzyka dla bezpieczeństwa infrastruktury ICT podmiotu świadczącego usługę kluczową (choćby targetowanie exploitów, spear phishing, celowane ataki APT, skoro stosowana infrastruktura i oprogramowanie jest możliwe do łatwego poznania, etc.). Poprzez bezkrytyczne, nadmiernie przezroczyste stosowanie obowiązującej Ustawy Prawo zamówień publicznych przez piony, departamenty i wydziały odpowiedzialne za procesy zamówień publicznych w jednostkach organizacyjnych podmiotów wchodzących w skład Infrastruktury Krytycznej RP, jest ona w	**Wyjaśnieni** Zrezygnowano z przepisów zmieniających Prawo Zamówień Publicznych

			niewystarczający sposób chroniona przez wypływem informacji dość wrażliwych z punktu widzenia cyberbezpieczeństwa RP, tj. dotyczących stosowanej w podmiotach i obiektach IK infrastruktury ICT, oprogramowania, wersji, systemów bezpieczeństwa, etc. Wg mojej oceny sytuacji prawnej obowiązującej w Polsce, informacje dotyczące infrastruktury ICT - w tym w szczególności systemów bezpieczeństwa - stosowanej w podmiotach wchodzących w skład IK są dalece niewystarczająco chronione, m.in. z poniższych powodów: 1. Najczęściej nie wchodzą w skład systemów przetwarzających informacje niejawne, więc nie są chronione obejmującą je ustawą. 2. Nie są też stricte systemami przetwarzającymi dane osobowe, więc nie obowiązuje je również w wystarczającym stopniu ochrona poprzez zapisy RODO. 3. Nie wszystkie podmioty IK wchodzą w skład wojska, resortów siłowych, służb specjalnych, więc nie obowiązuje je możliwa do zastosowania przez ww. instytucje niemalże domyślna ochrona wszelkich informacji dotyczących ich infrastruktury, możliwości i procedur. 4. Analogicznie j.w. – nie wszystkie podmioty i obiekty IK wchodzą w skład sektorów, więc nie obowiązuje je obszar zamówień sektorowych i pewnej ochrony z nimi związanej. 5. Bardzo często, z obawy przed sankcjami spowodowanymi potencjalnym naruszeniem dyscypliny finansów publicznych, jednostki organizacyjne resortów publicznych, a w szczególności pracownicy i decydenci pionów zamówień publicznych, przeprowadzają	

			wszystkie organizowane przez siebie zamówienia wyłącznie w formie przetargu nieograniczonego. Bardzo często dochodzi do tego nadmierna, swoiście rozumiana chęć zapewnienia wysokiej konkurencyjności rynkowej, która – podczas przeprowadzania procesu zakupowego - często prowadzi do: a) Zaznajamiania się z informacjami dot. zamówienia bardzo szerokiego grona odbiorców (w przypadku przetargu nieograniczonego jest to w zasadzie cały świat, wystarczy znajomość jęz. polskiego, ogłoszenia są publikowane na stronach internetowych); b) Konieczności wypisania/ujawniania wykorzystywanej infrastruktury ICT, w niektórych przypadkach już w ogłoszeniu, w niektórych przypadkach w formie odpowiedzi na zapytania przetargowe, gdyż jest to wymuszone przez zastosowaną formę zakupu, tj. przetarg nieograniczony (pytania są publiczne, odpowiedzi również muszą takie być, więc odpowiedzi są zamieszczane w formie otwartej, na stronach internetowych Zamawiającego lub BIP); c) Uczestnictwie w procesie przetargowym czasem nie do końca wiarygodnych i zweryfikowanych wykonawców, którzy czasami zadają pytania przetargowe w celu ujawnienia wrażliwych z punktu widzenia technologicznego i bezpieczeństwa, informacji dot. stosowanej u Zamawiającego infrastruktury. d) Braku możliwości ograniczania proponowanych rozwiązań ICT (a zwłaszcza rozwiązań i systemów bezpieczeństwa), z powodu np. ujawnionych, ogólnie znanych doniesień medialnych nt. potencjalnie	

			niepożądanych powiązań produkujących je firm, wątpliwości dot. faktycznej wydajności lub stopnia zabezpieczeń, etc. zwłaszcza, jeżeli wg. dokumentacji produktowej, rozwiązania te spełniają wymogi, etc. e) Dodatkowo to zjawisko jest wzmagane przez bezkrytyczny trend stosowania w znaczącej wadze kryterium ceny, do wyliczenia ostatecznej wyceny rozwiązania. Reputacja producenta produktu, jego uczestnictwo w UE, NATO, etc. nie ma najmniejszego znaczenia. Powoduje to pewne ryzyka w bezpieczeństwie łańcucha dostaw, mogące zostać wykorzystane. f) etc. etc. Poniższe artykuły są zapisane w sposób niewystarczająco nakazowy, a także jest – patrząc obiektywnie – niewielki objętościowo w stosunku do wielu artykułów Ustawy, nakazujących bezwzględne jej stosowanie i opisujących różne warianty. Ustawa w ogóle nie wspiera tego, co tak ewidentnie jest zapisane w *Strategii Cyberbezpieczeństwa RP na lata 2019-2024*, tj. tego, że obszar obronności państwa obejmuje również cyberprzestrzeń, a ta przecież powstaje poprzez uruchamianie i łączenie infrastruktur ICT, stąd postępowania zakupowe dot. infrastruktury ICT i bezpieczeństwa IT powinny być w szczególności chronione przed nieuzasadnionym szerokim wypływem informacji, przy zachowaniu kontroli nad finansami publicznymi. Dodatkowo, możliwości oferowane przez Art. 131e ust.1 (ograniczanie potencjalnych Wykonawców) należałoby rozszerzyć o zapisy proponowane przez Państwa projekt zmian Ustawy o ksc. Są bardzo sensowne z punktu widzenia cyberbezpieczeństwa. Na razie obecnie obowiązująca Ustawa	

			Prawo Zamówień publicznych nie wspiera w wystarczający sposób możliwość wykluczenia potencjalnego Wykonawcy z postępowania, wskutek obiektywnie wiarygodnych informacji na jego temat, dotyczących bezpieczeństwa, które w wystarczający sposób uzasadniają podjęcie daleko idącej ostrożności w stosunku do niego.	
170.	SayF	Art. 1 ust. 1 pkt 4)	Ustawa określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Projekt nowelizacji tej ustawy rozszerza zakres regulacji ustawy o krajowym systemie cyberbezpieczeństwa, dalej „KSC", o zadania i obowiązki przedsiębiorców komunikacji elektronicznej wykraczające poza obszar cyberbezpieczeństwa. Pojęcie bezpieczeństwa w komunikacji elektronicznej jest znacznie szerszy niż tylko sprawy określone w ustawie o KSC to znaczy sprawy związane z cyberbezpieczeństwem. **Proponujemy wykreślić art. 1 ust. 1 pkt 4 lub przeredagować treść art. 1 ust 1 pkt 4 i nadając mu treść:** **„4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących cyberbezpieczeństwa i zgłaszania incydentów;"** **Po wykreśleniu art. 1 ust. 2 pkt 1 KSC będzie odnosiła się również do przedsiębiorców komunikacji elektronicznej w takim samym zakresie jak do innych podmiotów.**	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w

				zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
171.	KIGEIT	Art. 1 ust. 1 pkt 4	**Propozycja zmiany:** wykreślenie: ~~„4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;”,~~ **Uzasadnienie:** Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

				incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
172.	PIIT	Art. 1	**1. <u>Art. 1</u> ustawy o krajowym systemie cyberbezpieczeństwa (dalej, jako KSC).** Projekt zakłada bardzo istotną, systemową zmianę w sposobie regulacji obecnych obowiązków przedsiębiorców telekomunikacyjnych, a w przyszłości przedsiębiorców komunikacji elektronicznej. Celem projektu jest, bowiem włączenie tej kategorii podmiotów do krajowego systemu cyberbezpieczeństwa, a także określenie nowych obowiązków, w tym w zakresie – przekraczającym postanowienia aktualnej ustawy – Prawo telekomunikacyjne oraz projektowanej ustawy – Prawo komunikacji elektronicznej. Tym samym, podmioty dotychczas wyłączone tj. m.in. przedsiębiorcy telekomunikacyjni mieliby zostać objęci wymaganiami ustawy KSC w zakresie wymogów dot. bezpieczeństwa i zgłaszania incydentów. Rozwiązanie to, jako rodzące daleko idące wątpliwości wymaga przynajmniej istotnej modyfikacji. Należy, bowiem zwrócić uwagę na podstawowe ramy nadawane w tym zakresie przez prawodawstwo unijne: • Zgodnie z art. 1 ust. 3 dyrektywy Parlamentu Europejskiego I Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. *w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii,* który stanowi, że: „3.*Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie* ***<u>nie mają</u>***	**Uwaga niewuzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			<u>zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy</u> *2002/21/WE,* ***ani do dostawców usług zaufania****, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014.".* • Zmiany w zakresie bezpieczeństwa i integralności sieci i usług w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, wobec dotychczasowych przepisów art. 13a i 13 b dyrektywy ramowej sprowadzają się do: o rozszerzenia zakresu regulacji z przedsiębiorców telekomunikacyjnych, na przedsiębiorców komunikacji elektronicznej; o uelastycznienia w zakresie możliwości określenia organu właściwego poprzez zastąpienie odwołania do właściwości organu regulacyjnego odwołaniem do „właściwego organu"; o doprecyzowania parametrów dla kryteriów zgłoszenia incydentów; o dodania możliwości zwracania się o pomoc CSIRT. Niepodważalne jest więc wyłączenie m.in. przedsiębiorców telekomunikacyjnych spod regulacji dyrektywy NIS. Tym samym nie jest możliwe wprowadzenie w polskich przepisach regulacji odmiennej, która mogłaby skutkować w przyszłości objęciem tego kręgu podmiotów regulacjami odnoszącymi się np. do usług kluczowych lub cyfrowych. Z drugiej strony implementacja EKŁE nie wymaga tak daleko idących zmian jak te przedstawione w ustawie. Do zakresu proponowanych regulacji odnosimy się jednak w kolejnych punktach stanowiska.	

			Postulat W zakresie art. 1 pkt 1 należy wprowadzić następujące zmiany: • przywrócić wyłączenie przewidziane w art. 1 ust. 3 dyrektywy NIS oraz aktualnym art. 1 ust. 2 pkt 1 i 2 KSC;	
173.	KIGEIT	Art 1 ust. 2 pkt 1)	**1)nałożenie obowiązków** wynikających z KSC na przedsiębiorców komunikacji elektronicznej) **Propozycja zmiany:** przywrócenie wyłączenia podmiotowego przedsiębiorców komunikacji elektronicznej o następującej treści: *2. Ustawy nie stosuje się do:* *1) przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ….Prawo komunikacji elektronicznej (Dz.U. z 2017 r., pozycje 1907 i 2201; 2018, pozycje 106, 138, 650 i 118) w zakresie wymogów dotyczących powiadamiania o zdarzeniach i bezpieczeństwa;* *2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania dla transakcji elektronicznych na rynku wewnętrznym i uchylające dyrektywę 1999/93/WE (Dz.U. L 25) 2005, s. 7, 28.08.2014, s. 73);* **Uzasadnienie:** Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorców komunikacji elektronicznej. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w

				zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
174.	Izba Gospodarcza Gazownictwa/PGNIG SA Oddział w Zielonej Górze	Art. 1 pkt 10)	Projekt ustawy zakłada znaczne spłaszczenie struktur poprzez wskazanie SOC (zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie) zamiast uprzednio wskazywanych „wewnętrznych struktur" odpowiedzialnych za cyberbezpieczeństwo. Takie podejście przy rozległych strukturach terytorialnych przedsiębiorstwa ma znaczny wpływ na ograniczenie zdolności operacyjnych zespołu. W naszej opinii powinno się uwzględnić włączenie w wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo przedsiębiorstwa SOC jako organu operacyjnego.	**Uwaga nieuwzględniona.** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników

				przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
175.	Polska Izba Handlu	Art. 1 ust. 1 pkt 4 KSC	**Propozycja zmiany:** Należy wykreślić **Uzasadnienie:** Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21 / WE	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

				incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
176.	Unia Metropolii Polskich	Art. 1. Ust. 13	Projekt ustawy przewiduje zgłaszanie incydentów przez podmioty samorządowe wojewodzie nie później niż w ciągu 24 godzin. Proponuje się wydłużyć ten termin do **48 godzin.** Biorąc pod uwagę ograniczone zasoby kadrowe urzędu oraz szeroki zakres realizowanych zadań z zakresu bezpieczeństwa IT, wnosi się o wydłużenie terminu raportowania do 48 godzin.	**Uwaga nieuwzględniona** Szczególnie w przypadku jednostek samorządowych incydenty powinny być zgłaszane jak najszybciej, aby te podmioty uzyskały niezbędną pomoc.
177.	KIGEIT	Art. 2 pkt 3b	**Propozycja zmiany:** wykreślenie *„~~3b) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej~~;”* **Uzasadnienie:** Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21 / WE. Nawet w wypadku nieuwzględnienia powyższego argumentu, za wykreśleniem definicji przemawia jej nadmiarowość – w projektowanym art. 2 pkt 3a) przewidziana została definicja CSIRT sektorowego, która obejmuje między innymi CSIRT dla sektora telekomunikacyjnego.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

				administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
178.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2 pkt 3b	1)W art. 2 pkt 3b tworzy się CSIRT Telco. Z jakiego powodu wybrano już nazwę dla CSIRT-u i czemu jest szczególnie wskazany w ustawie, a nie został dodany jako kolejny CSIRT sektorowy - zespół zakresem działania obejmujący usługi telekomunikacyjne. 2)W propozycji nowelizacji nie jest jasne kto pełni rolę organu właściwego dla CSIRT Telco? Czy jest w ogóle organ właściwy dla CSIRT Telco? Projekt nie wskazuje tego jednoznacznie.	CSIRT Telco nie jest CSIRT sektorowym ponieważ nie ma sektora telekomunikacja w ustawie. Organem zapewniającym funkcjonowanie CSIRT Telco jest minister właściwy do spraw informtyzacji
179.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2 pkt 3c	Nie jest jasne dlaczego zadania ISAC zostały ograniczone do wymiany i analizy informacji na temat podatności, zagrożeń i incydentów? Z reguły ISAC świadczą usługi w zależności od potrzeb swoich członków, nie ograniczając się tylko do zadań wskazanych w ustawie. Proponuje się następujące brzmienie przepisu: „centrum wymiany i analizy informacji świadczące wybrane usługi z zakresu cyberbezpieczeństwa na rzecz swoich członków lub funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa”. Przepisy projektu zmiany ustawy nie wyjaśniają również sensu powoływania i korzyści z powoływania ISAC, proponowany zakres działalności ISAC można zlecić np. CSIRT-om sektorowym	**Wyjaśnienie** ISAC nie są jednostkami operacyjnymi. Są to centra wymiany informacji.

			bez uszczerbku dla wymiany informacji w ramach KSC. Trudno o jednoznaczne wskazanie wartości dodanej dla wprowadzenia tego rozwiązania.	
180.	Związek Banków Polskich	Art. 2 pkt 3c	3c) ISAC – centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w celu wspierania**, w szczególności** podmiotów krajowego systemu cyberbezpieczeństwa**, a także podmiotów w ramach danego sektora, sektorów lub podsektorów;** ISAC powinien również wspomagać podmioty z danego sektora, sektorów lub podsektorów niezależnie od wydania decyzji o uznaniu za OUK – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od innych podmiotów – pozostałych banków, dostawców usług płatniczych, izb rozliczeniowych itd.	**Uwaga nieuwzględniona** ISAC mogą przekazywać informacje wszystkim podmiotom KSC.
181.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 2 pkt 3d	Proponuje się następujące brzmienie tłumaczenia Security Operation Center: „centrum operacji bezpieczeństwa" lub „centrum operacji cyberbezpieczeństwa". Jeśli natomiast przewidywana jest możliwość outsourcingu SOC to w definicji powinien być zapis „zespół pełniący funkcję centrum operacji cyberbezpieczeństwa w danym podmiocie lub na rzecz tego podmiotu".	**Uwaga nieuwzględniona** Obecna definicja SOC zapewnia możliwość funkcjonowania takich zespołów wewnątrz operatorów usług kluczowych jak i mogą być te zespoły prowadzone przez podmioty zewnętrzne na rzecz OUK.
182.	PKP Energetyka	Art. 2 pkt 3d	Projekt wprowadza definicję Operacyjne Centrum Bezpieczeństwa (SOC) i określa szereg obowiązków, które ma ten podmiot wykonywać. Należy zwrócić uwagę na ust. 6 art. 14 Projektu zgodnie z którym SOC na swojej stronie internetowej ma udostępnić szereg informacji na temat swojej działalności. Podsumowując kwestie związane z ujawnianiem danych chronionych – wielość tych danych oraz obowiązek wskazany w Projekcie w kontekście przekazywania ich różnym podmiotom,	**Wyjaśnienie** Projekt nawiązuje do praktyki rynkowej – udostępniania informacji według wzoru dokumentu RFC 2350. Skuteczną komunikację zapewni podłączenie podmiotu krajowego systemu cyberbezpieczeństwa do systemu o którym mowa w art. 46.

			przy braku konkretnego celu ich wykorzystania – wydaje się nadmiernym obowiązkiem. Wątpliwości rodzi budowanie złożonej siatki przekazywania informacji i wielu chronionych danych (np. osobowych lub o incydentach) pomiędzy podmiotami CSIRT-y centralne, sektorowe, Biuro Pełnomocnika, Kolegium ds. Cyberbezpieczeństwa oraz ISAC-e (takich podmiotów może być kilkadziesiąt), np. kiedy, do kogo aby spełnić wymagania 24 godzin. W zaproponowanych regulacjach brakuje klucza według którego podmioty miałyby się dzielić takimi informacjami. Mając na uwadze powyższe, proponujemy dla danego obszaru (branży) stworzenie jednego punktu kontaktu. Takie rozwiązanie (stosowane na wzór np. single point of contact w telekomunikacji, one stop shop w branży kolejowej) pozwoli na transparentność procesu w kontekście zbierania informacji.	
183.	SayF	Art. 2 pkt 3e	Proponuje się wykreślić wyraz „oznacza”. Wyraz ten użyto już w zdaniu wprowadzającym do wyliczania w art. 2.	**Wyjaśnienie** **Definicja została zmieniona**
184.	Związek Banków Polskich	Art. 2 pkt 3e	W pierwszym zdaniu mowa jest o dostawcy sprzętu lub oprogramowania, a rozwinięcie w podpunkcie a) mówi dodatkowo o usługach ICT. Jest to znacznie szerszy zakres.	**Wyjaśnienie** **Definicja została zmieniona**
185.	PKP Energetyka	art. 2 pkt. 3e	Projekt przewiduje w art. 2 pkt 3e) dodanie definicji *„dostawcy sprzętu lub oprogramowania”* (w tym definicje produktów, usług i procesów ICT) które jak rozumiemy, zostało wprowadzone w związku z uprawnieniem Kolegium do oceny Dostawców oraz objęciem ustawą rynku telekomunikacyjnego. Takie ujęcie ww. definicji może mieć negatywny wpływ na rozwój rynku, nie tylko informatycznego poprzez ustalanie listy Dostawców. Zgodnie z Projektem, centralizacja na szczeblu rządowym szeregu decyzji właściwych dla firm, podejmowanych na poziomie operacyjnym, takich jak np. wybór odpowiedniego dla danej organizacji	**Wyjaśnienie** **Definicja została zmieniona**

			Dostawcy lub korekty analizy ryzyka (poprzez polecenie zabezpieczające) i wdrożenie zabezpieczeń, ogranicza decyzyjność i niezależność biznesową tych podmiotów.	
186.	KIGEIT	Art. 2 pkt 8a	**Propozycja zmiany:** wykreślenie ~~*8a) incydent telekomunikacyjny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej;*~~ **Uzasadnienie:** Incydenty dotyczące wszystkich pozostałych sektorów nie zostały ujęte w definicjach. Brak jest również określenia mechanizmów oznaczania incydentów, np. dla operatora usługi komunikacji elektronicznej, sklasyfikowanej jako usługa kluczowa, pojawia się wątpliwość – czy incydent może być: telekomunikacyjny, istotny i poważny, czy tylko kluczowy (niejasne jest stopniowanie typów ryzyk).	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

				incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
187.	SayF	Art. 2 pkt 8a	Proponuje się wykreślić tę definicję lub zmienić definicję na odnoszącą się do bezpieczeństwa systemów informacyjnych wykorzystywanych w komunikacji elektronicznej – do cyberbezpieczeństwa w komunikacji elektronicznej. Incydent telekomunikacyjny nie dotyczy innego bezpieczeństwa jak tylko bezpieczeństwa w cyberprzestrzeni. Definicja incydentu (art. 2 pkt 5) odnosi się do wszystkich incydentów bez względu na podmiot, u którego wystąpi. **Jeśli jednak powinien autorzy projektu uznają, że należy zdefiniować pojęcie „incydent telekomunikacyjny" to proponuję:** **„incydent telekomunikacyjny – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo w komunikacji elektronicznej, w szczególności może spowodować lub spowoduje obniżenie; jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej**;	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki

				przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
188.	KIGEIT	art. 2 pkt 8f	**Propozycja zmiany:** *8f) bezpieczeństwo sieci i usług – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania lub minimalizowania skutków wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:* *a) tych sieci lub usług,* *b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,* *c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;* **Uzasadnienie:** Z praktycznego punktu widzenia nie jest możliwe zagwarantowanie absolutnej skuteczności stosowanych zabezpieczeń, zapewniających w każdym przypadku uniknięcie naruszenia.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Zaproponowana definicja jest wyczerpująca.
189.	SayF	Art. 2 pkt 8f	Konsekwencją przeredagowania art. 1 ust. 1 pkt 4 będzie usunięcie art. 1 pkt 8f. Definicja zawarta w art. 2 pkt 4 (i nie tylko ta definicja) dotyczy również systemów informacyjnych	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

			wykorzystywanych przez przedsiębiorców komunikacji elektronicznej.	przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
190.	KIGEIT	art. 2 pkt 8g	**Propozycja zmiany:** wykreślenie ~~*8g) sytuacja szczególnego zagrożenia – sytuacja, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej;*~~ **Uzasadnienie:** Art. 2 pkt 8g przedmiotowego projektu definiuje sytuację szczególnego zagrożenia jako sytuację, o której mowa w art. 2 pkt 65 ustawy z dnia … – Prawo komunikacji elektronicznej. Jednakże	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.

			zgodnie z powołanym przepisem projektowanego Prawa komunikacji elektronicznej, sytuacja szczególnego zagrożenia oznacza: *stan nadzwyczajny, sytuację kryzysową, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2019 r. poz. 1398 oraz z 2020 r. poz. 148, 284, 374 i 695) lub bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług*. Definicja sytuacji szczególnego zagrożenia określona została w Prawie komunikacji elektronicznej na potrzeby planowania działań przedsiębiorcy telekomunikacyjnego na wypadek wystąpienia stanu nadzwyczajnego (wojennego, wyjątkowego lub klęski żywiołowej), sytuacji kryzysowej lub szeroko rozumianego zagrożenia dla bezpieczeństwa sieci i usług, w tym również zagrożenia terrorystycznego, awarii sprzętu, przerwy w dostawie energii elektrycznej i innych. Przepisy ustawy o krajowym systemie cyberbezpieczeństwa nie odnoszą się do tak szeroko rozumianych sytuacji szczególnego zagrożenia. Przepisy te odnoszą się wyłącznie do zagrożenia dla bezpieczeństwa sieci i usług w zakresie cyberataków. W tej sytuacji definicja sytuacji szczególnego zagrożenia nie ma zastosowania w ustawie o krajowym systemie cyberbezpieczeństwa. Problematyka sytuacji szczególnego zagrożenia została wystarczająco uregulowana w Prawie telekomunikacyjnym oraz będzie uregulowana w Prawie komunikacji elektronicznej, którego przepisy odnoszą się również do cyberbezpieczeństwa. Co więcej, pojęcie sytuacji szczególnego zagrożenia w ogóle nie występuje na gruncie ustawy o KSC poza projektowanym art. 20a, który, jak wspomniano powyżej, stanowi powtórzenie art. 39 projektu PKE i z tego powodu winien zostać usunięty z Projektu.	EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
191.	SayF	Art. 2 pkt 15	Zła odmiana. Proponujemy zamienić „usługę świadczoną drogą elektroniczną” na „usługa świadczona drogą elektroniczną”	**Uwaga uwzględniona**

192.	SayF	Art. 2 pkt 16	Definicja niejasna. Proponujemy zmienić definicję na „usługa kluczowa – usługa wymieniona w wykazie usług kluczowych, o którym mowa w Art. 6 pkt 1;	**Uwaga nieuzględniona** Uwaga nie dotyczy projektu nowelizacji. Definicja usługi kluczowej nawiązuje do art. 5 ust. 2 dyrektywy NIS.
193.	SayF	Art. 2 pkt 18	Definicja niejasna. Proponujemy rozwinięcie definicji lub dodanie do definicji „o którym mowa w Art. 48”	**Uwaga nieuzględniona** **U**waga nie dotyczy projektu nowelizacji. Definicja usługi kluczowej nawiązuje do art. 2 pkt 8 dyrektywy NIS.
194.	SayF	Art. 2 pkt 19	Definicja niejasna. Proponujemy rozwinięcie definicji lub dodanie do definicji „o którym mowa w Art. 61 ust 1”	**Uwaga nieuzględniona** **U**waga nie dotyczy projektu nowelizacji.
195.	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	Art. 4	**Mediakom postuluje, by ograniczyć grono przedsiębiorców komunikacji elektronicznej będących częścią systemu cyberbezpieczeństwa do tych tylko, którzy zobowiązani są sporządzać plany działań w sytuacjach szczególnych zagrożeń, o którym mowa w art. 47 ust. 1 PKE.** Jak wskazano powyżej – plany mają obowiązek sporządzać przedsiębiorcy o dużej skali działalności, świadczący własne usługi, z wykorzystaniem własnej sieci i osiągający przychody przekraczające 10 mln złotych. Mają oni realne znaczenie dla krajowego systemu cyberbezpieczeństwa, zaś incydenty bezpieczeństwa, które mogą ich dotknąć z zasady będą miały istotne znaczenie z uwagi na ilość abonentów i obszar, który incydent może dotknąć. Inaczej jest w przypadku mniejszych przedsiębiorców, których liczba jest bardzo znacząca, a jednocześnie znaczenie z uwagi na ilość obsługiwanych abonentów i obszar działania – niewielkie. Przedsiębiorcy ci nie mają realnego znaczenia dla krajowego systemu cyberbezpieczeństwa. Jak pokazała praktyka przedsiębiorcy osiągający przychody do 10 mln złotych nie mieli istotnego znaczenia z punktu widzenia lokalnych podmiotów odpowiedzialnych za zarządzanie kryzysowe – stąd zwolnienie ich	**Wyjaśnienie** W sytuacji gdy tak duża liczba różnych usług kluczowych dla bezpieczeństwa państwa i obywateli jest zależna od niezakłóconego świadczenia usług komunikacji elektronicznej niezbędne jest włączenie wszystkich przedsiębiorców komunikacji elektronicznej do jednolitego systemu cyberbezpieczeństwa.

			z obowiązku tworzenia i uzgadniania z właściwymi podmiotami planów działania, o których mowa w art. 47 ust. 1 PKE. Jednocześnie wielość przedsiębiorców prowadzących działalność na mniejszą skalę jest tak duża – sięgająca aż 6.000 podmiotów, że sama obsługa zgłoszeń incydentów bezpieczeństwa będzie wymagała ogromnej pracy logistycznej. Dodanie do niego pkt 2a i tym samym włączenie do krajowego systemu cyberbezpieczeństwa wszystkich podmiotów komunikacji elektronicznej „2a) przedsiębiorców komunikacji elektronicznej sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy Prawo komunikacji elektronicznej”	
196.			**3.** Art. 4 pkt 2a dot. włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa Tak jak wskazaliśmy w części ogólnej, w naszej ocenie proponowane przepisy KSC wykraczają poza zakres niezbędny dla wdrożenia EKŁE. Jednocześnie zakres proponowanych zmian jest tak szeroki i budzi tak daleko idące wątpliwości, że nie będzie możliwe wykonanie nowych obowiązków w przewidywanych w projekcie ustawy terminach. Co więcej dublowanie obowiązków raportowych uważamy za nieproporcjonalne i nieefektywne rozwiązanie. Nie negując na tym etapie ewentualnej potrzeby wzmocnienia aspektów cyberbezpieczeństwa w dotychczasowym modelu raportowym postulujemy przeniesienie dyskusji w tym zakresie na okres po wdrożeniu PKE, tak aby zarówno model raportowania jak i przepisy w tym zakresie, zostały odpowiednio	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

			dopracowane, spójne, a przede wszystkim dawały odpowiedni czas na podjęcie organizacyjnego i finansowego wysiłku w zakresie dostosowania się do nowych wymagań. Postulat: o Art. 4 ust. 2a oraz 5a należy usunąć z obecnego projektu. Dyskusję nad przepisami w tym zakresie powinna poprzedzić rzetelna debata nad realnymi potrzebami, przeprowadzona z udziałem zainteresowanych partnerów społecznych, w tym podmiotów, które miałyby zostać objęte tymi wymaganiami.	administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
197.	KIGEIT	Art. 4 pkt 2a i 5a	**Propozycja zmiany:** wykreślenie ~~*2a) przedsiębiorców komunikacji elektronicznej;*~~ ~~*5a) CSIRT Telco;*~~ **Uzasadnienie:** Zgodnie z dyrektywą NIS wymogi w zakresie sprawozdawczości dotyczące bezpieczeństwa i incydentów wynikające z przedmiotowej dyrektywy nie mają zastosowania do przedsiębiorstw telekomunikacyjnych. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE.	Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w

				zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
198.	ISSA Polska	Art. 4 pkt 6	Proponujemy dla art. 14 dla punktu 6 zastosować terminologię przyjętą w ustawie w zakresie określania deklaracji działania SOC. W związku z powyższym proponujemy punkt 6. zamienić na: 6) posiadać i udostępniać w języku polskim i angielskim deklarację polityki działania w zakresie określnym w dokumencie RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF);	**Wyjaśnienie** Przywoływany przepis prawa dotyczy jedynie SOC prowadzonych podmioty nie będące operatorami usług kluczowych.
199.	ISSA Polska	Art. 4 pkt 16	**Propozycja zmiany** SOC i podmioty świadczące usługi z zakresu cyberbezpieczeństwa;" Wykreślenie podmiotów świadczących usługi mogłoby spowodować naruszenie równowagi rynku oraz wyrzucić dostawców usług np. specjalizowanej usługi forensic poza ustawę. W naszej ocenie nie każdy podmiot świadczący usługi z zakresu cyberbezpieczeństwa jest lub będzie SOC.	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych

				aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
200.	Związek Banków Polskich	Art. 4 pkt 16	Przepis budzi wątpliwości. Aktualna treść tego punktu to: „podmioty świadczące usługi z zakresu cyberbezpieczeństwa;" – jest to znacznie szersze określenie dotyczące wielu podmiotów. Zmiana zapisu na SOC jest niejasna, niejednoznaczna i wskazuje na pojedynczą komórkę jakiegoś podmiotu.	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników

				przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
201.	Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo - Technicznych	Art. 4a	art. 4a *„(…) 4. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu następuje na wniosek podmiotu prowadzącego ISAC po uzyskaniu pozytywnej opinii CSIRT MON, CSIRT NASK lub CSIRT GOV. Wniosek zawiera dane, o których mowa w ust. 3 pkt 1-5. (…)”.* W związku z tym, że do zakresu zadań ISAC ma należeć m.in. wymiana informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności oraz incydentów rekomendujemy, aby we wskazanym katalogu organów uprawnionych do wydania opinii pozytywnej na temat ISAC włączyć również CSIRT sektorowy oraz CSIRT Telco	**Wyjaśnienie** Przepis został zmieniony. ISAC będzie opiniowany przez organy właściwe do spraw cyberbezpieczeństwa.
202.	Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o.	Art. 4a. 1.	**Nowy rodzaj podmiotu ISAC - brak zdefiniowanych kryteriów i wymagań, które ISAC powinny spełniać** ISAC powinno podlegać i spełniać wymagania ustawy na poziomie nie mniejszym niż OUK	**Uwaga nieuwzględniona** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.
203.	Izba Gospodarcza Gazownictwa/Polska Spółka	Art. 4.a	**Zespoły ISAC** Nie zostały doprecyzowane : funkcja, miejsce i rola ISAC, co rodzi m.in. poniższe pytania: Czy w ramach CSiRT mogą być powołane ISAC?	**Wyjaśnieni** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do

	Gazownictwa Sp. z.o.o.		Czy ISAC będzie pełnił role wymiany informacji z podmiotami OUK i DUC, czy też komercyjne. Na jakich zasadach OUK, DUC będą mogły korzystać z usług lub pomocy ISAC – na zasadach komercyjnych czy nieodpłatnych ?	utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.
204.	Związek Banków Polskich	Art. 4a ust. 1	„Art. 4a. 1. W ramach krajowego systemu cyberbezpieczeństwa może funkcjonować ISAC **realizujący zadania dla podmiotów z danego sektora, sektorów lub podsektorów**, w szczególności związane z wymianą informacji, dobrych praktyk i doświadczeń dotyczących zagrożeń cyberbezpieczeństwa, podatności lub incydentów;**”** ISAC (centra wymiany i analizy informacji), tworzone jako inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. ISAC powinien jednak wspomagać również podmioty z danego sektora lub sektorów, niezależnie od wydania decyzji o uznaniu za OUK – zapewni to szczelność systemu. Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od innych podmiotów – pozostałych banków, dostawców usług płatniczych, izb rozliczeniowych itd.	**Uwaga nieuwzględniona** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC. Nic nie broni, aby ISAC świadczyły swoje usługi podmiotom spoza KSC.
205.	Fundacja Bezpieczna Cyberprzestrzeń	art. 4a ust. 1	w przepisie powinna być zastosowana liczba mnoga tj. „mogą funkcjonować ISAC”, ponadto zakres zadań wskazanych w tym artykule jest odmienny od wskazanego w definicji ISAC w art. 2 pkt 3c	**Wyjaśnienie** W technice legislacyjnej używa się liczby pojedynczej dla określenia podmiotów, które będą spełniać cechy określone w ustawie.
206.	Fundacja Bezpieczna Cyberprzestrzeń	art. 4a ust. 2	Nie jest jasne w jakim celu minister prowadzi wykaz ISAC? Czy jest to forma wyrażenia zgody na prowadzenie tego typu działalności, wbrew ust. 7? Nie są również podane żadne zadania jakie miałby realizować ISAC, poza celem jego funkcjonowania. Z uzasadnienia wynika, że celem jest dostęp do wiedzy eksperckiej	**Wyjaśnienie** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada

			dotyczącej cyberzagrożeń, ale ustawodawca nie określił na jakie konkretne zadania należy ten cel przełożyć	wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.
207.	Związek Banków Polskich	Art. 4a ust. 2	Nowe brzmienie ust. 2 – **dalsze ustępy art. 4a uległyby przenumerowaniu.** **2)ISAC może wykonywać zadania powierzone SOC, w szczególności związane z zarządzaniem, koordynowaniem i obsługą incydentów (bezpieczeństwa) zagrażających bezpieczeństwu podmiotów, o których mowa w ust. 1 lub ich klientom.** Taka propozycja podniesie efektywność wymiany informacji o incydentach, będzie zgodna z formą działania ISAC praktykowaną w Europie polegającą na tworzeniu zespołów zadaniowych w celu reagowania na incydenty (Ad hoc investigative working group). Umożliwi również realne wsparcie podmiotów krajowego systemu cyberebzpieczeństwa oraz podmiotów z danego sektora, sektorów lub podsektorów. https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/at_download/fullReport Np. Luxemburg CERT jest jednocześnie ISAC.	**Uwaga nieuwzględniona** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.
208.	Fundacja Bezpieczna Cyberprzestrzeń	art. 4a ust. 4	Konieczne jest doprecyzowanie w jakim zakresie opiniowany jest wniosek o wpisanie do wykazu ISAC. Dodatkowo przepis wymaga uszczegółowienia kwestia czy bez uzyskania pozytywnej opinii wszystkich CSIRT-ów poziomu krajowego można zostać wpisanym do wykazu oraz czy bez takiej opinii nie można zaprzestać prowadzenia ISAC. Sama idea ISAC zakłada samoorganizację podmiotów (najczęściej danego sektora) w celu	**Wyjasnienie** ISAC są inicjatywą dobrowolną. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w

			wymiany istotnych informacji z zakresu cyberbezpieczeństwa. Podmioty te działają na własną rzecz i we własnym zakresie się finansują. Z założenia ISAC nie są tworzone w celach komercyjnych (choć ten cel nie jest wykluczony). Z uzasadnienia wynika, że celem jest dostęp do wiedzy eksperckiej dotyczącej cyberzagrożeń. Prowadzenie rejestru, konieczność uzyskania opinii CSIRT-u poziomu krajowego oraz obowiązek przedkładania sprawozdania z realizacji zadań za poprzedni rok kalendarzowy na pewno nie są czynnikami sprzyjającymi i zachęcającym do tworzenia ISAC, co jest zaprzeczeniem idei przedstawionej w uzasadnieniu projektu.	różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC. W nowej wersji projektu zrezygnowano z opiniowania ISAC przez CSIRT poziomu krajowego natomiast będą opiniować wszystkie organy właściwe do spraw cyberbezpieczeństwa.
209.	Fundacja Bezpieczna Cyberprzestrzeń	art. 4a ust. 9	Istnieje konieczność doprecyzowania jaki jest cel przedstawiania sprawozdania oraz jaki miałby być zakres informacji przedstawianych w sprawozdaniu, biorąc pod uwagę brak precyzyjnie określonych dla ISAC zadań.	**Wyjaśnienie** ISAC są inicjatywą dobrowolną i nie są jednostkami operacyjnymi. Ich zadaniem ma być gromadzenie i dzielenie się przydatnymi informacjami z zakresu cyberbezpieczeństwa. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC. Sprawozdanie jest niezbędne dla oceny funkcjonowania ISAC w ramach KSC.
210.	Związek Banków Polskich	Art. 4a ust. 9	**4a. ust. 9. ISAC** współpracują ze sobą oraz z CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowymi, w szczególności w zakresie wymiany wiedzy i informacji o podatnościach, zagrożeniach i zidentyfikowanych incydentach oraz ich obsługi i koordynacji.** **Propozycja nowego ust. 10 w brzmieniu:**	**Uwaga częściowo uwzględniona** ISAC nie ma kompetencji operacyjnych. Nie bierze udziału w obsłudze i reagowaniu na incydenty. Może uczestniczyć w wymianie informacji o zagrożeniach, podatnościach czy zaobserwowanych incydentach.

			4a. ust. 10.ISAC przedkładają ministrowi spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy. Dotychczasowy ust. 10 uległby przenumerowaniu. Zapewnienie wymiany informacji między sektorami. Proponujemy również rozdzielić kwestię współpracy z CSIRTami od kwestii przedkładania sprawozdań i zawarcie tej kwestii w kolejnym ustępie (dalsze ustępy uległy by przenumerowaniu).	
211.	Fundacja Bezpieczna Cyberprzestrzeń	art. 4a ust. 10	Istnieje konieczność doprecyzowania w jakim zakresie działalność ISAC może być niezgodna z prawem oraz zasad współpracy obowiązujących w ramach KSC.	**Wyjaśnienie** Chodzi o przypadki naruszenia ustawy ksc lub prawa karnego albo nie respektowanie warunków zawartych w porozumieniu ws. korzystania z systemu z art. 46.
212.	Home.pl	Art. 5 ustawy zmieniającej	Zgodnie z przepisem art. 5 ustawy zmieniającej, nowelizacja ma wejść w życie 21 grudnia 2020 r. to jest wraz z PKE. **Uwagi w ramach konsultacji:** - do art. 5 ustawy zmieniającej: ustawodawca planuje, aby nowelizacja i ustawa Prawo komunikacji elektronicznej, weszły w życie z dniem 21 grudnia 2020 r. Biorąc pod uwagę, dalszą pracę w ramach komisji sejmowych, procedurę głosowania nad projektami w parlamencie oraz podpis pod projektami Prezydenta RP, przewiduję iż ustawy zostaną opublikowana na przełomie listopada i grudnia. W obliczu znacznej ilości zmian, które projekty zawierają okres vacatio legis wynoszący być może niecały miesiąc jest zdecydowanie za krótki. Należy w związku z tym zasugerować przesunięcie daty wejścia w życie przepisów, aby zapewnić adresatom ustawy niezbędny okres na wdrożenie zmian.	**Wyjaśnienie** Wejście w życie ustawy jest wstępnie planowane na II kwartał 2021 r.

213.	ISSA Polska	Art. 8 pkt 2 lit. e	Modyfikacja Objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania cyberbezpieczeństwa w trybie ciągłym w sposób umożliwiający wykrycie i prowadzenie natychmiastowych czynności reakcji na incydent lub zagrożenie.	**Uwaga nieuwzględniona** Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne.
214.	ISSA Polska	Art. 8 pkt 3	Modyfikacja adekwatne do oceny ryzyka reagowanie na zagrożenia cyberbezpieczeństwa i ujawnione podatności w systemach informacyjnych wykorzystywanych do świadczenia usługi kluczowej;	**Uwaga nieuwzględniona** Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne.
215.	ISSA Polska	Art. 8 pkt 5 lit. e	Dodanie zapisu Przeprowadzania okresowej oceny parametrów konfiguracyjnych systemów wpływających na cyberbezpieczeństwo zgodnie z uznanymi standardami i praktykami.	**Uwaga nieuwzględniona** Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne.
216.	ISSA Polska	Art. 8 pkt 5 lit. b	w art. 8 w pkt 5 lit. b otrzymuje brzmienie: „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,”; Na: „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, na podstawie analizy ryzyka wpływu podatności zawartych w aktualizacjach,”; Zapis jest adekwatny do czynności przeprowadzanych w ramach procesy zarządzania podatnościami oraz wydaniami.	**Uwaga nieuwzględniona** Prowadzenie regularnych aktualizacji oprogramowania przygotowanych przez producenta danego oprogramowania przy wykorzystaniu zaleceń tegoż producenta jest nieodzownym elementem zarządzania ryzykiem. Brak szybkiej reakcji i aktualizacji oprogramowania zgodnie z zaleceniami jego producenta niesie dużo większe ryzyko, gdyż luka bezpieczeństwa może zostać wykorzystana przez podmioty trzecie w celu nieautoryzowanego dostępu do systemu.

217.	ISACA Warsaw Chapter	Ustawa KSC ustęp 7) w art. 8 w pkt 5 lit. b	b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem poziomu krytyczności poszczególnych aktualizacji,"; **Propozycja treści:** „b) regularne przeprowadzanie aktualizacji oprogramowania z wykorzystaniem zweryfikowanych aktualizacji; wersjonowanie oprogramowania,"	**Uwaga nieuwzględniona** Prowadzenie regularnych aktualizacji oprogramowania przygotowanych przez producenta danego oprogramowania przy wykorzystaniu zaleceń tegoż producenta jest nieodzownym elementem zarządzania ryzykiem. Brak szybkiej reakcji i aktualizacji oprogramowania zgodnie z zaleceniami jego producenta niesie dużo większe ryzyko, gdyż luka bezpieczeństwa może zostać wykorzystana przez podmioty trzecie w celu nieautoryzowanego dostępu do systemu.
218.	SayF	Art. 10 ust 2	Brakuje CSIRT Telco	**Uwaga uwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
219.	Transition Software	Art. 11, ust.1, pkt. 4,5 oraz powiązane z nim art.12 i zwłaszcza art. 13, ust.1,	Należy w ustawie dodać artykuł, który ma zawierać jedną ogólną zbiorczą informację (na poziomie ustawy), że wymiana informacji (rozumiana w sposób całościowy) musi odbywać się w sposób bezpieczny, tj. z zastosowaniem bezpiecznych sposobów organizacyjnych oraz minimalnych mechanizmach technicznych/technologicznych (bezpieczny tunel, szyfrowanie, IPSec, PKI, etc.), ogólnouznawanych (rynek, branża IT) za bezpieczne, w okresie ich wdrożenia (np. w obecnym okresie, ogólnouznawany w branży IT za taki jest minimum AES256, etc.).	**Uwaga nieuwzględniona** Operator usługi kluczowej będzie wprowadzać proporcjonalne do oszacowanych ryzyk środki bezpieczeństwa w tym organizacyjne oraz techniczne.

		pkt.2 (o elektronicznym kanale przesyłu), jak również wszystkie powiązane z nimi analogiczne artykuły na przestrzeni całej ustawy (np. Art. 18, ust. 5, Art.20, Art. 20c, ust.1., pkt 3) i ust2 i ust.3 pkt1),2),3), Art.22, ust.1 i 2, Art.23, Art.24, 24a pkt 1), etc.	Jest obecnie w *Rozporządzeniu Ministra Cyfryzacji z dn. 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów (…)* opisane to ogólnie w §2, ust. 1 pkt. d) oraz pkt. 2), ale w obecnej formie jest niewystarczający (bez konkretnych wymogów technicznych, które należy traktować jako wymagane niezbędne minimum), dlatego ten paragraf w tej formie powinien zostać przeniesiony do ustawy. Natomiast w ww. Rozporządzeniu należy go zastąpić artykułem, który będzie precyzował i podawał konkretne minimalne technologie (np. AES256, IPSec, PKI, etc.), na jakich muszą się opierać wdrażane środki bezpieczeństwa. Analogicznie, jak jest to podane chociażby w przypadku stopnia ochrony stropu, drzwi, ścian w §2 ust. 2 tegoż rozporządzenia. Podane mechanizmy zabezpieczeń powinny być przez podmiot zapewnione i wdrożone, niezależnie od wyniku przeprowadzonej przez dane przedsiębiorstwo analizy ryzyka, która zawsze ma charakter subiektywny w obrębie danej organizacji.	

220.	Związek Banków Polskich	Art. 11 ust. 3 pkt 1-3	3. W przypadku ustanowienia CSIRT sektorowego **lub ISAC działającego w danym sektorze, sektorach lub podsektorach** operator usługi kluczowej niezależnie od zadań określonych w ust. 1: 1) przekazuje jednocześnie właściwemu CSIRT sektorowemu oraz **właściwemu ISAC** w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4; 2) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora oraz **właściwym ISAC** podczas obsługi incydentu**, w tym incydentu** poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym **informacje stanowiące tajemnice prawnie chronione oraz dane osobowe**; 3)zapewnia właściwemu CSIRT sektorowemu oraz **właściwemu ISAC** dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań. ISAC to centra wymiany i analiz informacji tworzone jako inicjatywy sektorowe lub dziedzinowe. W celu prawidłowej realizacji zadań powierzonych ISAC, OUK powinni przekazywać mu informacje analogiczne jak przekazywane CSIRT sektorowemu. Zgodnie z uzasadnieniem projektu zadaniem ISAC jest wspieranie podmiotów krajowego systemu cyberbezpieczeństwa – nie byłoby to możliwe bez zapewnienia możliwości pozyskiwania informacji o incydentach przez ISAC. Należy również zapewnić możliwość przekazywania informacji stanowiących informacje prawnie chronione.	**Uwaga nieuwzględniona** Nie przewiduje się właściwości ISAC. To nie są jednostki operacyjne. ISAC wymieniają informacje z podmiotami, z którymi porozumieją się.
221.	SayF	Art. 12 ust 1 pkt, Art. 14a ust 2 pkt 3	Jaki „właściwy rejestr”?	**Wyjaśnienie** Chodzi przede wszystkim o numer KRS.

222.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 14	Wydaje się, że przypisanie realizacji wszystkich zadań, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13 w zakresie cyberbezpieczeństwa do struktury zwanej SOC jest nieuzasadnione. Zespoły SOC są powoływane do realizacji usług związanych z zarządzaniem zdarzeniami i incydentami, rzadziej prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem czy zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach – tym samym w projekcie dokonano nieuzasadnionego połączenia działań operacyjnych z działaniami typowo zarządczymi. Nawet sam projektodawca w OSR posługuje się pojęciami „usługi tzw. CERTowe (analityczne) oraz SOCowe (reagowania na incydenty)". Proponuje się wyłączenie zadań nieoperacyjnych z obowiązków zespołu SOC, pozostawiając OUK możliwość zawierania umów z podmiotami świadczącymi usługi z zakresu bezpieczeństwa inne niż SOC (zarzadzanie zdarzeniami i incydentami). Jako alternatywę można przyjąć wyodrębnienie katalogu usług z zakresu cyberbezpieczeństwa (np. na bazie tłumaczenia katalogu CSIRT Services Framework FIRST) do załącznika do ustawy lub odrębnego rozporządzenia i przypisanie konkretnego zestawu tych usług do poszczególnych rodzajów podmiotów krajowego systemu cyberbezpieczeństwa tj. SOC, ISAC, CSIRT sektorowy czy CSIRT poziomu krajowego. Pozwoli to na wyraźny podział pomiędzy tymi podmiotami oraz uniknięcie nakładających się kompetencji i obowiązków.	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
223.	Naczelna Organizacja	Art. 14	*„art. 14 (…) 5. W przypadkach, kiedy to niezbędne dla zapewnienia cyberbezpieczeństwa, podmiot prowadzący SOC zapewnia bezpieczny zdalny dostęp do swoich systemów dla*	**Uwaga nieuwzględniona** Obowiązkiem operatora usługi kluczowej prowadzącego SOC lub podmiotów zewnętrznych

	Techniczna. Federacja Stowarzyszeń Naukowo - Technicznych		*obsługiwanego operatora usługi kluczowej przez co najmniej: 1) ustalenie zasad dostępu do systemu; 2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację; 3) <u>minimalizację przechowywanych danych poza bezpiecznym środowiskiem</u>*". Biorąc pod uwagę krytyczność danych do których dostęp w związku ze świadczonymi usługami może posiadać podmiot prowadzący SOC rekomendujemy wykreślenie punktu 3, ponieważ w opinii Federacji wszelkie dane powinny być przechowywane wyłącznie w bezpiecznym środowisku.	prowadzących SOC na rzecz OUK jest zapewnienie takich technicznych i organizacyjnych środków bezpieczeństwa, proporcjonalnych do oszacowanego ryzyka.
224.	ISSA Polska	Art. 14 pkt 5	Proponujemy dla art. 14 dla punktu 5 doprecyzować zapis umożliwiający realizacje obowiązku bezpiecznego dostępu zdalnego. Proponujemy następujący zapis: 5. W przypadkach, kiedy jest to niezbędne podmiot prowadzący SOC zapewnia kryptograficznie zabezpieczony, rozliczany dostęp pomiędzy swoimi systemami realizującymi usługi SOC, a monitorowanymi systemami informacyjnych operatora usługi kluczowej.	**Uwaga nieuwzględniona** Obowiązkiem operatora usługi kluczowej prowadzącego SOC lub podmiotów zewnętrznych prowadzących SOC na rzecz OUK jest zapewnienie takich technicznych i organizacyjnych środków bezpieczeństwa, proporcjonalnych do oszacowanego ryzyka.
225.	KGHM/Związek Pracodawców Polska Miedź	14.1	Zgodnie z nowym brzmieniem art. 14.1 zespół operacyjnego centrum bezpieczeństwa (SOC) ma odpowiadać m.in. za wdrożenie systemu zarządzania bezpieczeństwem oraz wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych (w tym bezpieczeństwo fizyczne i środowiskowe). Obarczenie SOC zadaniami innymi niż operacyjne, tj. odpowiedzialność za wdrożenie SZB odpowiedzialność za wdrożenie środków tech/org zabezpieczających przez ryzykiem zmienia zasadniczo charakter zespołu z operacyjnego. W dużych firmach gdzie odpowiedzialność za obszar szeroko rozumianego bezpieczeństwa (compliance, zarządzanie, raportowanie, operacyjne) jest umiejscowiona strukturalnie w różnych pionach koncentracja w SOC więcej kompetencji niż operacyjne	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi.

			cyberbezpieczeństwo będzie trudne czy wręcz niemożliwe do zrealizowania. Proponuje się utrzymanie zapisów pierwotnego brzmienia Ustawy, tj. że to Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej itp. Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8.3, 8.4, 8.5, 8.6 art. 9 <i dalej bez zmian>	Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
226.	Federacja Przedsiębiorców Polskich	Art. 14 ust. 1 (w zw. z art. 8)	Przepis art. 14 ust. 1 ustawy o cyberbezpieczeństwie w nowym, projektowanym brzmieniu przewiduje, że zespół operacyjnego centrum bezpieczeństwa (SOC) ma m.in. wdrażać system zarządzania bezpieczeństwem oraz wdrażać odpowiednie i proporcjonalne do oszacowanego ryzyka środki techniczne i organizacyjne (w tym zapewniać bezpieczeństwo fizyczne i środowiskowe). Nałożenie na SOC obowiązku wdrażania systemu zarządzania bezpieczeństwem, a nie tylko wykonywanie działalności operacyjnej, będzie trudne lub nawet niemożliwe. Zwłaszcza w dużych podmiotach, w których odpowiedzialność za szeroko rozumiane bezpieczeństwo spoczywa na różnych pionach, skupienie tych zadań w SOC utrudni wykonywanie zadań	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.

			operacyjnych. W związku z powyższym uprzejmie zwracam się o odstąpienie od zmiany art. 14 ust. 1.	Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
227.	PIIT		**1. Art. 14 - SOC** Kluczowe zmiany przewidziano w art. 14 ustawy KSC, gdzie dotychczasowe wewnętrzne struktury bezpieczeństwa zastępowane są SOC. Jednocześnie popieraną przez nas zmianą jest przeniesienie na strukturę operatora usługi kluczowej dokonania oceny ryzyka i uzależnienie od niej zakresu wdrażanych środków technicznych i organizacyjnych. Stanowi to realizację naszego podstawowego postulatu przedstawianego w toku prac nad dwoma kolejnymi iteracjami rozporządzeń w tym zakresie. W zakresie zmiany nazewnictwa i wskazania na konieczność powołania SOC, w naszej ocenie przyjęta w tym przepisie konstrukcja realizacji przez operatora usługi kluczowej zadań wskazanych w ustawie w ramach SOC opiera się na błędnym założeniu, że wszystkie zadania realizowane są w ramach SOC. W strukturach dużych i rozproszonych nałożone na operatora usługi kluczowej obowiązki mogą i często są realizowane przez wiele komórek organizacyjnych, które wspólnie tworzą system	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych

			bezpieczeństwa całej organizacji. Ponadto warto zwrócić uwagę, że nawet sam projektodawca definiując SOC podkreślił jego operacyjny charakter - SOC to zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym podmiocie. Zadania przypisane strukturze bezpieczeństwa OUK nie zawsze jednak mają charakter operacyjny i nie zawsze będą one pozostawały w zakresie odpowiedzialności już istniejących w firmach SOC, które dzisiaj nie zajmują się wyłącznie usługą kluczową i na pewno nie jej pełnym spektrum (np. SOC, jako jednostka operacyjna nie powinna, co do zasady zarządzać ryzykiem, nie zawsze też jest odpowiedzialna za obszar utrzymania i eksploatacji systemów teleinformatycznych). W praktyce w ramach całościowego zarządzania bezpieczeństwem angażowane są różne obszary, dla których odpowiedzialność za część zadań związanych z usługą kluczową jest jedynie ułamkiem działalności. Tym samym nie jest powoływany SOC, jako jednolita struktura dedykowana wyłącznie usłudze kluczowej. Takie rozwiązanie, w przypadku wielości usług i dużej skali działania byłoby rażąco nieefektywne i nieskuteczne. Wprowadzenie powyższego wymagania może się wiązać w praktyce z koniecznością reorganizacji i przebudowy przyjętego modelu zarządzania usługą kluczową i jej bezpieczeństwem. Nie znajdujemy racjonalnego uzasadnienia dla tak daleko idącej ingerencji państwa w strukturę podmiotów. **Postulaty:** o Zwrot SOC jest powszechnie używanym określeniem dla centrów operacyjnych bezpieczeństwa, również w zdecydowanie szerszym niż cyberbezpieczeństwo zakresie. W naszej ocenie na potrzeby usługi kluczowej należy pozostawić dotychczasowe	aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.

			nazewnictwo dla struktury wewnętrznej, a wobec usług zewnętrznych użyć innego, bardziej precyzyjnego określenia, jak np. SOC-OUK lub podobnego akronimu, który jasno wskaże, że chodzi o SOC dla Operatora Usługi Kluczowej. ○ Ewentualnie należy doprecyzować, że SOC w rozumieniu art. 14 może mieć również formułę opisanej w dokumentacji wewnętrznej, rozproszonej struktury bezpieczeństwa. ○ Należy rozwiązać potencjalny problem, jaki będzie występował w przypadku powołania (np. w formie zamówienia publicznego) zewnętrznego SOC. Dopiero taki zewnętrzny SOC dokona oceny potrzeb w zakresie środków technicznych i organizacyjnych i tym samym w zależności od dokonanej oceny będzie potrzebował środków na ich wdrożenie, które powinien zapewnić zamawiający usługę OUK. Na tym tle mogą występować konflikty i różnice zdań, które mogą być problematyczne również z uwagi na budżetowanie w ramach zamówień publicznych i jego ograniczoną elastyczność. ○ W art. 14 ust. 3 pkt 4 słowo „jakością" proponujemy zastąpić słowem „skutecznością". ○ W art. 14 ust. 5 proponujemy doprecyzować, że dostęp jest zapewniany w „uzasadnionych przypadkach", a także postulujemy dodanie zwrotu, że: „*Dostęp operatora usługi kluczowej do systemów podmiotu świadczącego usługę SOC nie może prowadzić do naruszenia tajemnic prawnie chronionych, do których przestrzegania podmiot*	

			świadczący usługę SOC jest zobowiązany na podstawie przepisów prawa lub zawartych umów."	
228.	Federacja Przedsiębiorców Polskich	Art. 14 ust. 2	Projektowany przepis art. 14 ust. 2 budzi wątpliwość, czy możliwe będzie powierzanie (zawieranie umów) poszczególnych zadań rożnym podmiotom. Projektowane obecnie brzmienie sugeruje, że zlecenie może dotyczyć tylko całość zadań SOC. W związku z powyższym powyższy przepis powinien być zmieniony, aby nie pozostawiać wątpliwości, że możliwe będzie zlecanie różnych zadań, z jednoczesnym utrzymaniem SOC w ramach własnej struktury.	**Wyjaśnienie** Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.
229.	KGHM/Związek Pracodawców Polska Miedź	14. 2	W 14.2 daje się możliwość realizacji zadań SOC poprzez zlecenie ich innemu podmiotowi. Zapis nie precyzuje, że jest możliwe częściowe wyotsourcowanie niektórych jedynie zadań SOC. Wg opiniodawcy konieczne jest doprecyzowanie – umożliwienie częściowego outsourcingu. Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury lub zawiera umowę dotyczącą prowadzenia SOC w zdefiniowanym przez niego zakresie działań i na jego zlecenie z innym podmiotem.	**Wyjaśnienie** Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.
230.	Bank Handlowy Pan Szymon Kurnicki	Art 14 2.	Z uwagi na szerokie spektrum działania SOC, częstą praktyką jest model mieszany, w którym część zadań wykonywanych jest w ramach wewnętrznych struktur cyberbezpieczeństwa a część zlecana podmiotom zewnętrznym. Rozumiemy, że zgodnie z brzmieniem cytowanego ust. 2 ustawodawca dopuszcza model hybrydowy działania SOC tj. SOC działający w ramach organizacji OUK przy jednoczesnym powierzeniu wykonaniu części zadań SOK podmiotom zewnętrznym. Zasadnym jest potwierdzenie, że taki model jest dopuszczalny. Jeśli tak, to celem uniknięcia wątpliwości zwracamy się z prośbą o potwierdzenie, czy w takiej	**Wyjaśnienie** Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.

			sytuacji należy rozróżnić jednoczesne funkcjonowanie dwóch SOC tj. wewnętrznego oraz zewnętrznego.	
231.	Związek Banków Polskich	Art. 14 ust. 3	3. **SOC**, na podstawie przeprowadzonego szacowania ryzyka, **wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji**, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu **[ucięte w uwagach – uwaga DC KPRM].** SOC to zgodnie z definicją „zespół pełniący funkcję operacyjnego centrum bezpieczeństwa w danym Podmiocie". Odpowiedzialność za wprowadzanie konkretnych zabezpieczeń powinno zostać przypisane do OUK a nie do pojedynczego zespołu w ramach OUK, ponieważ SOC może nie mieć odpowiednich umocowań do wprowadzania konkretnych zabezpieczeń. Niezależnie zakres zadań który stawiany jest przed SOC może wykraczać poza ramy zadań SOC u konkretnego OUK co może powodować trudności związane z dopasowaniem struktury organizacyjnej do wymogów ustawy. W szczególności zadania związane z projektowaniem konkretnych zabezpieczeń mogą być realizowane przez role Architektów bezpieczeństwa które nie muszą być umieszczone w SOC. **Proponujemy uchylić ust. 3**	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.

232.	Krajowy Depozyt Papierów Wartościowych	Art. 14 ust. 3	Zgodnie z propozycją treści ust. 3 *„SOC, na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji…”* Mając na względzie pierwszy wariant funkcjonowania SOC przewidziany we wcześniejszym ust. 2 (*„Operator usługi kluczowej powołuje SOC wewnątrz swojej struktury”*), niewłaściwym wydaje się założenie, że taki SOC będzie mógł sam wprowadzić jakiekolwiek zabezpieczenia czy też podejmować inne tego rodzaju decyzje. Jako część struktury organizacyjnej operatora usługi kluczowej może raczej posiadać te zabezpieczenia, których wprowadzenia dokonać może wyłącznie sam operator. W związku z tym proponujemy, aby art. 14 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa brzmiał: *„SOC, na podstawie przeprowadzonego szacowania ryzyka, posiada zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji…”*	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
233.	KIGEIT	art. 14 ust. 3	**Propozycja zmiany:** *3. SOC, ~~na podstawie przeprowadzonego szacowania ryzyka, wprowadza zabezpieczenia zapewniające~~ nadzoruje i uczestniczy*	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur

			we wprowadzaniu zabezpieczeń zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów, w celu: *1) monitorowania i wykrywania incydentów;* *2) reagowania na incydenty;* *3) zapobiegania incydentom;* *4) zarządzania jakością zabezpieczeń systemów, informacji i powierzonych aktywów;* *5) aktualizowania ryzyk ~~w przypadku zmiany struktury organizacyjnej, procesów i technologii~~, które mogą wpływać na reakcję na incydent.* **Uzasadnienie:** Propozycja zmian w celu zapewnienia elastycznej pracy SOC i możliwości reagowania na bieżące zagrożenia niezależnie od procesu szacowania ryzyka i zmian w strukturze organizacyjnej	odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
234.	Bank Handlowy Pan Szymon Kurnicki	Art. 14 4.	Z uwagi na nowe obowiązki wynikające z nowelizacji ustawy, w szczególności związane z obowiązkiem powołania przez OUK operacyjnych centrów bezpieczeństwa koniecznym wydaje się doprecyzowanie w jakim terminie OUK zobowiązani są do ich powołania. Biorąc pod uwagę wskazany termin wejścia ustawy w życie tj. 21 grudnia 2020 r. rozumiemy, że dotyczy on SOC	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa".

			działających w ramach struktury wewnętrznej OUK. Nie jest jednak jasne w jakim terminie należy powołać SOC zewnętrzny jeżeli OUK zdecyduje się na podpisanie umowy z innym podmiotem. Tym samy koniecznym jest doprecyzowanie i wyjaśnienie jaki jest termin na powołanie SOC oraz jaki jest termin na podpisanie umowy z zewnętrznym SOC. Dodatkowo, z uwagi na brak ustalonego trybu komunikacji z organem właściwym ds. Cyberbezpieczeństwa tj. z Ministrem Cyfryzacji należy określić w jaki sposób OUK ma dokonać zgłoszenia takiej umowy do Ministerstwa cyfryzacji.	
235.	Transition Software	Art.14 ust. 5 pkt 3	Przestawić miejscami słowa „przechowywanych" i „danych". Zdanie powinno mieć docelowe brzmienie: „minimalizację danych przechowywanych poza bezpiecznym środowiskiem".	**Uwaga nieuwzględniona** Szyk zdania jest właściwy.
236.	Krajowy Depozyt Papierów Wartościowych	Art. 14 ust. 6	Zgodnie z propozycją treści ust. 6 *„Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności…"* W naszej opinii niniejszy przepis powinien brać pod uwagę również sytuację często spotykaną w grupach kapitałowych, w których dany podmiot świadczy określone usługi, np. informatyczne czy w zakresie cyberbezpieczeństwa, ale wyłącznie na potrzeby podmiotów należących do tej grupy kapitałowej. Taki podmiot, sam niebędący operatorem usługi kluczowej, ale świadczący usługi operatorowi wchodzącemu w skład grupy kapitałowej, nie zamierza ani nie jest przygotowany do tego, aby świadczyć takie usługi szerokiemu odbiorcy, co uzasadniałoby potrzebę udostępniania na stronie internetowej informacji na temat jego działalności jako SOC. Zaistniała sytuacja, w której podmiot ten świadczy usługi SOC, wynika wyłącznie ze sposobu zorganizowania procesów wewnętrznych w ramach powiązanych kapitałowo podmiotów, które organizacyjnie stanowią wspólną	**Uwaga nieuwzględniona** W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350.

			całość (a SOC działa wyłącznie wewnątrz tej całości, której integralną częścią jest operator usługi kluczowej). Naszym zdaniem w takim przypadku obowiązek publikowania na stronie internetowej informacji na temat działalności SOC nie powinien mieć zastosowania.	
237.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 14 ust. 6	proponuje się pozostawienie obecnego wymogu dla podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa, jakim jest publikacja RFC2350. Publikacja RFC2350 była wymogiem w akcie wykonawczym do zmienianej ustawy i w większości przypadków został on zrealizowany, ponadto RFC2350 stanowi uznany standard w społeczności zespołów reagowania na incydenty komputerowe i warto ten standard utrzymać, nie nakładając na te podmioty dodatkowych obciążeń związanych z publikacją odmiennego zakresu informacji lub tych samych informacji w różnych formach. Trudno o wyjaśnienie i wskazanie uzasadnienia czemu SOC-i mają publikować informacje takie jak np. wymagana w pkt 2 lit. c polityka komunikacji i uwierzytelnienia informacji. Rozsądnym wydaje się powrót do obecnie obowiązującego wymogu publikacji dokumentu RFC2350	**Wyjaśnienie** W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350.
238.	Polskie Centrum Badań i Certyfikacji	Art. 14 ust. 6	Proponujemy zmienić zapisy art. 14 ust. 6 KSC na następujące: „6. Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności: 1) nazwa SOC; 2) dane kontaktowe, w tym: a) adres ze wskazaniem strefy czasowej, b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC. **<u>Komentarz (uzasadnienie) do art. 14 ust. 6 nowelizacji KSC</u>**	**Wyjaśnienie** W tym zakresie ustawa nawiązuje do praktyki rynkowej – udostępniania informacji według dokumentu RFC2350.

			W uzasadnieniu poszczególnych przepisów materialnych, ustawodawca wskazuje, iż cyt.: *„Nawiązując do praktyki obecnej na rynku podmioty trzecie świadczące funkcje SOC udostępniają na stronie internetowej podstawowej informacje o swojej działalności.”.* Konsekwencją powyższego, jest zaproponowanie regulacji art. 14 ust. 6 KSC, w którym ustawodawca wymienia elementy jakie SOC winien udostępnić na swojej stronie internetowej, przy czym w części „uzasadnienie poszczególnych przepisów materialnych” nie wyjaśnia przesłanek, którymi kierował się formułując wyszczególniony w niniejszym przepisie katalog. W opinii komentatora katalog ten jest nieprecyzyjny i zbyt szeroki. Dla przykładu – w projektowanym art. 14 ust. 6 pkt 2 lit. b i lit. c oraz pkt 3 ustawodawca wskazuje następująco: Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej posiadane przez siebie kompetencje (art. 14 ust. 6 pkt 1 KSC), zasady współpracy i wymiany informacji (art. 14 ust. 6 pkt 2 lit. b KSC), politykę komunikacji i uwierzytelniania informacji (art. 14 ust. 6 pkt 2 lit. c KSC), oferowane usługi, w tym politykę obsługi incydentów i koordynacji incydentów (art. 14 ust. 6 pkt 3 KSC) oraz (art. 14 ust. 6 pkt 4 lit. c i lit. d KSC). Ujawnienie w/w zakresu informacji nie odpowiada zasadom cyberbezpieczeństwa, gdyż ujawnia zastosowane zabezpieczenia, metody szyfrowania, metodologię pracy, środki techniczne i organizacyjne w podmiotach obsługiwanych przez SOC, oraz nie odpowiada zasadom konkurencyjności wolnego rynku, a wręcz ujawnia tajemnicę przedsiębiorstwa oraz zastosowane know-how. Przedstawienie w/w informacji pozwala zidentyfikować słabe punkty zabezpieczeń oraz ich metod zastosowanych przez SOC względem	

			operatorów usług kluczowych, których *de facto i de iure* ma chronić i zabezpieczać. Dostęp cyberprzestępców do wiadomości o stosowanych metodach zabezpieczeń jest niczym nieskrępowany i pozwalający już od razu przejść do poszukiwanie sposobów ich przełamania, zamiast ewentualnej początkowo identyfikacji technologii, a następnie poszukiwania sposobów jej obejścia. Powyższe elementy winny pozostawać tajemnicą SOC działającego wewnątrz struktury operatora usługi kluczowej lub tajemnicą przedsiębiorstwa działającego w ramach SOC, w tym umowy z operatorem usługi kluczowej na rzecz którego świadczona jest usługa, ewentualnie pozostawać podawane do wiadomości podczas kontroli dokonywanej przez organ nadzorczy – organ właściwy do spraw cyberbezpieczeństwa. Ograniczony dostęp do w/w informacji jest uzasadniony tym bardziej, że wskazuje się w „uzasadnieniu poszczególnych przepisów materialnych": *„Do wykazu* [od komentatora: prowadzonego przez ministra właściwego do spraw informatyzacji] *mogą być wpisane SOC, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk.".* Cytowany fragment, jak i przepisy nowelizacji KSC, wskazują wyraźnie na dopuszczenie podmiotów wolnorynkowych do krajowego systemu cyberbezpieczeństwa, w związku z czym również ze względów tajemnicy przedsiębiorstwa w zakresie dotyczącym ich metodologii pracy, umiejętności, zasobów kadry	

			pracowniczej, elementy o których mowa w art. 14 ust. 1, ust. 6 pkt 2 lit. b i lit. c, pkt 3 oraz pkt 4 lit. c i lit. KSC nie mogą być powszechnie dostępne. Powszechna, łatwo dostępna wiedza w zakresie wskazanymi przepisami pozwoli kopiować stosowane metody, „podkupować" kadrę pracowniczą (tj. dopuszczać się czynów nieuczciwej konkurencji), a tym samym dopuszczać do rynku podmioty nieodpowiednio przygotowane do pełnienia funkcji SOC, których eliminacja przez operatora usługi kluczowej na etapie wyboru kontrahenta będzie de facto niemożliwa. Wpłynie to negatywnie na podmiot i sam sektor mający być rzekomo poddany ochronie przepisami KSC.	
239.	Transition Software	Art.14 ust.7, pkt 2), Art. 26, ust. 3, pkt 9)	Bezpieczeństwo osobowe osób pracujących/świadczących usługi w podmiotach SOC/CSIRT obsługujących podmioty infrastruktury krytycznej powinno być zweryfikowane i potwierdzone przez odpowiednie służby przed faktycznym rozpoczęciem świadczenia przez nich obowiązków pracy/usług w SOC/CSIRT. Zaleca się przeprowadzenie przynajmniej postępowania podstawowego wobec każdej osoby rozpoczynającej świadczenie obowiązków. Również z uwagi na potencjalną klauzulę informacji stanowiących tajemnicę przedsiębiorstwa (tj. może się zdarzyć, że informacja stanowiąca tajemnicę danego przedsiębiorstwa będzie jednocześnie oklauzulowana jako niejawna). Personel SOC/CSIRT musi być wcześniej zweryfikowany i przygotowany na taką okoliczność, tj. posiadać poświadczenie bezpieczeństwa osobowego przynajmniej równe klauzulą, jaki mogą posiadać potencjalne otrzymywane dane. Przy uwzględnieniu outsourcingu również należy sprawdzić - przez dedykowane służby – bezpieczeństwo osobowe personelu, który będzie miał wykonywać powierzone prace. Przed rozpoczęciem świadczenia obowiązków, musi on posiadać	**<u>Wyjaśnienie</u>** O dostępie do informacji wrażliwych np. tajemnicy przedsiębiorstwa decyduje dany przedsiębiorca.

			aktualne poświadczenie bezpieczeństwa, o stopniu przynajmniej równym do klauzuli potencjalnych otrzymywanych informacji niejawnych. Powinien zostać zachowany bezpieczny łańcuch dostaw sprzętu i oprogramowania dla SOC/CSIRT, w obszarze ICT (PC, data center, storage, laptopy, telefony i inne urządzenia mobilne). Jeżeli weryfikacja pod kątem bezpieczeństwa każdego egzemplarza sprzętu wykorzystywanego przez SOC/CSIRT nie jest to możliwa - np. z powodów logistycznych, w kontekście skali i ilości podmiotów – to dedykowane służby (np. trzy główne CSIRT: MON, GOV, NASK) we współpracy powinny przekazać wytyczne/standardy (np. w sposób niepubliczny, wyłącznie do wskazanych podmiotów), jakie musi spełniać sprzęt i oprogramowanie wykorzystywane w SOC/CSIRT i sposoby ich konfiguracji/zabezpieczenia. Wdrożenie i stosowanie tych wytycznych musi podlegać okresowemu audytowi przez ww. główne CSIRTy lub ich podwykonawców, związanych odpowiednimi umowami poufnościowymi. Powinno to być wprowadzone w ramach wdrażania Narodowych Standardów Cyberbezpieczeństwa, wzmiankowanych w *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (Uchwała nr 125 Rady Ministrów z dn. 22 października 2019r.)	
240.	ISSA Polska	Art. 14a pkt 7	Proponujemy dla projektowanego artkułu „14a.” w zakresie punku 7. o treści: „7. Minister właściwy do spraw informatyzacji może na wniosek zainteresowanego przedsiębiorcy lub z urzędu, wpisać do wykazu, o którym mowa w ust. 1, SOC inny …”	**Uwaga nieuwzględniona**, dotychczasowa redakcja jest jasna.
241.			Przyjęta w art. 14a ust. 7 konstrukcja wpisania przez ministra danego SOC z urzędu budzi wątpliwości. Czy przesłanki wskazane w ust. 2 mają być spełnione łącznie? Prośba o uzasadnienie	**Wyjaśnienie**

			wymagania dotyczącego przedstawienia dokumentu potwierdzające zdolność do ochrony informacji niejawnych przez ten podmiot – w odniesieniu do SOC-ów takiego wymagania (słusznie!) nie zdefiniowano.	Przesłanki mają być spełnione łącznie. Chodzi o możliwość dodania do KSC takiego SOC, który nie świadczy usług na rzecz operatora usługi kluczowej.
242.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 14a	Nie jest jasny cel w jakim został wprowadzony. Po pierwsze informacja o SOC, z którymi OUK zawarł umowę jest przekazywana przez OUK organowi właściwemu, nie jest zatem konieczne tworzenie kolejnych obciążeń administracyjnych w postaci wnioskowanie o ujęcie w wykazie (art. 14a ust. 3), wystarczającym wydaje się przekazanie tej informacji ministrowi właściwemu do spraw informatyzacji. Po drugie, nie jest jasny cel wpisywania SOC „z urzędu" oraz czy ten przepis dotyczy SOC, z którymi OUK zawarł umowę czy SOC powołany wewnątrz swojej struktury. Po trzecie przepis w ust. 7 pkt 1 tworzy kolejny zestaw usług dla SOC z niecodzienną usługą „aktualizowania ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent", a w pkt. 2 wymóg, który nie ma zastosowania do innych SOC-ów niż wpisywane z urzędu, przy czym wyraźnie należy zaznaczyć, że zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych jest wymogiem nadmiarowym i nieuzasadnionym, gdyż taka zdolność powinna wynikać z faktu lub przewidywanego przetwarzania informacji niejawnych.	**Wyjaśnienie** Przepis jest niezbędny, aby minister właściwy do spraw informatyzacji mógł wypełniać swoje uprawnienia nadzorcze wobec SOC.
243.	Home.pl	Art. 14 Art. 14a	Do krajowego systemu cyberbezpieczeństwa planuje się wprowadzić pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: ,,SOC" (Security operations center). Zastąpią one dotychczasowe struktury odpowiedzialne za cyberbezpieczeństwo operatora usług kluczowych. Do tej pory operator usługi kluczowej mógł powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawierał umowę z	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo" oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa". SOC będą realizowały zadania, które obecnie są realizowane przez

			podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (art. 14). Po nowelizacji operator usługi kluczowej może powołać SOC wewnątrz swojej struktury lub zawrzeć umowę prowadzenia SOC z innym podmiotem. Minister właściwy do spraw informatyzacji będzie prowadził wykaz, do którego będą wpisywane podmioty SOC (art. 14a). Dotychczasowe centra SOC w ocenie ustawodawcy posiadają ugruntowaną na rynku pozycję struktur realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek. **Uwagi w ramach konsultacji:** - do art. 14a ust. 3: w sposób nieprecyzyjny wskazują, czy każdy SOC będzie musiał zostać ujęty w wykazie SOC, czy tylko te SOC, które w ramach outsourcingu świadczą usługi na rzecz operatora usługi kluczowej – należy w trybie konsultacji publicznych zwrócić się o korektę przepisów precyzującą tę kwestię - do art. 14 ust. 1-3: zmiany dot. wymogów związanych z wdrożeniem SOC. Jeżeli wdrożenie zmian będzie się wiązało z istotnymi kosztami dla OUK, należy rozważyć zgłoszenie w trybie konsultacji publicznych postulatu zawarcia w ustawie nowelizującej przepisów dot. rekompensat dla operatorów usługi kluczowej, bądź zmianę przepisów umożliwiającą redukcję kosztów wdrożenia zmian.	wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.
244.	ISSA Polska	Art. 14a ust 7	Proponujemy dla projektowanego artkułu „14a.” w zakresie ustępu 7. dodać punkt 4) „złożyć oświadczenie w zakresie spełniania warunków technicznych określonych w rozporządzeniu Ministra właściwego do spraw informatyzacji”	**Uwaga nieuwzględniona** W związku z całkowitym nowym brzmieniem nie będzie już obowiązywało rozporządzenie z art. 14 ksc
245.	Politechnika	Art. 14a ust. 7	Zawarta w Projekcie zmiana w **pkt. 11)** wprowadzająca **art. 14a ust. 7** do Ustawy o KSC, stawia warunek na uzyskanie przez SOC	**Wyjaśnienie**

	Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe		dostępu do systemu teleinformatycznego, o którym mowa w art. 46 Ustawy o KSC, w postaci dokonania wpisu przez Ministra właściwego do spraw informatyzacji do wykazu SOC. Z kolei dokonanie wpisu do ww. wykazu dla SOC innego niż określony w art. 14a ust. 3, warunkowane jest m.in. przez **art. 14a ust. 7 pkt. 2**, zgodnie z którym SOC: *„2) przedstawi dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) oraz;* *„* Zapis ten nie precyzuje o jakiej klauzuli tajności informacji niejawnych jest mowa (zastrzeżone, poufne, tajne, ściśle tajne). Równocześnie, ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych w art. 54. [Zdolność do ochrony informacji niejawnych] mówi o przeprowadzeniu audytu przemysłowego w podmiocie, nie części podmiotu, jaką stanowiłby SOC działający w strukturach Uczelni. Jeżeli Uczelnia posiada kancelarię tajną uprawnioną do przetwarzania informacji niejawnych o klauzuli tajności „zastrzeżone", to zgodnie z art. 54 ust. 9 oraz art. 55 ust. 1 nie posiada świadectwa bezpieczeństwa, gdyż dla tej klauzuli tajności takowe nie jest przez ABW wydawane. Skoro w omawianym **art. 14a ust. 7 pkt. 2**. dokument jest wymagany, wydaje się, że oznaczałoby to konieczność wydania Uczelni przez ABW świadectwa o zdolności do ochrony informacji niejawnych o klauzuli tajności „poufne" lub wyższej. Nie jest jasne czy taka była intencja autora omawianego punktu. Proponuje się doprecyzowanie zapisu w odniesieniu do charakteru wymaganego dokumentu i/lub dopuszczenie przedstawiania przez SOC poświadczeń bezpieczeństwa osób stanowiących jego personel.	Przepis ten dotyczy SOC znajdujących się poza krajowym systemem cyberbezpieczeństwa, które mogą być włączone w jego skład.

246.	SayF	Art. 14a ust 10	Proponujemy odwołać się do artykułów w ustawach dotyczących konkretnej służby., np. art. 20c ust 2 ustawy o policji, art. 10b ust 2 ustawy o służbie granicznej, art. 30 ust 2 ustawy o żandarmerii wojskowej itd.	**Uwaga nieuwzględniona** przepis opiera się o dotychczasową sprawdzoną praktykę z art. 7 ust.8.
247.	Santander	Strona 8 pkt. 10	Określenie „*niezbędnym*" jest mało precyzyjne i rodzi ryzyko nadużyć. Adresy, gdzie prowadzony jest SOC powinny być ściśle strzeżone, gdyż mają wpływ na bezpieczeństwo tych podmiotów jak również całego rynku, w naszym przypadku finansowego, oraz Państwa. Przykładowo nie widać silnego uzasadnienia dostępu dla KAS.	**Uwaga nieuwzględniona** przepis opiera się o dotychczasową sprawdzoną praktykę z art. 7 ust.8.
248.	Transition Software	Art. 15, ust. 2, pkt 3	Należy rozważyć, czy CSIRT sektorowy lub podsektorowy powinien w interwale 2 letnim, audytować system, który sam zabezpiecza i/lub nadzoruje, jako jednostka cyberbezpieczeństwa dedykowana do ochrony danego sektora/podsektora? Czy nie powinna raz na dwa lata tego jednak robić jednostka nadrzędna, adekwatny do obszaru jeden z trzech głównych CSIRTów (NASK, GOV, MIL), NIK, lub jednostka akredytowana, o której mowa w tym samym art. w ust. 2 pkt 1)?	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji
249.	Transition Software	Art. 15, ust. 2, pkt 3	Rozporządzenie Ministra Cyfryzacji z dn. 12 października 2018r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu powinno również zawierać punkt wymieniający poświadczenie bezpieczeństwa osobowego o klauzuli nie niższej niż audytowany system. Ww. punkt miałby zastosowanie wszędzie tam, gdzie system świadczący usługę kluczową przetwarza również informacje niejawne. Potencjalnie taka sytuacja może mieć miejsce (np. w MON, w służbach, etc.). Częściowo jest to wzmiankowane w pkt.4) tego samego ustępu, jednak jest to ujęte w kontekście nie ujawniania wyników audytu,	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji

			a nie w kontekście spełniania wymogów do jego przeprowadzenia.	
250.	SayF	Art. 15 ust 4 Art. 37 ust 4 Art. 40 ust 3	W naszej ocenie zapis jest niepotrzebny. Kwestie zachowania określonych informacji w tajemnicy regulują odrębne ustawie np. ustawa o ochronie informacji niejawnych, ustawa o ochronie danych osobowych, ustawa o zwalczaniu nieuczciwej konkurencji itd.	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji
251.	Transition Software	Art. 15 ust. 6	Czy należy to rozumieć tak, że w przypadku posiadania przez danego operatora kluczowego zespołu audytorów wewnętrznych i przeprowadzania przez niego okresowego (co 2 lata) audytu wewnętrznego własnymi siłami, nie jest on zobowiązany do przechodzenia - w zasadzie nigdy w takim razie – jakichkolwiek audytów zewnętrznych, tj. przez jakąkolwiek jednostkę nadrzędną/nadzorującą, lub akredytowaną jednostkę uprawnioną do wykonywania tego typu audytów?	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji
252.	Transition Software	Art. 15, ust. 7	Jest tu jasno opisane, że kopia raportu jest przedstawiana wymienionym trzem podmiotom, na ich wyraźny i uzasadniony wniosek. Należy rozważyć wprowadzenie obligatoryjnego przesyłania co 2 lata kopii tego raportu bezpiecznym kanałem do wskazanych odbiorców oraz – ew. – NIK? Wtedy istniałaby możliwość jakiejś, wyrywkowej nawet, okresowej weryfikacji poszczególnych raportów lub zbioru raportów, co powinno dać możliwość uzyskania jakiegoś zbiorczego obrazu sytuacji, choćby bardzo zgrubnego. Może zaistnieć sytuacja, że nawet przez kilka kolejnych interwałów żaden z wymienionych podmiotów nie zwróci się ze wspomnianym uzasadnionym wnioskiem odnośnie raportów np. danych konkretnych organizacji (banków, energetyki, administracji, produkcji, w tym produkcji specjalnej, etc.) i	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji

			kolejne audyty – przeprowadzane przez operatorów kluczowych własnymi siłami, w ramach struktury własnej organizacji i na własnym obszarze – nie będą w żaden sposób weryfikowane przez instytucje nadrzędne/wyznaczone, etc.	
253.	SayF	Art. 17 ust 1	Dlaczego wyklucza się mikro i małych przedsiębiorców?	**Uwaga nieuwzględniona** Uwaga nie jest do projektu nowelizacji
254.	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM Reprezentowany przez adw. Annę Gąsecką	art. 39 PKE i art. 20a ustawy o krajowym systemie cyberbezpieczeństwa, art.43 ust. 2 i 3 PKE i art. 20e ustawy o krajowym systemie cyberbezpieczeństwa art. 44 ust.1 PKE i art. 20f ustawy o krajowym systemie cyberbez	Niejasny jest stosunek projektowanych przepisów do zapisów projektu Prawa Komunikacji Elektronicznej (dalej PKE). Oba akty regulują tę samą materię, a część projektowanych przepisów jest tożsama.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w

		pieczeństwa		zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
255.	PIIT	Art. 20a	**Art. 20a, art. 2 pkt 8f, 8g** Proponowany przepis stanowi kopię projektowanego art. 39 ustawy PKE. Aktualne są więc uwagi przedstawione w tym zakresie do projektu PKE, w szczególności w zakresie upoważnienia ustawowego do wydania rozporządzenia dot. warunków technicznych i organizacyjnych, w tym wyjaśnienia statusu obowiązującego rozporządzenia do art. 175d PT, którego moc obowiązująca nie jest w projekcie PKE utrzymywana. Jedyna zmiana art. 20a to dodanie odwołań niezbędnych, aby wprowadzić ten przepis do ustawy KSC. Jednocześnie zupełnie niezrozumiała jest intencja powtarzania tego samego przepisu w dwóch projektowanych aktach prawnych, a tym bardziej utrzymywanie dwóch podstaw prawnych do wydania rozporządzenia w potencjalnie tym samym zakresie. **Postulaty:** W zakresie art. 20a należy: • Wykreślić przepis z projektu ustawy nowelizującej KSC i zachować go w PKE ze zmianami zaadresowanymi w stanowisku PIIT przekazanym w konsultacjach projektu PKE.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

			• W przypadku zamiaru dodatkowego podkreślenia potrzeby uwzględniania incydentów w rozumieniu KSC, tj. incydentów cyberbezpieczeństwa można podkreślić ten aspekt w projekcie PKE. • Wykreślić z KSC związane z art. 20a definicje, które miałyby być dodane w art. 2 pkt 8f-g, czyli definicje bezpieczeństwa sieci i usług oraz sytuacji szczególnego zagrożenia. W przypadku braku usunięcia ww. definicji z projektu KSC definicję bezpieczeństwa sieci i usług (8f) należy zapisać tak jak definicję sytuacji szczególnego zagrożenia (8g) tj. przez odwołanie do definicji PKE. • W zakresie brzmienia definicji bezpieczeństwa sieci i usług ponawiamy uwagę przedstawioną w tym zakresie do stanowiska do PKE, tj. jej niespójności z EKŁE: *Definicja bezpieczeństwa sieci i usług w projekcie PKE różni się od definicji wskazanej w EKŁE* <u>Definicja z PKE</u>: *„bezpieczeństwo sieci i usług – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:* *a) tych sieci lub usług,* *b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,* *c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy”* <u>Definicja z EKŁE</u> *„bezpieczeństwo sieci i usług” oznacza zdolność sieci i usług łączności elektronicznej do odpierania,* ***<u>na danym poziomie pewności</u>****, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci i usług, przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez te sieci lub usługi łączności elektronicznej lub dostępnych za ich pośrednictwem*;	incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.

			Prośba o wskazanie argumentacji leżącej u podstaw pominięcia w definicji określenia „na danym poziomie pewności". Naszym zdaniem wskazanie przez europejskiego prawodawcę w ww. definicji określenia jest celowe i koresponduje z koncepcją dostosowania zabezpieczeń do wyników analizy ryzyka – motyw 94 „Środki te powinny zapewniać poziom bezpieczeństwa sieci i usług proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii". Kategoryczne sformułowanie zdolności do odpierania wszelkich działań oznaczałoby de facto obowiązek zapewnienia 100% odporności. Taki poziom wydaje się nierealny do osiągnięcia nie tylko dla operatorów telekomunikacyjnych, ale i nawet dla najbardziej zabezpieczonych systemów służb i organów państwowych. Stąd niezbędne jest doprecyzowanie zgodne z EKŁE	
256.	PIIT	Art. 20b-d	**1.1. Art. 20b-d, art. 2 pkt 8a** Proponowane przepisy art. 20b-d wraz ze związanymi z nimi definicjami: incydentu telekomunikacyjnego i CSIRT Telco stanowią znaczącą modyfikację dotychczasowego sposobu działania przedsiębiorców telekomunikacyjnych w zakresie obsługi incydentów, w tym w zakresie incydentów cyberbezpieczeństwa. Zgodnie z obowiązującym prawem telekomunikacyjnym, system, który miał być przeniesiony również na grunt PKE jest następujący. Przedsiębiorca, zgodnie z art. 175a ma obowiązek niezwłocznego poinformowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności, podjętych działaniach zapobiegawczych i środkach naprawczych oraz innych działaniach w tym zakresie. W części IV.4 obowiązującego formularza raportowego przedsiębiorca określa przyczynę zaistniałego naruszenia, przy czym jedną z opcji jest wskazanie, że przyczyną był cyberatak. Jeśli natomiast zdarzenie miało charakter incydentu w rozumieniu KSC, tj. incydentu w zakresie cyberbezpieczeństwa wówczas Prezes UKE przekazywał informację właściwemu CSIRT. Prezes UKE jest też uprawniony do korzystania z systemu teleinformatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa, o którym mowa w art. 46 KSC. Jednocześnie określone w rozporządzeniu progi są uniwersalne i odnoszą się de facto do ciągłości działania	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

			usługi (czasu niedostępności) w relacji do zakresu objętych użytkowników. Tym samym aktualny stan prawny, jak i ten, który miał zostać wprowadzony w projekcie PKE zapewniają, że po pierwsze naruszenia/incydenty związane z cyberprzestrzenią będą raportowane, a po drugie informacja ta zostanie przekazana właściwym CSIRT. W projektowanym art. 45 ust. 3 PKE przewidziano również możliwość zwrócenia się przez UKE o pomoc do właściwego CSIRT, co implementuje w pełni art. 41 ust. 4 EKŁE. Należy więc wskazać, że pod kątem pełnej zgodności z przepisami unijnymi oraz z uwagi na wieloletnią już i zasadniczo bezproblemową praktykę raportowania za pożądane rozwiązanie należy uznać utrzymanie istniejącego rozdziału między regulacją właściwą przedsiębiorcom telekomunikacyjnym/komunikacji elektronicznej i ich relacji z UKE, a regulacjami właściwymi dla krajowego systemu cyberbezpieczeństwa w jego dotychczasowym zakresie. Szczególnie biorąc pod uwagę bardzo bliskie terminy wejścia w życie projektowanych obecnie przepisów oraz skalę wątpliwości i praktycznych problemów, jakie mogą wyniknąć z nakładania się na siebie obowiązków. W tym miejscu **należy spróbować zrekonstruować podstawowe elementy docelowego stanu prawnego, jaki wystąpiłby po jednoczesnym wejściu w życie nowego PKE oraz zmian KSC**, które jak zakładamy zostałyby wprowadzone do ustawy wprowadzającej PKE. Poniższe porównanie jest również istotne dla przedstawienia różnic, szczególnie w zakresie definicji incydentu, dla scenariusza w którym obowiązki raportowe miałyby zostać przeniesione z UKE do CSIRT. **[Tabela usunięta ze względu na brak miejsca – dostępna na stronie Rządowego Procesu Legislacyjnego – DC KPRM)**	incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			Podsumowując powyższe zestawienie odrębnych reżimów raportowych wyraźnie widoczne są istotne różnice na poziomie podstawowych definicji, zakresu objętych podmiotów, organów właściwych. Brak jest również aktów wykonawczych do realizacji nowych obowiązków, o których mowa w projekcie ustawy KSC. Obowiązki wobec CSIRT Telco będą niemożliwe do realizacji w istotnym okresie obowiązywania przepisów, albowiem jego powołanie ma nastąpić dopiero w okresie 18 miesięcy od wejścia w życie ustawy. Nie przewidziano w tym zakresie odpowiednich regulacji intertemporalnych. Poza powyższym, należy wskazać, że przedsiębiorcy komunikacji elektronicznej nie będą mieli możliwości przygotowania się do realizacji nowych obowiązków raportowych, a w szczególności wdrożenia odpowiednich zmian organizacyjnych i technicznych pod kątem nowych (jeszcze nieznanych) progów incydentów. **Postulaty:** • **Art. 20b-d projektu KSC powinny zostać usunięte z projektu.** Nie jest zasadne utrzymanie propozycji zakładającej dwa nakładające się reżimy zgłaszania incydentów bezpieczeństwa (PKE) i incydentów telekomunikacyjnych (KSC). Nie jest również zasadne przeniesienie przedsiębiorstw komunikacji elektronicznej pod reżim KSC. Obowiązki raportowe przedsiębiorców komunikacji elektronicznej powinny zostać utrzymane jedynie wobec Prezesa UKE, a w każdym razie powinien istnieć wyłącznie jeden kanał zgłoszeń. • **Definicja incydentu, jaki ma zgłaszać przedsiębiorca komunikacji elektronicznej musi być jedna, podobnie jak**	

			spójne muszą być kryteria dokonywania zgłoszeń – nawet, jeśli miałyby dotyczyć szerokiego spektrum sytuacji. **Ewentualne dodatkowe potrzeby w zakresie incydentów w rozumieniu ustawy KSC można zaspokoić przez odpowiednie uzupełnienie ustawy PKE lub dostosowanie praktyki działania**. Jeśli podmioty krajowego systemu potrzebują szerszej informacji, także dot. samego przerwania ciągłości bez związku z przyczyną, nie widzimy istotnych przeszkód, aby takie informacje były przekazywane przez UKE do odpowiednich CSIRT. Możliwe wydaje się również, aby te informacje były dostępne w ramach budowanego systemu S46. Ewentualnie, w przypadkach, w których przedsiębiorca kwalifikuje incydent, jako wpływający na cyberbezpieczeństwo, mógłby zostać zobowiązany do przekazywania tej samej informacji zarówno do UKE jak i właściwego CSIRT krajowego. • Ponadto, w celu potwierdzenia możliwości komunikowania o zagrożeniach postulujemy wprowadzenie do projektu PKE przepisu art. 175c ust. 5 PT, który nie został przeniesiony do PKE, a który wskazuje *przedsiębiorca telekomunikacyjny może informować innych przedsiębiorców telekomunikacyjnych i podmioty zajmujące się bezpieczeństwem teleinformatycznym o zidentyfikowanych zagrożeniach, o których mowa w ust. 1. Informacja może zawierać dane niezbędne do identyfikacji oraz ograniczenia zagrożenia.* W nowym brzmieniu przepis powinien odnosić się do przedsiębiorstw komunikacji elektronicznej oraz do podmiotów krajowego systemu cyberbezpieczeństwa.	

			• Niezależnie od przyjętego finalnie sposobu regulacji, kluczowe pozostaje, że konkretny **przedsiębiorca komunikacji elektronicznej może odpowiadać jedynie za bezpieczeństwo i integralność swoich usług i swojej infrastruktury**. Tym samym projektowane przepisy nie mogą ingerować w tą sferę skutkując nałożeniem na tych przedsiębiorców szerszych obowiązków. Byłaby to bardzo istotna ingerencja w konkurencyjny rynek rozwiązań bezpieczeństwa teleinformatycznego.	
257.	Home.pl	Art. 20a-d	Nowelizacja nawiązuje w swej treści do nowej ustawy – Prawo komunikacji elektronicznej (dalej również jak PKE), która obecnie jest w fazie prac legislacyjnych, a docelowo ma wejść w życie 21 grudnia 2020 r. Prawo komunikacji elektronicznej ma zastąpić dotychczasową ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Wprowadzenie nowej ustawy wynika z konieczności wdrożenia do polskiego porządku prawnego przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: Dyrektywa). Ustawa o KSC posługuje się pojęciami zdefiniowanymi w PKE, w tym między innymi: pojęciem „przedsiębiorca komunikacji elektronicznej”, który jest w rozumieniu projektu ustawy prawo komunikacji elektronicznej - przedsiębiorcą telekomunikacyjnym lub podmiotem świadczącym usługę komunikacji interpersonalnej niewykorzystującą numerów. Ze względu na brak jasnej definicji pojęcia „komunikacji interpersonalnej niewykorzystującej numerów nie można mieć pewności, czy podmiot będzie posiadać status przedsiębiorca komunikacji elektronicznej i w konsekwencji – czy będą do niego miały	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

			zastosowania przepisy PKE oraz nowelizacji dotyczące tej kategorii przedsiębiorców (nowy rozdział 4a „ Obowiązki przedsiębiorców komunikacji elektronicznej" wprowadzany do ustawy o KSC nowelizacją, przepisy o tzw. incydencie telekomunikacyjnym: nowy art. 2 pkt 8a ustawy o KSC itd. **Uwagi w ramach konsultacji:** - do nowego art. 20a ust. 1 ustawy o KSC: doprecyzowanie kto dokładnie jest adresatem nowelizacji w zakresie dot. przedsiębiorcy komunikacji elektronicznej.	administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
258.	PIIT	Art. 20c	1.2. Art. 20c ust. 4 wprowadza upoważnienie do wydania rozporządzenia określające progi, które jest identyczne z tym przewidzianym w art. 42 ust. 2 PKE. Uwagi w zakresie braku zrozumienia dla takiego zabiegu legislacyjnego zostały sformułowane już powyżej. Dodatkowo aktualne są poniższe uwagi przedstawione w stanowisku przekazanym do projektu PKE: W proponowanym przepisie znacznemu rozbudowaniu uległ katalog przesłanek, jakie będą brane pod uwagę przy określaniu progów istotności incydentów. W pierwszej kolejności, tak jak w uwagach ogólnych wskazujemy, że do czasu przedstawienia projektu rozporządzenia lub chociaż jego założeń nie jest możliwe dokonanie oceny wpływu zmiany upoważnienia ustawowego na działalność przedsiębiorców. Tym samym postulujemy pilne przedstawienie, przynajmniej jego założeń. Postulujemy, aby doprecyzować art. 42 ust. 2 pkt 1 lit. e, że progi mogą zostać ustalone dla „sieci telekomunikacyjnych" oraz „usług komunikacji elektronicznej". Obecnie wskazano jedynie na „sieci i usługi", co wydaje się niewystarczająco precyzyjne.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów

				Poza tym, katalog ten został określony w sposób zmodyfikowany wobec zapisów EKŁE, w szczególności poprzez nieuwzględnienie wskazanej w EKŁE przesłanki „wpływu na działalność ekonomiczną i społeczną". W to miejsce wprowadzono szeroki katalog okoliczności tj.: *e) wpływ incydentu bezpieczeństwa na zachowanie tajemnicy komunikacji elektronicznej,* *f) wpływ incydentu bezpieczeństwa na świadczenie usług kluczowych w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,* *g) wpływ incydentu bezpieczeństwa na połączenia do numerów alarmowych,* *h) wpływ incydentu bezpieczeństwa na wykonywanie obowiązków, o których mowa w art. 46-56 ustawy;* Przede wszystkim postulujemy usunięcie lit. f odnoszącej się do wpływu na usługi kluczowe oraz infrastrukturę krytyczną. W przypadku gdyby w rozporządzeniu określono odrębne progi odnoszące się wyłącznie do tego zakresu, wykonanie obowiązku zgłoszenia mogłoby być niemożliwe. Z perspektywy operatora obowiązanego do dokonania zgłoszenia trudne do ustalenia byłoby bowiem czy dany incydent miał wpływ na usługi kluczowe (lista takich operatorów nie jest jawna) tudzież infrastrukturę krytyczną (lista obiektów jest zastrzeżona). Ewentualne zgłoszenie incydentu mającego wpływ w tym zakresie byłoby faktycznie możliwe jedynie w przypadku, gdy operator posiada wiedzę w zakresie takiego wpływu lub sam jest operatorem usługi kluczowej lub posiadaczem infrastruktury krytycznej. W zakresie lit. g) podobnie jak w ramach pre-konsultacji projektu PKE postulujemy następujące doprecyzowanie: *g) wpływ incydentu na funkcjonowanie systemów alarmowania, powiadamiania ratunkowego, numery alarmowe ustawowo powołane do niesienia pomocy 997, 998, 998 i numer 112* Odnośnie lit. h) tj. odniesienia do wykonywania obowiązków, o których mowa w art. 45-56 sygnalizujemy, że daleko idące wątpliwości budzi zasadność wprowadzenia tej przesłanki. Przepisy, do których się odwołano to np. obowiązki Prezesa UKE (45-46), posiadanie planu (47), nakładania dodatkowych obowiązków (48), radioamatorów (49), zawieszania obowiązków przez Prezesa UKE (52), upoważnienia do wydania rozporządzenia (54), czy zakresu obowiązków retencyjnych (56). W naszej ocenie lit. h) powinna zostać usunięta z projektu ustawy. **Postulat:**	usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.

			• Art. 20c należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji PKE.	
259.	PIIT	Art. 20d	1.3. Zgodnie z ust. 3-5 przedsiębiorca miałby przekazywać CSIRT, w tym CSIRT Telco informacje stanowiące prawnie chronione. Podobne przepisy zawarto w projekcie PKE w art. 42 ust. 8, które budziły nasze istotne wątpliwości w przypadku przekazywania takich informacji do Prezesa UKE. W naszej ocenie przepis ten zbyt szeroko określa uprawnienia CSIRT. Tajemnice prawnie chronione to bardzo szeroki katalog, dalece wykraczający poza samą tajemnicę przedsiębiorstwa czy tajemnicę telekomunikacyjną. Kwestii tych dotyczy kilkadziesiąt ustaw znajdujących się obecnie w obrocie prawnym i może dochodzić do sytuacji, w których przedsiębiorca telekomunikacyjny nie jest zobowiązany do ich zachowania. Nie zawsze bowiem będzie on w pełni dysponentem danej informacji, tj. nie w każdym przypadku będzie dotyczyła ona wyłączenie jego samego i tym samym będzie mógł przekazać ją CSIRT bez ryzyka naruszenia praw innych podmiotów. W niektórych przypadkach, aby możliwe było przekazanie takich informacji potrzebne byłoby uzyskanie zgody sądu. Ponadto już nawet przekazanie pełnych informacji w zakresie tajemnicy komunikacji elektronicznej budzi wątpliwości, pod kątem określenia czy np. treść	**Wyjaśnienie** Przedsiębiorca komunikacji elektronicznej będzie mógł a nie musiał przekazać informacje prawnie chronione. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania

			indywidualnych komunikatów jest niezbędna CSIRT do wykonywania jego zadań. W przypadku braku utrzymania przepisów w projekcie ustawy postulujemy proporcjonalne ograniczenie uprawnienia CSIRT. W każdym jednak wypadku to CSIRT powinien być odpowiedzialny za precyzyjne wskazanie, jakie informacje, w tym ewentualne tajemnice mają zostać przekazane. Określanie tego katalogu nie może być obowiązkiem i odpowiedzialnością przedsiębiorcy. Ponadto należy określić minimalny termin na udzielenie odpowiedzi przez przedsiębiorcę, który powinien być proporcjonalny do zakresu wniosku. **Postulat:** • Art. 20d należy usunąć z projektu i przenieść dyskusję na jego temat na okres po implementacji PKE.	incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
260.	PIIT	Art. 20e	**2. Art. 20e** Proponowany art. 20e stanowi kopię projektowanego art. 43 ust. 2 i 3 PKE. Nie widzimy zasadności powtarzania tych samych przepisów w dwóch aktach prawnych, które odnosiłyby się do potencjalnie wspólnych zakresów incydentów. W przypadku utrzymania przepisów w projekcie aktualne pozostają uwagi przedstawione w tym zakresie do PKE w pkt 19-20 zestawienia uwag do PKE dot. bezpieczeństwa. **Postulat:**	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do

			• Art. 20e należy usunąć z projektu.	właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
261.	PIIT	Art. 20f	**3. Art. 20f** Proponowany art. 20f stanowi powtórzenie przepisu art. 44 ust. 1 projektu PKE, przy czym pominięto bardzo istotny dla możliwości jego realizacji ust. 2, który w projekcie PKE wskazuje, że *„2. Zastosowanie środków, o których mowa w ust. 1, nie wyklucza zastosowania środków, o których mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego internetu i dotyczące opłat detalicznych za uregulowane usługi łączności wewnątrzunijnej oraz zmieniającego dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012.”* **Postulat:**	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

			• Art. 20f należy usunąć z projektu. Aktualne pozostają również uwagi przedstawione w pkt 21-22 zestawienia uwag do PKE dot. Bezpieczeństwa.	administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
262.	PIIT	Art. 26 ust 2 i 32 ust 4	8. Art. 26 ust. 2 i art. 32 ust. 4 dot. współpracy CSIRT i przedsiębiorców Proponowany przepis daje możliwość wnioskowania do CSIRT MON, NASK, GOV o wsparcie w zakresie obsługi incydentów. W związku z powyższymi uwagami proponujemy, aby tą propozycję utrzymać w projekcie, przy czym z uwagi na postulowane wykreślenie przedsiębiorców komunikacji elektronicznej z KSC, w projektowanym przepisie należałoby odwołać się bezpośrednio do przedsiębiorców komunikacji elektronicznej, o których mowa w PKE (podobnie jak odwołano się do dysponentów infrastruktury krytycznej). Podobne rozwiązanie proponujemy przyjąć dla projektowanego art. 32 ust. 4 dot. wymiany informacji. Postulat: • Proponowane modyfikacje należy wprowadzić poprzez odwołanie do przedsiębiorców komunikacji elektronicznej, o których mowa w PKE.	**Wyjaśnienie** **Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.** **Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.** **Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.** **Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki**

				przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
263.	PIIT	Art. 26 ust. 3	9. Art. 26 ust 3 - zadania CSIRT Prowadzenie działań na rzecz podnoszenia poziomu Cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności przez: a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi i właściwymi podmiotami, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz zagrożeniach cyberbezpieczeństwa W kontekście uprawnienia wskazanego w lit. a i b – prośba o wyjaśnienie rozumienia użytego w tym punkcie określenia „właściwych podmiotów”? Jeżeli to podmioty krajowego systemu cyberbezpieczeństwa, to czy należy rozumieć, że CSIRT-y będą uprawnione do wykonywania testów bezpieczeństwa rozwiązań poszczególnych podmiotów wchodzących w skład systemu, np. SOC?	**Wyjaśnienie** **CSIRT będą mogły dokonywać testów bezpieczeństwa za zgodą podmiotu nadzorującego.**
264.	PIIT	Art. 34a	10. Art. 34a dot. współpracy CSIRT i UKE Tak jak już wskazywaliśmy, na obecnym etapie i w zakładanym terminie nie jest zasadne wprowadzanie dodatkowego mechanizmu raportowego. Postulat:	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			• W związku z powyższymi uwagami, postulujemy, aby przepis dotyczył możliwej współpracy w zakresie incydentów, które zgłaszane są do Prezesa UKE.	Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
265.	PIIT	Art. 44a	11. Art. 44a dot. CSIRT Telco Zgodnie z powyższym stanowiskiem, na tym etapie postulujemy usunięcie z projektu ustawy CSIRT Telco. Wprowadzenie regulacji dotyczących włączenia sektora komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa powinno być poprzedzone odpowiednią dyskusją z podmiotami objętymi tą regulacją. Brak wcześniejszej debaty w tym zakresie, bliski termin wejścia w życie oraz nakładanie się z regulacjami PKE byłyby w naszej ocenie bardzo szkodliwe dla takiego dialogu i wypracowania konstruktywnych rozwiązań.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.

			Ewentualne wprowadzenie CSIRT Telco wymaga pogłębionej dyskusji, której dotychczas nie mieliśmy możliwości przeprowadzić. Jednocześnie tempo prac nie jest uzasadnione żadnymi szczególnymi zdarzeniami. Postulat: • Na obecnym etapie należy wykreślić przepisy z projektu. • W ramach dyskusji o docelowym rozwiązaniu należy rozważyć możliwość wzmocnienia UKE i powołanie zespołu cyberbezpieczeństwa w jego strukturze, jako dodatkowego elementu już istniejącej struktury bezpieczeństwa. W tym celu należałoby wprowadzić możliwość powierzenia realizacji tego zadania także organowi nadzorowanemu lub wprost wskazać, że podmiotem odpowiedzialnym za realizację jest Prezes UKE.	Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
266.	PIIT	Art. 46	12. Art. 46 ust. 2b W celu wprowadzenia rozwiązania pośredniego proponujemy w ust. 2b. wskazać, że do takiego porozumienia w sprawie dostępu do systemu informatycznego może przystąpić również przedsiębiorca komunikacji elektronicznej. W razie potrzeby możliwe jest doprecyzowanie kryteriów, jakie powinien spełniać.	**Wyjaśnienie** Docelowo przedsiębiorcy komunikacji elektronicznej mają stać się podmiotami krajowego systemu cyberbezieczeństwa. Jako podmioty ksc będą mogły być dołączone do systemu z art. 46.
267.	ISACA Warsaw Chapter	Art. 20a 1.	Art. 2. Użyte w ustawie określenia oznaczają: … 17) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę wystąpienia incydentu; …	**Uwaga nieuwzględniona** Ustawa KSC uwzględnia Polskie Normy, m. in. definicja zarządzania ryzykiem nawiązuje do Normy ISO 27005.

			19) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia. Problem generalny związany z niespójnością nazewnictwa. Podaję tu jeden przykład, warto jednak, skoro mamy ustawę o PKN i mamy w Polsce polskie normy, stosować nazewnictwo i definicje w nich istniejące, a nie wymyślać kolejne znaczenia. Tym bardziej, że projekt przedmiotowej ustawy w art.42 ust. 8 mówi również o uwzględnianiu w dziedzinie cyberbezpieczeństwa polskich norm. **Przykłady:** Określenie: zagrożenie cyberbezpieczeństwa z rozdz. 2 a opis „szczególne zagrożenie z Art.20 – co znaczy szczególne? W projekcie ustawy jest definicja: szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka; W ISO 31000 definicja jest następująca: ocena ryzyka – całościowy proces identyfikacji, analizy i ewaluacji ryzyka; W ISO 27005: szacowanie ryzyka to analiza ryzyka i jego ocena ryzyka, natomiast analiza ryzyka składa się z identyfikowania, estymowania.	

			Problem obejmuje również podstawową dla ustawy definicję „cyberbezpieczeństwa”, która nie wskazuje szerszego spektrum jakim jest bezpieczeństwo informacyjne oparte na systemach zarządzania ale mówi o odporności systemów teleinformatycznych. Podobnie jest z incydentem poważnym, wielokrotnie zgłaszanym w dyskusji jako zdefiniowanym nieczytelnie. Zarówno incydent poważny jak i krytyczny w swojej interpretacji praktycznej nie mogą budzić wątpliwości.	
268.	SayF	Art. 20a ust 2 pkt 1	Proponuje się doprecyzować pojęcie „systematyczną”. Proponuje się wyraz „ocenę” zastąpić wyrazami „wykonuje szacowanie ryzyka wystąpienia incydentu co najmniej raz w roku oraz każdorazowo po wystąpieniu incydentu …… „	**Uwaga nieuwzględniona** Ocena ryzyka musi być dokonywana przed uruchomieniem sieci i usług a następnie ponawiana w przypadku zmian organizacyjnych i technicznych mogących mieć wpływ na bezpieczeństwo sieci i usług. Systematyczna ocena ryzyka powinna być prowadzona z uwzględnieniem faktu wystąpienia nowych zagrożeń, które mogą mieć wpływ na poziom oceny ryzyka. Ponadto należy wziąć pod uwagę postęp technologiczny, najbardziej aktualny stan prawny i normy techniczne.
269.	SayF	Art. 20a ust 3 pkt (nie podano)	Czy zapis ten należy rozumieć, że należy uwzględnić ust 2 pkt 1 i 2 w systematycznej ocenie ryzyka, która wynika z planu? Jeżeli przedsiębiorca nie ma obowiązku sporządzenia planu, gdzie…	**Uwaga nieuwzględniona** Przedsiębiorca ma prowadzić dokumentację zastosowanych środków technicznych i organizacyjnych a także wyników oceny ryzyka.
270.	SayF	Art. 20a ust 3	Proponuje się wykreślić art. 20a ust. 3 KSC. Rekomendujemy nie łączyć dokumentacji dotyczącej cyberbezpieczeństwa z planem działań przedsiębiorcy telekomunikacyjnego. Dokumentacja związana z cyberbezpieczeństwem powinna być	**Uwaga nieuwzględniona** Dokumentacja o której mowa w art. 20a ust 3 dotyczy wszystkich aspektów bezpieczeństwa, w tym także bezpieczeństwa fizycznego co wynika z obowiązków

			- dostępna wyłącznie osobom upoważnionym zgodnie z realizowanymi przez nie zadaniami; - chroniona przed przypadkowym zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;"; Do planów działań powinny mieć dostęp również inne osoby niż związane z cyberbezpieczeństwem. Ponadto każda zmiana zawartości planu wymaga jego aktualizacji i uzgodnienia po aktualizacji. Oznacza to, że po udokumentowaniu incydentu należy plan poddać aktualizacji i ponownie uzgodnić jego treść z właściwym organem administracji publicznej.	związanych z wdrożeniem proporcjonalnych do oszacowanego ryzyka środków bezpieczeństwa.
271.	SayF	Art. 20a ust 4	Proponuje się w ustawie doprecyzować obowiązki przedsiębiorców komunikacji elektronicznej w zakresie zastosowania środków bezpieczeństwa, o których mowa w art. 20a ust. 2 pkt 2 KSC. W rozporządzeniu (obligatoryjnym a nie fakultatywnym) ministra właściwego do spraw informatyzacji określić wyłącznie sposób dokumentowania stosowania tych środków bezpieczeństwa.	**Wyjaśnienie** Przedsiębiorcy komunikacji elektronicznicznej będą stosować wspomniane środki po przeprowadzeniu systematycznej oceny ryzyka. To wyniki oceny wskażą jakie środki należy zastosować aby zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
272.	KIGEIT	Art. 20a, 20e, 20f	**Propozycja zmiany:** wykreślenie w całości ~~*Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest*~~	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

			~~*obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia.*~~ ~~*2. Przedsiębiorca komunikacji elektronicznej:*~~ ~~*1) przeprowadza systematyczną ocenę ryzyka wystąpienia sytuacji szczególnego zagrożenia;*~~ ~~*2) podejmuje środki techniczne i organizacyjne zapewniające poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:*~~ ~~*a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, o której mowa w art. 2 pkt 14 ustawy z dnia … – Prawo komunikacji elektronicznej,*~~ ~~*b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia,*~~ ~~*c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,*~~ ~~*d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej*~~ ~~*– przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków;*~~ ~~*3) dokumentuje czynności, o których mowa w pkt 1 i 2.*~~ ~~*3. Przedsiębiorca komunikacji elektronicznej, o którym mowa w art. 2 pkt 42 ustawy – Prawo komunikacji elektronicznej, sporządzający plan, o którym mowa w art. 47 ust. 1 tej ustawy, dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2.*~~ ~~*4. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności, biorąc*~~	przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.

			~~*pod uwagę skalę działalności, wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, lub sposób ich dokumentowania, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci i usług.*~~ ~~*Art. 20e. 1. Przedsiębiorca komunikacji elektronicznej wykonujący działalność na rynku detalicznym, w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego, informuje o nim swoich użytkowników, na których takie zagrożenie może mieć wpływ, w tym o możliwych środkach, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach.*~~ ~~*2. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 1, informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.*~~ ~~*Art. 20f. W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, może zastosować środki polegające na:*~~ ~~*1) zablokowaniu przesłania takiego komunikatu,*~~ ~~*2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia*~~ **Uzasadnienie:**	

			Przepisy art. 20a konsultowanego projektu stanowią powielenie przepisów zawartych w art. 39 projektu z dnia 29 lipca 2020 ustawy – Prawo komunikacji elektronicznej, przepisy art. 20e – przepisów art. 42 ust. 2 i 3 projektu ustawy – Prawo komunikacji elektronicznej, a przepis art. 20f – przepisu art. 44 ust. 1 projektu ustawy – Prawo komunikacji elektronicznej. Delegacja dla ministra właściwego do spraw informatyzacji ujęta w art. 20a ust. 4 przedmiotowego projektu jest tożsama z delegacją zawartą w art. 39 projektowanej ustawy – Prawo komunikacji elektronicznej, a ujęta w art. 20c ust. 4 – z art. 42 ust. 2 projektowanej ustawy – Prawo komunikacji elektronicznej. Ujmowanie tych samych przepisów w różnych aktach prawnych jest niezgodne z zasadami techniki legislacyjnej. Zapewne nie było również intencją ustawodawcy, aby w systemie prawnym miały funkcjonować dwa rozporządzenia tej samej treści, wydane na podstawie upoważnień przewidzianych w dwóch różnych ustawach. W tej sytuacji proponuje się usunięcie tych przepisów z niniejszego Projektu. Na wypadek nieuwzględnienia niniejszej uwagi należy wskazać na błąd w ujętym w art. 20a ust. 3 odwołaniu do ustawy Prawo komunikacji elektronicznej – definicja przedsiębiorcy komunikacji elektronicznej ujęta jest w art. 2 pkt 41, a nie pkt 42	
273.	Signum Edward Kuś Marcin Kuś	Art. 20a-f	**Przedmiot** Projekt nie powinien mieć zastosowania bezpośrednio do operatorów telekomunikacyjnych **Ustawa** Ustawa o KSC jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatorów telekomunikacyjnych. Prawa	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			i obowiązki operatorów telekomunikacyjnych zostały szczegółowo określone w projekcie ustawy Prawo Komunikacji Elektronicznej (PKE), który implementuje Europejski Kodeks Łączności Elektronicznej (EECC). **Uzasadnienie** Dodanie przedsiębiorstwa komunikacji elektronicznej, jako podmiotu, do którego stosuje się KSC, powoduje potencjalny konflikt przepisów o randze ustawowej. Operator telekomunikacyjny jest zazwyczaj istotnym dostawcą usług dla operatorów infrastruktury kluczowej.. Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE spowoduje wątpliwości interpretacyjne. **Przepisy** art. 1 KSC art. 20a-f KSC **Sugestie** 1. Postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC. 2. KSC nie ma zastosowania do przedsiębiorstw komunikacji elektronicznej.	Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
274.	SayF	Art. 20b pkt 1	Art. 20b pkt 1 nadać brzmienie: „zapewnia zarządzanie incydentem” Pojęcie „zarządzanie incydentem” jest pojęciem szerszym, obejmującym więcej elementów działalności związanej z postępowaniem po wystąpieniu incydentu: wyszukiwanie	**Uwaga nieuwzględniona** Przedsiębiorca komunikacji elektronicznej zapewnia obsługę incydentu telekomunikacyjnego. Natomiast

			powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;	koordynacją obsługi incydentu zajmuje się CSIRT poziomu krajowego. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
275.	SayF	Art. 20b pkt 2	Doprecyzowania wymaga na czym ma polegać zapewnienie dostępu udostępnianie informacji o incydentach właściwemu CSIRT. Zapewnienie dostępu słownikowo oznacza, że podmiot, któremu umożliwia się dostęp ma możliwość skorzystania z tych danych. Czy warunek ten będzie spełniony, jeśli przedsiębiorca umożliwi skorzystanie z tych danych jedynie w swojej siedzibie i z informacji zgromadzonych np. w formie papierowej? Ponadto zauważyć należy, że informacje dotyczące incydentów cyberbezpieczeństwa powinna być chroniona a tym samym kanał komunikacyjny służący do ich przesyłania powinien być zabezpieczony. Przedsiębiorca komunikacji elektronicznej nie ma obowiązku spełniania wymogu posiadania narzędzi bezpiecznej komunikacji.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Aby właściwy CSIRT mógł wesprzeć przedsiębiorcę komunikacji elektronicznej w obsłudze incydentu, musi mieć dostęp do danych o incydencie.
276.	Związek Banków Polskich	Art. 20b pkt 2	Art. 20b pkt 2: zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub **właściwym CSIRT sektorowym** w zakresie niezbędnym do realizacji jego zadań, a także **właściwemu ISAC, jeżeli dotyczą one incydentów, które mogą mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

			Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego i ISACów w proces wymiany informacji.	przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. CSIRT sektorowe nie obsługują przedsiębiorców komunikacji elektronicznej.
277.	KIGEIT	Art. 20c ust. 1,2,3,4	**Propozycja zmiany:** *Art. 20c. 1. Przedsiębiorca komunikacji elektronicznej, ~~sporządzający plan, o którym mowa w art. 47 ust. 1 ustawy – Prawo komunikacji elektronicznej~~:* *1) klasyfikuje incydent jako incydent telekomunikacyjny na podstawie progów uznania incydentu za telekomunikacyjny;* *2) zgłasza incydent telekomunikacyjny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT ~~MON, CSIRT NASK lub CSIRT GOV~~ Telco;* *3) współdziała podczas obsługi incydentu telekomunikacyjnego i incydentu krytycznego z właściwym CSIRT ~~MON, CSIRT NASK lub CSIRT GOV~~ Telco, przekazując niezbędne dane, w tym dane osobowe.* *4) zapewnia CSIRT Telco dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.* *2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej - przy użyciu innych dostępnych środków komunikacji.* *~~3. Przedsiębiorca komunikacji elektronicznej niezależnie od zadań określonych w ust. 1:~~* *~~1) przekazuje jednocześnie CSIRT Telco w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 2;~~*	**Uwaga nieuwzględniona** Jeżeli przedsiębiorcy komunikacji elektronicznej zawrą porozumienie w sprawie podłączenia się do systemu z art. 46 to uzyskają prosty sposób przekazywania informacji o incydentach. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			~~*2) współdziała z CSIRT Telco podczas obsługi incydentu telekomunikacyjnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;*~~ ~~*3) zapewnia CSIRT Telco dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań.*~~ ~~*4.*~~*3 Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, progi uznania incydentu za incydent telekomunikacyjn~~*ego*~~*y, ~~których przekroczenie powoduje powstanie obowiązku zgłoszenia incydentu,~~ uwzględniając:* **Uzasadnienie:** W celu zapewnienia efektywności podejmowanych działań stosowne wydaje się ustalenie jednego podmiotu, któremu przedsiębiorca komunikacji elektronicznej przekazywać będzie zgłoszenie i który będzie koordynować działania w ramach obsługi incydentu. CSIRT Telco winien pełnić taką wiodącą rolę w powyższym zakresie, a działać niejako równolegle w stosunku do pozostałych CSIRT, powodując konieczność dublowania działań podejmowanych przez przedsiębiorcę komunikacji elektronicznej. CSIRT Telco może być umiejscowiony w Urzędzie Komunikacji Elektronicznej. Upoważnienie przewidziane w ust. 4 odpowiada treścią art. 42 ust. 2 projektowanej ustawy Prawo komunikacji elektronicznej. Nie wydaje się więc zasadne tworzenie dodatkowego pojęcia incydentu telekomunikacyjnego. Niezależnie od powyższego, w projekcie przewidziano obowiązek klasyfikowania przez przedsiębiorcę incydentu na podstawie progów uznania za incydent telekomunikacyjny, wobec czego delegacja powinna przewidywać określenie tych progów. Z kolei określanie progów pozwalających na podział incydentów telekomunikacyjnych na podlegające oraz na niepodlegające obowiązkowi zgłoszenia jest zbędne, bowiem w ust. 1 pkt 2)	

			przewidziano obowiązek zgłaszania wszystkich incydentów telekomunikacyjnych. Zgodnie z projektowanym art. 1 ust. 1 pkt 4, ustawa ma określać zadania i obowiązki wszystkich przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie Prawo komunikacji elektronicznej, w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów, natomiast zgodnie z projektowanym art. 4 pkt 2a, Krajowy system cyberbezpieczeństwa ma obejmować wszystkich przedsiębiorców komunikacji elektronicznej. W związku z tym w wypadku objęcia przedsiębiorców komunikacji elektronicznej zakresem ustawy, obowiązki określone w przepisie powinny zostać nałożone na wszystkich przedsiębiorców komunikacji elektronicznej, bez ograniczenia do przedsiębiorców sporządzających plan, o którym mowa w art. 47 ust. 1 ustawy – Prawo komunikacji elektronicznej.	

278.	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	Art. 20c KSC Art. 42 PKE Art. 20c KSC Art. 42 PKE	Ustawa o krajowym systemie cyberbezpieczeństwa, równolegle do PKE reguluje obowiązek zgłaszania incydentów bezpieczeństwa, przy czym różny jest krąg podmiotów zobowiązanych i organ właściwy do przyjmowania zgłoszeń: PKE nakłada obowiązek na wszystkich przedsiębiorców telekomunikacyjnych i nakazuje zgłaszać incydenty do UKE (art. 42) , zaś ustawa o krajowym systemie bezpieczeństwa nakłada obowiązki jedynie na tych przedsiębiorców, którzy mają obowiązek sporządzania planów działania w sytuacjach szczególnych zagrożeń i nakazuje zgłaszać incydenty do właściwego CSIRT (art. 20c). Ponadto, wobec wyżej wskazanych rozbieżności pomiędzy projektowanymi art. 42 PKE i art. 20c ustawy o krajowym systemie cyberbezpieczeństwa **Mediakom postuluje, by pozostać przy rozwiązaniu przyjętym w art. 20c – tak, by obowiązek zgłaszania incydentów obciążał wyłącznie tych przedsiębiorców telekomunikacyjnych, którzy są zobowiązani do sporządzania planów działania w sytuacjach szczególnych zagrożeń.** Są to podmioty duże, osiągające ponad 10 mln przychodów, często posiadające rozbudowane sieci i dużą liczbę abonentów. To właśnie incydenty bezpieczeństwa dotykające tych podmiotów, z uwagi na skalę ich działalności, winny być raportowane. Natomiast mniejsi przedsiębiorcy, działający na mniejszą skalę, o znacznie mniejszym zasięgu sieci i liczbie abonentów nie powinni być objęci obowiązkiem raportowania incydentów bezpieczeństwa.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Przedsiębiorcy komunikacji elektronicznej będą zgłaszać te incydenty telekomunikacyjne, które będą spełniać progi określone w rozporządzeniu.

279.	ISSA Polska	Art. 20c ust. 2	Art 20c ust 2. wymaga uszczegółowienia w kontekście realiów rynkowych. Czy niniejszy zapis należy rozważyć w taki sposób, że jeżeli przykładowo przedsiębiorca telekomunikacyjny zauważy „niestandardowy" ruch do podmiotu nadzorowanego przez CSIRT MON to ma obowiązek w przeciągu 24h o tym poinformować mil.cert? Przedsiębiorcy telekomunikacyjni często udostępniają klientom usługi SOC w formie komercyjnej usługi, taki przedsiębiorca nie powinien mieć nakładanych żadnych obowiązków w zakresie monitorowania bezpieczeństwa podmiotom, które nie wykupiły specjalistycznej usługi SOC. Podobnie sam fakt „niestandardowego" ruchu mógłby wyłącznie zostać zarejestrowany w systemach telekomunikacyjnych a niekoniecznie zostałby zidentyfikowany. Zapisy punktu należy doprecyzować biorąc pod uwagę, że jakiekolwiek usługi na rzecz podmiotów nie będących klientami SOC mogą być realizowane jedynie fakultatywnie.	Uwaga nieuwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Przedsiębiorca komunikacji elektronicznej ma zgłosić incydent telekomunikacyjny do tego CSIRT, który zgodnie z art. 26 będzie właściwy dla danego przedsiębiorcy.
280.	Digital Poland	Art. 20c	Warto w tym miejsce jeszcze zwrócić uwagę na pewną terminologiczną niedbałość w stworzeniu projektu KSC. Art. 20c ustawy o KSC przywołuje pojęcie „przedsiębiorcy komunikacji elektronicznej" z art. 47 ust. 1 projektu PKE, podczas gdy przepis ten odnosi się do przedsiębiorcy telekomunikacyjnego, a zatem nie do całej kategorii przedsiębiorców komunikacji elektronicznej. Podsumowując to zagadnienie, ujęcie w rozdziale 4a usług komunikacji interpersonalnej niewykorzystującej numerów wymaga korekty, bowiem jest całkowicie nieuzasadnione. Ponadto, projekt zmiany ustawy o KSC zawiera w rozdziale 4a nieścisłości terminologiczne, które mają olbrzymie znaczenie i także wymagają korelacji w innymi aktami prawnymi.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Wszyscy przedsiębiorcy komunikacji elektronicznej będą zgłaszać incydenty telekomunikacyjne przekraczające progi ustalone w rozporządzeniu.
281.	SayF	Art. 20c ust 1	Skoro nadrzędnym celem przepisów dotyczących bezpieczeństwa, a cyberbezpieczeństwa w szczególności, jest	**Wyjaśnienie**

			stworzenie systemu stwarzające warunki do szczelnego systemu bezpieczeństwa, to przepisy określają w bardzo różny sposób obowiązek realizacji tych obowiązków. W inny sposób określono obowiązki operatora usługi kluczowej, dostawców usług cyfrowych i w inny sposób przedsiębiorcy komunikacji elektronicznej. Dodatkowo podzielono przedsiębiorców komunikacji elektronicznej na dwie grupy tych, którzy sporządzają plany działań oraz tych, którzy nie mają takiego obowiązku. Kryterium obowiązku posiadania planu działań przez przedsiębiorcę telekomunikacyjnego nie będzie w każdym przypadku właściwą granicą podziału przedsiębiorców na grupy o różnych obowiązkach zapewnienia cyberbezpieczeństwa. Zdarza się, że przedsiębiorca telekomunikacyjny świadczący usługi np. w technologii VoIP dla kilkudziesięciu tysięcy abonentów, nieposiadający własnej infrastruktury telekomunikacyjnej, jest zwolniony z obowiązku posiadania planu działań. Oznacza to, że również jego działania w zakresie bezpieczeństwa usług będą ograniczone jak dla przedsiębiorców nie mających obowiązku wykonania planu działań, czyli będzie wykonywał te zadania w ograniczonym zakresie. Ponadto należy podkreślić, że projektowanie przepisów regulujących w odmienny sposób te same zagadnienie (obowiązki) wykonywane przez różne podmioty powoduje lub może powodować różne interpretacje i też różne wykonanie tych obowiązków. .	Przepisy zostały zmienione Przedsiębiorca komunikacji elektronicznej ma zapewnić obsługę każdego incydentu telekomunikacyjnego. Zgłaszać będzie takie incydenty telekomunikacyjne, które będą spełniały progi określone w rozporządzeniu. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
282.	SayF	Art. 20c ust 1 pkt 1	Dlaczego tylko wybrany przedsiębiorca kwalifikuje incydent jako incydent telekomunikacyjny. Czy incydent jest lub nie jest incydentem telekomunikacyjnym decyduje charakter incydentu i jego skutki a nie rodzaj podmiotu, u którego taki incydent zaistnieje?	**Wyjaśnienie** Przepisy zostały zmienione Przedsiębiorca komunikacji elektronicznej ma zapewnić obsługę każdego incydentu telekomunikacyjnego. Zgłaszać będzie takie incydenty

				telekomunikacyjne, które będą spełniały progi określone w rozporządzeniu. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
283.	Związek Banków Polskich	Art. 20c ust. 1 pkt 2	Art.20c ust. 1 pkt 2: zgłasza incydent telekomunikacyjny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV i **właściwych CSIRT sektorowych,** a także **właściwego ISAC, jeżeli incydent telekomunikacyjny może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**; Zapewnienie skutecznej wymiany informacji w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji	**Uwaga nieuwzględniona** CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej. ISAC nie jest jednostką operacyjną. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
284.	SayF	Art. 20c ust 3	Czy ten przepis dotyczy tylko przedsiębiorców telekomunikacyjnych zobowiązanych do posiadania planu działań czy dotyczy wszystkich przedsiębiorców komunikacji elektronicznej?	**Wyjaśnienie** Według nowego brzmienia przepisów będzie dotyczył wszystkich przedsiębiorców komunikacji elektronicznej. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

				przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
285.	Związek Banków Polskich	Art. 20c ust. 1 pkt 3	3) współdziała podczas obsługi incydentu telekomunikacyjnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV i **właściwym CSIRT sektorowym, a także właściwym ISAC jeżeli incydent telekomunikacyjny może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów**, przekazując niezbędne dane, w tym dane osobowe. Zapewnienie skutecznej wymiany informacji w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji.	**Uwaga nieuwzględniona** CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej. ISAC nie jest jednostką operacyjną. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
286.	Związek Banków Polskich	Art. 20d ust. 3	**Art.20d ust. 3:Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20c ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco i inny właściwy CSIRT sektorowy, a także właściwy ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów.** Zapewnienie wymiany informacji między sektorami w celu skutecznej obsługi incydentu.	**Uwaga nieuwzględniona** CSIRT sektorowe nie będą obsługiwać incydentów telekomunikacyjnych. W ich właściwości nie jest obsługa przedsiębiorców komunikacji elektronicznej. ISAC nie jest jednostką operacyjną. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

				przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
287.	SayF	Art. 20e ust. 1	Czy warto ten obowiązek do przedsiębiorcy komunikacji elektronicznej wykonującego działalność na rynku detalicznym? Ponadto art. 20e ust. 1 zobowiązuje przedsiębiorcę komunikacji elektronicznej do informowania swoich użytkowników o szczególnym i znacznym zagrożeniu wystąpienia incydentu telekomunikacyjnego. Wątpliwości nasze dotyczą: 1)W jaki sposób przedsiębiorca może wiedzieć o zagrożeniu wystąpienia incydentu telekomunikacyjnego. Takie zdarzenie wydarzy się w przyszłości. Przedsiębiorca może stwierdzić (i to nie zawsze) wystąpienie incydentu. Natomiast zagrożenie wystąpienia incydentu istnieje zawsze, w każdej chwili istnieje zagrożenie wystąpienia incydentu. 2)W jaki sposób przedsiębiorca będzie mógł stwierdzić istnienie szczególnego i znacznego zagrożenia.	**Uwaga nieuwzględniona.** Obecnie już funkcjonuje analogiczny przepis w art. 175e Prawa telekomunikacyjnego.
288.	SayF	Art. 20f	Spójnik „i” we frazie „sieci i usług” proponuje się zastąpić spójnikiem „lub”. Może się zdarzyć, że przesyłany komunikat może zagrozić tylko bezpieczeństwu sieci albo tylko bezpieczeństwu usług.	**Uwaga nieuwzględniona** Spójnik „i” pełni tutaj funkcję wyliczenia. Poza tym należy czytać to zgodnie z definicją bezpieczeństwa sieci i usług komunikacji elektronicznej
289.	Związek Banków Polskich	Art. 20f	Art. 20f W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia ... – Prawo komunikacji elektronicznej, może zastosować środki polegające na: 1) zablokowaniu przesłania takiego komunikatu,	**Uwaga nieuwzględniona** Obecne Prawo telekomunikacyjne zawiera analogiczny przepis i nie ma potrzeby jego rozszerzania.

			2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu **3) w sytuacji przesłania już komunikatu przed podjęciem działań zapobiegawczych poinformowaniu odbiorcy o zagrożeniu i jego skutkach wynikających z przesłanego komunikatu, a także sposobie jego neutralizacji** - w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia. Pierwotny zapis zakłada, że zagrożenie będzie niwelowane przed jego dystrybucją. Brak jest wskazówek co powinno nastąpić, gdy zagrożenie zostało zidentyfikowane w trakcie trwania incydentu.	
290.	ISACA Warsaw Chapter	Art. 20f	„Art. 20f. W przypadku stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu sieci i usług, przedsiębiorca komunikacji elektronicznej, z uwzględnieniem art. 349 ust. 2 ustawy z dnia … – Prawo komunikacji elektronicznej, może zastosować środki polegające na: 1) zablokowaniu przesłania takiego komunikatu, 2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej na zakończeniu sieci, z którego następuje wysyłanie takiego komunikatu - w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia” Propozycja rozszerzenia zapisu o to, kto będzie miał upoważnienie do stosowania wymienionych działań.	**Uwaga nieuwzględniona** Obecne Prawo telekomunikacyjne zawiera analogiczny przepis i nie ma potrzeby jego rozszerzania.
291.	SayF	Art. 20f pkt 1 i 2	Proponuje się wykreślić art. 20f pkt 1, ponieważ w celu określenia jaki komunikat powoduje zagrożenie bezpieczeństwu sieci lub usług przedsiębiorca będzie musiał wykonać kontrolę i analizę tego komunikatu. Ponadto w celu zrealizowania tego przepisu	**Uwaga niewuzględniona** Analogiczny przepis jest w art. 175c Prawa telekomunikacyjnego.

			będzie musiał zablokować przesłania tylko tego komunikatu, który zagraża bezpieczeństwu. W naszej ocenie prawnie jest to niedopuszczalne a technicznie bardzo trudne do wykonania. Pkt 2 w art. 20f w pełni obejmuje również zakres określony w pkt1	
292.	SayF	Art. 20f myślnik po punkcie 2	Wzorem przepisów ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne proponuje się uzupełnić ten zapis o przepisy zwalniające przedsiębiorcę z odpowiedzialności za skutki działań, o których mowa w art. 20f. (chyba, że przepisy te znajdą się w PKE)	**Uwaga nieuwzględniona** W chwili obecnej nie są planowane zmiany w projekcie, o których mowa w uwadze.
293.	Liquid Systems	Art. 20a-f	Projekt nie powinien mieć zastosowania bezpośrednio do operatorów telekomunikacyjnych. Ustawa KSC jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatorów telekomunikacyjnych, ponieważ prawa i obowiązki operatorów telekomunikacyjnych zostały szczegółowo określone w ustawie Prawo Komunikacji Elektronicznej, implementującej do prawa polskiego Europejski Kodeks łączności Elektronicznej (EECC). Dodanie przedsiębiorstwa komunikacji elektronicznej jako podmiotu, do którego stosuje się KSC, powoduje nakładanie się przepisów i potencjalny konflikt między nimi. Operator telekomunikacyjny jest zazwyczaj bardzo ważnym dostawcą usług operatora infrastruktury krytycznej.. Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

			powoduje wątpliwości w zakresie interpretacji przepisów. **Sugestie:** 1.Postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC . 2.KSC nie powinno mie6 zastosowania do przedsiębiorstw Komunikacji elektronicznej.	administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich definicji z PKE do ustawy KSC.
294.	Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o.	Art. 22 ust. 1 pkt 2a	**Pominięte słowo** będący jednostką samorządu terytorialnego, niezależnie od obowiązku, o którym mowa w punkcie 2, zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego wojewody	**Uwaga uwzględniona**
295.	Transition Software	Art.24 pkt.3 ppkt c) i d)	Podmioty świadczące usługę kluczową oraz inne podmioty wchodzące w skład systemu cyberbezpieczeństwa powinny obligatoryjnie przeprowadzać - minimum wśród personelu pełniącego obowiązki w procesie świadczenia usługi kluczowej – cykliczne (minimum raz w roku kalendarzowym) szkolenia z zakresu świadomości zagrożeń cyberbezpieczeństwa (tzw. *Security Awareness*).	**Uwaga nieuwzględniona** Operator usługi kluczowej odpowiada za swój personel.

			Zalecane jest natomiast cykliczne szkolenie całego personelu przedsiębiorstwa/podmiotu, z powodu minimalizacji ryzyka poprzez minimalizację powierzchni potencjalnego ataku (zasada *„najsłabszego ogniwa łańcucha*).	
296.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 24a	Należy rozważyć powołanie CSIRT-u sektorowego dla "sektora administracji samorządowej" z organem właściwym przy ministrze właściwym do spraw administracji. Zakres obowiązków i zadań w stosunku do jednostek samorządu terytorialnego uzasadnia taką propozycję.	**Uwaga nieuwzględniona** Podmioty publiczne w tym jednostki samorządu terytorialnego są specyficzną kategorią podmiotów ksc i nie mogą być traktowane jak operatorzy usługi kluczowej. Wsparciem w obsłudze incydentu dla JST zajmuje się CSIRT NASK.
297.	Związek Banków Polskich	Art. 24a	24a. Wojewoda: 1) zapewnia wymianę informacji na temat zagrożeń cyberbezpieczeństwa, podatności oraz incydentów dotyczących podmiotów publicznych w województwie; 2)prowadzi listę danych kontaktowych osób z poszczególnych podmiotów publicznych w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV oraz właściwym CSIRT sektorowym i właściwym ISAC; 3)we współpracy z Pełnomocnikiem oraz właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV oraz właściwym CSIRT sektorowym i właściwym ISAC przekazuje marszałkowi województwa, starostom, wójtom, burmistrzom, prezydentom miast w informacje dotyczące: (…) Włączenie CSIRT sektorowych oraz ISAC w kanał informacyjny.	**Uwaga nieuwzględniona** CSIRT sektorowe nie będą obsługiwać incydentów w podmiocie publicznym. W ich właściwości nie jest obsługa podmiotów publicznych. ISAC nie jest jednostką operacyjną.
298.	Transition Software	Art.26, ust. 3, pkt 14	Rozważyć wprowadzenie zapisów umożliwiających zastosowania outsourcingu/body leasingu w przypadku braku zasobów kadrowych. Przy uwzględnieniu outsourcingu/body leasingu również należy sprawdzić - przez dedykowane służby – bezpieczeństwo osobowe personelu, który będzie miał	**Uwaga nieuwzględniona,** nie dotyczy nowelizacji

			wykonywać powierzone prace. W przypadku istnienia potencjalnej możliwości odbioru informacji niejawnych jako danych niezbędnych do świadczenia obowiązków, przed rozpoczęciem świadczenia obowiązków musi on posiadać aktualne poświadczenie bezpieczeństwa, o stopniu przynajmniej równym do klauzuli potencjalnych otrzymywanych informacji niejawnych.	
299.	Transition Software	Art. 26, ust. 3, pkt 15	Wprowadzić zapis, który jednoznacznie wskazuje, że „obsługa" musi obejmować również to, że ta potencjalna platforma i kanały przekazu zgłoszeń muszą być zawsze bezpieczne, z bieżącymi aktualizacjami i regularnie przeglądane pod kątem istnienia ew. luk/podatności.	**Uwaga nieuwzględniona,** nie dotyczy nowelizacji
300.	ISSA Polska	Art. 26 ust. 3 pkt 21	Prosimy o informacje, w jaki sposób regulator rozgranicza otwarte sieci teleinformatyczne od tych, w zakresie których sieci mają niezamierzone błędy konfiguracji lub są wynikiem ujawnionej podatności itp. w kontekście ustawowej zgody na skanowanie sieci wyrażoną w punkcie 21 ustępu 3 artykułu 26. Nie został przedstawione konsekwencje w zakresie regresji i odszkodowań na skutek skanowania lub dostępu do informacji na systemach informacyjnych osoby fizycznej, podmiotów gospodarczych czy międzynarodowych podmiotów będących uczestnikami sieci teleinformatycznych. Prosimy dodatkowo prosimy o określenie czasu retencji informacji pozyskanych w ramach skanowania - prawo do bycia zapomnianym / zatarcie.	**Wyjaśnienie** Zespoły Csirt poziomu krajowego takie działania będą mogły prowadzić jedynie w porozumieniu z podmiotem.
301.	Transition Software	Art. 32 ust.4, Art.35, ust.4	3 główne CSIRTy nie „mogą", tylko POWINNY się informować wzajemnie o zagrożeniach bezpieczeństwa oraz POWINNY wspomagać merytorycznie inne wzmiankowane podmioty. POWINNY oznacza nakaz wykonania danej czynności, tj. w tym przypadku ww. wsparcia/współpracy, chyba, że istnieją	**Uwaga nieuzwględniona** Taki przepis doprowadziłby do chaosu informacyjnego – CSIRT poziomu krajowego musiałyby informować o każdym cyberzagrożeniu.

			okoliczności, obiektywnie i wysoce uzasadniające odstąpienie od tych czynności informacyjnych/współpracy (decyduje Kierownik Jednostki Organizacyjnej danego CSIRT, decyzja ta podlega ew. późniejszej analizie/audytowi).	
302.	Związek Banków Polskich	Art. 34 ust. 1	1)CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco oraz SOC i **ISAC współpracują między sobą** oraz z organami ścigania i wymiaru sprawiedliwości i służbami specjalnymi przy realizacji ich ustawowych zadań."; Włączenie do wymiany również ISAC. Zapewnienie wymiany informacji między sektorami w celu skutecznej obsługi działań zmierzających do wyjaśnienia incydentu.	**Uwaga nieuzględniona** ISAC nie pełnią funkcji operacyjnej.
303.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 34a pkt 3	ten artykuł wprowadza rozmytą odpowiedzialność. Należy odpowiedzialność ustanowić jasno, tzn. sprawozdanie, o którym mowa w tym artykule powinien przygotowywać CSIRT Telco we współpracy z CSIRTami poziomu krajowego	**Wyjaśnienie** Wynika to z obecnej praktyki, czyli że sprawozdanie przygotowuje i przekazuje Prezes UKE.
304.	Transition Software	Rozdział 7, Art.37, ust. 1	Bardzo dobry artykuł. Zapisy należy dodatkowo rozszerzyć, tj. uwzględnić i dodatkowo zapisać wyjęcie również spod zapisów Ustawy o dostępie do informacji publicznej, wykorzystywaną przez dany podmiot infrastrukturę ICT, tj. sprzęt (modele, firmware, numery seryjne, licencje, wersje oprogramowania), stosowane systemy i oprogramowanie infrastrukturalne/usługowe oraz – w szczególności - oczywiście stosowane systemy i oprogramowanie bezpieczeństwa, zarówno te biorące bezpośrednio udział w świadczeniu usługi kluczowej, jak i wchodzące w skład infrastruktury ICT ogólnej, funkcjonującej w ramach organizacji podmiotu, a wspomagającej świadczenie usługi lub tworzącej jej szkielet (minimalizacja ryzyka poprzez minimalizację udzielanych informacji dot. infrastruktury ICT).	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.

305.	SayF	Art. 39 ust. 5 i 6	Proponujemy zastąpienie słowa „lub” na „albo”. Warto też się zastanowić, czy jest sens zanonimizowania danych, skoro są już niepotrzebne?	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.
306.	SayF	Art. 39 ust. 9	Warto przeanalizować Czy zapisy w tym ustępie nie są powielone przez ustawę o ochronie danych osobowych oraz RODO? jeżeli tak to proponujemy wykreślić	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.
307.	SayF	Art. 41	Brak organu odpowiedzialnego za przedsiębiorców komunikacji elektronicznej	**Wyjaśnienie** Organem regulacyjnym wobec przedsiębiorców komunikacji elektronicznej będzie Prezes Urzędu Komunikacji Elektronicznej
308.	SayF	Art. 41 pkt 8 i 9	Brak definicji infrastruktury cyfrowej.	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji, w załączniku nr 1 znajduje się pojęcie infrastruktury cyfrowej
309.	ISSA Polska	Art. 44 ust. 6 pkt 4	Proponujemy dodać do zapisu nowo proponowanego ustępu 6 artykułu 44 punktu 4) obecności na wykazie podmiotów realizujących zadania SOC.	**Uwaga nieuwzględniona** CSIRT sektorowe będą mogły przyjmować zgłoszenia nawet zwykłych incydentów.
310.	Związek Banków Polskich	Art. 44 ust. 1	1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do ustawy, do którego zadań należy: 1) przyjmowanie zgłoszeń **o incydentach poważnych**; W aktualnym brzmieniu ustawy mowa jest jedynie o przyjmowaniu przez SZC zgłoszeń o incydentach poważnych. Jeżeli celem projektowanego przepisu jest zwiększenie ilości incydentów, które będą notyfikowane należy przede wszystkim rozważyć zmianę kryteriów kwalifikowania incydentów jako incydenty poważne lub krytyczne. W innym przypadku dojdzie do powstania szumu informacyjnego, w szczególności poprzez przekazywanie informacji o bardzo drobnych incydentach.	

311.	Fundacja Bezpieczna Cyberprzestrzeń	Art. 44 ust. 1	Należy uzupełnić przepis o obowiązek ustanowienia CSIRT-ów sektorowych np. poprzez dodanie zdanie pierwszego: „Organy właściwe do spraw cyberbezpieczeństwa tworzą CSIRT sektorowe.”. W art. 3 ust. 1 ustawy zamieniającej jest bowiem przepis wskazujący termin na ustanowienie takiego zespołu. Przede wszystkim jednak należy poddać analizie zasadność obowiązkowego powoływania takich zespołów. W uzasadnieniu czytamy bowiem: „Mimo ustawowej możliwości, sektorowe zespoły cyberbezpieczeństwa nie były dotychczas powoływane. Dla podniesienia skuteczności reagowania na incydenty zachodzi konieczność ustanowienia CSIRT sektorowych dla każdego z sektorów. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami”. Czy została przeprowadzona analiza jaki był powód niepowoływania zespołów sektorowych oraz analiza rzeczywistego podniesienia skuteczności reagowania na incydenty w przypadku funkcjonowania zespołu sektorowego? Na jakiej podstawie wysunięto wniosek, że dzięki funkcjonowaniu CSIRT sektorowego operatorzy usług kluczowych będą w stanie szybciej i efektywniej radzić sobie z incydentami? W przypadku istnienia takiej analizy naszą uwagę prosimy uznać za nieważną i jednocześnie prosimy o wskazanie wyników tych analiz lub ich źródła.	**Wyjaśnienie** CSIRT sektorowe efektywnie wspomogą podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów.
312.	PKN Orlen	Art. 44 ust. 1	Propozycja zmiany art. 44 ust. 1 Ustawy o KSC jak poniżej: *„ Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionym w załączniku nr 1 do ustawy, **a także może ustanowić CSIRT grupy kapitałowej do** których zadań należy:* *1) przyjmowanie zgłoszeń o incydentach;*	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.

			2) reagowanie na incydenty; *3) gromadzenie informacji o podatnościach i zagrożeniach, które mogą mieć negatywny wpływ na cyberbezpieczeństwo;* *4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i zagrożeniach, organizację i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;* *5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach. ",* 2. Ponadto w projektowanym: ■ art. 44 ust. la) Projektu należy zastąpić pojęcie: *„CSIRT sektorowy"* użytymi w odpowiedniej liczbie i odpowiednim przypadku pojęciami: *„CSIRT sektorowy oraz CSIRT grupy kapitałowej"',* art. 44 ust. 5 Projektu należy dodać: *„(...) a w przypadku CSIRT grupy kapitałowej podmiotowi wchodzącemu w jej skład, który spełnia warunki o których mowa w art. 44 ust. 6, a także po zasięgnięciu opinii Pełnomocnika. "* W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa *„CSIRT grupy kapitałowej"* **niezbędne jest wskazanie sposobu ustanowienia takiego podmiotu.**	
313.	Związek Banków Polskich	Art. 44 ust. 1 pkt 5	*5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV* ***oraz innymi właściwymi CSIRT sektorowymi, a także właściwym ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo***	**Uwaga częściowo uwzględniona,** zostanie dodana możliwość współpracy między CSIRT sektorowymi

			podmiotów danego sektora, sektorów lub podsektorów lub ich klientów, *w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o* ***podatnościach i*** *zagrożeniach.",* Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji z innymi CSIRT. Nadrzędnym celem dla instytucji jest pozyskiwanie wszelkich informacji i wsparcia pochodzącego od innych uczestników krajowego systemu cyberbezpieczeństwa, w tym innych CSIRT sektorowych i ISAC.	
314.	Związek Banków Polskich	Art. 44 po ustępie 1 dodaje się ustęp 1a	„1a. CSIRT sektorowy może, w szczególności: 1)zapewniać dynamiczną analizę ryzyka i incydentów oraz wspomagać w podnoszeniu świadomości zagrożeń cyberbezpieczeństwa; 2)koordynować w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które dotyczą różnych podmiotów w danym sektorze lub podsektorze.", ***3)nawiązywać współpracę z innymi CSIRT sektorowymi oraz ISAC w celu wymiany informacji o zagrożeniach i incydentach.*** Wymiana informacji powinna mieć charakter poziomy i pionowy.	**Uwaga nieuwzględniona.** Współpraca CSIRT sektorowych została ujęta w poprzednim stanowisku. ISAC nie jest jednostką operacyjną.
315.	Związek Banków Polskich	Art. 44a pkt 5	4. Do zadań CSIRT Telco należy: ….. 5)współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV **oraz innymi właściwymi CSIRT sektorowymi, a także właściwym ISAC, jeżeli incydent może mieć wpływ na bezpieczeństwo podmiotów danego sektora, sektorów lub podsektorów lub ich klientów,** w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymianę informacji **o podatnościach** i zagrożeniach.".	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.

			Zapewnienie wymiany informacji między sektorami i w ramach sektora. Włączenie CSIRT sektorowego oraz ISAC w proces wymiany informacji z innymi CSIRT. Nadrzędnym celem dla instytucji jest pozyskiwanie wszelkich informacji i wsparcia pochodzącego od innych uczestników krajowego systemu cyberbezpieczeństwa, w tym innych CSIRT sektorowych i ISAC.	
316.	PKN Orlen	Art. 53 ust. 1	*Propozycja zmiany aktualnego art. 53 ust. 1 punkt 1 Ustawy o KSC, w myśl której w/w przepis miałby następujące brzmienie: „Nadzór w zakresie stosowania przepisów ustawy sprawują:* *1) minister właściwy do spraw informatyzacji w zakresie spełniania przez **podmioty prowadzące SOC,** wymogów, o których mowa w art. 14 ust. 2; (...). ”* Zmiana wynika z zawartej w Projekcie propozycji zastąpienia w art. 4 punkt 16 pojęcia *„podmioty świadczące usługi z zakresu cyberbezpieczeństwa”* pojęciem SOC.	**Uwaga uwzględniona**
317.	SayF	Art. 53 ust 1 pkt 2	Kto sprawuje nadzór w zakresie przedsiębiorców komunikacji elektronicznej? Wymaga uzupełnienia	**Wyjaśnienie** Nadzór nad przedsiębiorcami komunikacji elektronicznej sprawuje Prezes UKE. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
318.	ISACA Warsaw Chapter	Art. 62 ust. 1 pkt 6	Art. 62. 1. W ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa do zadań Pełnomocnika należy: wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.	**Wyjaśnienie** Przepis ten dotyczy rekomendacji z art. 33. Uwaga nie dotyczy nowelizacji ustawy.

			Art. 62 ust. 6 upoważnia pełnomocnika do „wydawania „rekomendacji dotyczących sprzętu lub oprogramowania na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV” Cóż ta rekomendacja lub raczej jej brak może oznaczać? Ustawa tego nie reguluje, a powinna. Co gdy podmiot nie zastosuje się do rekomendacji pełnomocnika? Problem jednak jest dużo poważniejszy. Mamy już bardzo dobrą regulację dotycząca certyfikacji w zakresie cyberbezpieczeństwa. Jest ona budowana w ramach ENISA, oparta miedzy innymi o: „DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union” “REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity)” Ostatni akt ma dwa podstawowe cele: “objectives, tasks and organisational matters relating to ENISA, a framework for the establishment of European cybersecurity certification schemes.” I właśnie schematy certyfikacji cybersecurity powinny być podstawą do klasyfikacji sprzętu, oprogramowania i usług jako bezpieczne. Dokument ten w artykule 54 mówi: “54 certification schemes will include at least:	

			* 54(1a) Scope (type and categories of ICT products, ICT services and ICT processes), * 54(1c) References to international standards". Zatem to nie CSIRTy i pełnomonik rządu mają rekomendować produkty, usługi czy procesy, a niezależne podmioty certyfikujące. Przypomnę obowiązki z tego wynikające dla RP: "58(1) Each member state shall designate one or more national cybersecurity certification authorities. 62(1) European Cybersecurity Certification Group shall be established, composed by national cybersecurity certification authorities representatives. 58(7a) enforce rules of cybersecurity certification schemes in cooperation with marked surveillance authorities"	
319.	SayF	Art. 65	Brak CSIRT Telco	**Uwaga uwzględniona**
320.	SayF	Art. 66	Czemu w skład kolegium nie wchodzi Prezes Urzędu Komunikacji Elektronicznej?	**Wyjaśnienie** Przewodniczący Kolegium może zaprosić na posiedzenie Kolegium przedstawicieli instytucji których udział uzna za niezbędny.
321.	Pracodawcy RP	Art. 66a	**a) Naruszenie polskich przepisów** 1) Naruszenie prawa konstytucyjnego **a)** Zasada proporcjonalności Proponowane kryteria procedury ocennej, której efektem może być zakaz prowadzenia działalności gospodarczej w Polsce zostały określone w sposób nieprecyzyjny. Przepisy Projektu przyznają Kolegium, które nie jest kompetencyjnie i ustrojowo umocowane, inwazyjną, niczym nieograniczoną, opartą na niejasnych kryteriach, pozbawioną kontroli sądowej kompetencję do prowadzenia jednostronnego postępowania ocennego. Konsekwencje tego postępowania mogą wywrzeć olbrzymi	**Uwaga nieuwzględniona** Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny.

			wpływ na sytuację ekonomiczną danego dostawy, ale również operatorów telekomunikacyjnych oraz konsumentów. Postępowanie przed Kolegium do spraw cyberbezpieczeństwa ma się w całości odbywać bez udziału ocenianego dostawcy, który dopiero z komunikatu w Monitorze Polskim dowie się, o przeprowadzonej ocenie. Dlatego też przyjęte rozwiązania legislacyjne są sprzeczne z zasadą proporcjonalności wyprowadzoną z zasady demokratycznego państwa prawnego (Art. 2 Konstytucji).	
322.	Pracodawcy RP	Art. 66a	Projektowane przepisy w rażący sposób podważają zaufanie obywateli do Państwa. Projekt zakłada rażąco niekonstytucyjny obowiązek usunięcia z rynku przejawów dotychczasowej działalności dostawcy. W związku z powyższym analizowany zakaz należy poddać kontroli w zakresie zgodności z zasadą lex retro non agit (niedziałania prawa wstecz). W związku z tym, że demokratyczne państwo prawne oznacza państwo w którym chroni się zaufanie obywatela do państwa i stanowionego przez nie prawa, ustawodawca dokonując kolejnych zmian stanu prawnego nie może stracić z pola widzenia interesów podmiotów, jakie ukształtowały się przed dokonaniem zmiany stanu prawnego .	**Uwaga nieuwzględniona** Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny.
323.	Pracodawcy RP	Art. 66a	**Naruszenie zasady równości wobec prawa** Projektowane rozwiązania w zakresie wyboru dostawcy sprzętu i oprogramowania sieci 5G pozwalają na arbitralne wykluczenie dostawców z udziału we wdrożeniu sieci 5G w oparciu o dowolne, nieokreślone kryteria. Nie przyznają przy tym dostawcom środków prawnych pozwalających na wniesienie odwołania od decyzji wykluczających. Wobec tego uznać je należy za sprzeczne z konstytucyjnymi zasadami równości wobec prawa (art. 32 Konstytucji).	**Uwaga nieuwzględniona** Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny.

324.	Pracodawcy RP	Art. 66a	a) Istotne braki przy ocenie skutków regulacji Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu.	**Uwaga częściowo uwzględniona** **OSR zostanie uzupełniony.**
325.	Pracodawcy RP	Art. 66a	b) Naruszenie przepisów procedury administracyjnej W projektowanych przepisach nie przewidziano prawa strony do udziału w postępowaniu ocennym, prowadzonym przez Kolegium. Proponowane rozwiązania naruszają więc podstawowe zasady postępowania administracyjnego wyrażone w ogólnych przepisach Kodeksu postępowania administracyjnego., m.in. zasadę pogłębiania zaufania obywateli do władzy publicznej (art. 8 kpa), zasadę udzielenia informacji przez organ (art. 9), zasadę wysłuchania stron (art. 10). Wprowadzone przepisy naruszają więc podstawowe prawo jednostki do czynnego udziału w postępowaniu.	**Uwaga uwzględniona** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.

326.	Pracodawcy RP	Art. 66a	**Naruszenie prawa konkurencji w Polsce** Uregulowanie kwestii wykluczenia dostawców w ustawie KSC narusza również podstawowe zasady prawa konkurencji. Zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy reguluje inna ustawa tj. ustawa z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, Dz. U. nr 50, poz. 331 ze zm. Zgodnie z art. 1 ust. 2 tej ustawy, reguluje ona w szczególności zasady i tryb postępowania w stosunku do pomiotów działających na konkurencyjnym rynku, jeżeli podmioty te naruszają przepisy tej ustawy. Oznacza to faktyczne naruszenie przez Kolegium kompetencji właściwego organu administracyjnego, jakim jest Prezes Urzędu Ochrony Konkurencji i Konsumentów.	**Uwaga nieuwzględniona** Projekt jest zgodny z Konstytucją, która umożliwia ograniczenie prawa swobody działalności gospodarczej ze względu na ważny interes publiczny.
327.	Pracodawcy RP	Art. 66a	Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego.	**Uwaga uwzględniona** Projekt zostanie notyfikowany.
328.	Pracodawcy RP	Art. 66a	**Naruszenie praw człowieka regulowane przez EKPC** ECHR(Europejska konwencja praw człowieka) stwierdza, że: „Każda osoba fizyczna i prawna ma prawo do poszanowania swego mienia. Nikt nie może być pozbawiony swojej własności, chyba że w interesie publicznym i na warunkach przewidzianych	**Uwaga nieuwzględniona** **Projekt jest zgodny z EKPCz.**

			przez ustawę oraz zgodnie z ogólnymi zasadami prawa międzynarodowego".	
329.	Pracodawcy RP	Art. 66a	**a) Naruszenie zasad TFUE** Każda ocena ryzyka lub decyzja o wprowadzeniu ograniczeń rynkowych i pozataryfowych barier w handlu na podstawie niejednoznacznych kryteriów (np. kraj pochodzenia dostawców zawarty w projekcie) i nietransparentne procedury administracyjne, naszym zdaniem, są sprzeczne z podstawowymi zasadami równego traktowania/niedyskryminacji, które znajdują odzwierciedlenie w art. 18 (zakaz dyskryminacji ze względu na narodowość), Art. 34 (zakaz ograniczeń ilościowych w przywozie oraz wszystkich środków o skutku równoważnym), Art. 49 (zakaz ograniczeń swobody przedsiębiorczości) TFUE.	**Uwaga nieuwzględniona** **Projekt jest proporcjonalny i zgodny z prawem europejskim.**
330.	Pracodawcy RP	Art. 66a	**d) Naruszenie zasady niedyskryminacji w prawie UE** Kluczową zasadą praworządności jest to, że prawo musi mieć zastosowanie do wszystkich i być stosowane jednakowo i w sposób konsekwentny. Jest to powtórzone w Karcie Praw Podstawowych Unii Europejskiej (art. 20), w której "każdy jest równy wobec prawa". Karta (art. 21 ust. 2) zabrania „wszelkiej dyskryminacji ze względu na narodowość". Europejski Trybunał Sprawiedliwości zauważył, że „zakaz dyskryminacji ustanowiony w prawie UE. jest szczególnym wyrazem ogólnej zasady równości, która jest jedną z podstawowych zasad prawa wspólnotowego". Jest zatem zgodne z zasadą praworządności, że wymogi bezpieczeństwa powinny być powszechnie stosowane do wszystkich dostawców, a nie dotyczyć wybranych dostawców lub dostawców z określonych krajów.	**Uwaga nieuwzględniona** **Projekt jest proporcjonalny i zgodny z prawem europejskim.**
331.	Pracodawcy RP	Art. 66a	**Naruszenie zasady proporcjonalności określonej przez ETS**	**Uwaga nieuwzględniona**

			Pkt 13 w sprawie C-331/88 Fedesa odnosi się do zasady proporcjonalności: Po wprowadzeniu środka dyskryminującego Trybunał przyjrzy się proporcjonalności środka w odniesieniu do jego celu. Innymi słowy, środek taki musi być (1) konieczny do osiągnięcia celu i nie może wykraczać poza to, co jest konieczne do osiągnięcia celu, (2) najmniej restrykcyjny środek do osiągnięcia tego celu, oraz (3) spowodowane niedogodności nie mogą być nieproporcjonalne do zamierzonych celów.	**Projekt jest proporcjonalny i zgodny z prawem europejskim.**
332.	Pracodawcy RP	Art. 66a	**Naruszenie zasady swobodnego przepływu towarów** Zasada ta może być nadal naruszona, nawet jeśli państwo członkowskie nie ustanawia wyraźnego przepisu zakazującego przywozu produktów od niektórych dostawców. Jak wyjaśnił Europejski Trybunał Sprawiedliwości, każdy zakaz używania produktu na terytorium państwa członkowskiego UE wpłynie na zachowanie nabywców i wpłynie na dostęp tego produktu na rynku tego państwa członkowskiego. Przepisy mające na celu odsunięcie określonego dostawcy od łańcucha dostaw w niektórych państwach członkowskich UE powstrzymają potencjalnych klientów przed kupowaniem produktów/technologii danego dostawcy.	**Uwaga nieuwzględniona** **Projekt jest proporcjonalny i zgodny z prawem europejskim.**
333.	Pracodawcy RP	Art. 66a	**Naruszenie postanowień umów międzynarodowych** Naszym zdaniem ustawodawca koncentruje się na ocenie cech dotyczących dostawców, a nie na bezpieczeństwie sprzętu czy oprogramowania, jakie zapewnia. Jedną z istotnych cech ocenianych w profilu dostawcy jest kryterium pochodzenia dostawcy z danego kraju. Rodzi to zagrożenie, że Polska naruszy umowy międzynarodowe zakazujące dyskryminacji ze względu na pochodzenie. Kryteria powinny opierać się o ustandaryzowane	**Uwaga nieuzwględniona** **Projekt jest zgodny z prawem międzynarodowym. Porozumienie o Wolnym Handlu GATT w art. XXI pozwala na stosowanie przez strony porozumienia wszelkich działań, jakie uważają one za niezbędne do ochrony swych żywotnych interesów bezpieczeństwa. Projektowane przepisy wpisują się wobec tego w środki opisane w art. XXI GATT.**

			metody weryfikacji i certyfikacji w oparciu o normy międzynarodowe, takie jak normy ISO, branżowe standardy NESAS i europejskie schematy certyfikacji przewidziane w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.	
334.	Pracodawcy RP	Art. 66a	Istotne braki przy ocenie skutków regulacji oraz negatywne skutki dla gospodarki Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o niekonstytucyjnym charakterze Projektu. W zakresie skutków Projektu na budżet Polski i gospodarkę krajową wskazać należy, iż Projekt będzie miał negatywny wpływ na gotowość podmiotów do składania ofert na pasma częstotliwości 5G. Fakt niemożności wybrania dostawcy sprzętu lub usług odroczy uruchomienie sieci 5G oraz rozwój Przemysłu	**Uwaga częściowo uwzględniona** OSR zostanie uzupełniony W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

			4.0. Według analizy wymiarów strat (aktywów, dodatkowych kosztów migracji, zwiększonej niestabilności OPEX oraz sieci), bezpośrednie straty operatorów przekroczą 2,5 mld euro. Nie bez znaczenia dla polskiej gospodarki pozostaje również fakt, iż wykluczone podmioty gospodarcze będą uprawnione do dochodzenia odszkodowania od Skarbu Państwa. Roszczenia odszkodowawcze operatorów i dostawców wobec Skarbu Państwa zostaną ostatecznie wypłacone przez podatników i konsumentów. Budżet państwa będzie zasilał operatorów i producentów zamiast ułatwiać życie obywatelom, szczególnie po pandemii. W zakresie skutków społecznych należy opisać wpływ Projektu na likwidację miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego wynikający z wyższego kosztu usług dla konsumentów i przedsiębiorstw: w szczególności w obszarach pracy zdalnej, zdalnej edukacji, telemedycyny, rozwoju inteligentnych usług samorządowych (smart cities) oraz nowoczesnych rozwiązań w rolnictwie, ochronie środowiska czy energetyce.	
335.	Pracodawcy RP	Art. 66a	1. Kryteria powinny być neutralne technologicznie, i dotyczyć wyłącznie zagadnień mających rzeczywisty wpływ na bezpieczeństwo podmiotów krajowego systemu cyberbezpieczeństwa: 1) Przedmiotem oceny ryzyka powinien być sprzęt i oprogramowanie uznane za krytyczne (takie jak sieć rdzeniowa 5G, kluczowe systemy kontroli przemysłowej), a nie charakterystyka dostawcy; 2) Kryteria powinny mieć charakter techniczny, być obiektywne, rozsądne i proporcjonalne, oraz opierać się na standardach weryfikacji odpowiednich dla poszczególnych	**Uwaga nieuwzględniona** Zgodnie z Toolbox 5G ocena powinna dotyczyć dostawcy i jego powiązań z państwem pochodzenia.

			rodzajów sprzętu i oprogramowania, w szczególności normach ISO, branżowych standardach NESAS i europejskich schematach certyfikacji przewidzianych w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r.	
336.	Polska Izba Handlu	Art. 66a	**Projekt:** brak środków odwoławczych w ramach postępowania administracyjnego Propozycja zmiany: W Art. 66a Projektu należy dodać nowy ust. 10: *„Postępowanie przed Kolegium prowadzone jest zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego”* **Uzasadnienie** Postanowienia k.p.a. regulują tryb postępowania i wydawanie decyzji przez organy i podmioty państwowe. Obecnie projektowane przepisy odrębnie regulują te kwestie za pomocą zaledwie kilku przepisów, które posiadają charakter proceduralny. Przepisy te nie mogą zastąpić odpowiednich regulacji k.p.a. Uwagi te dotyczą także projektowanego postanowienia w zakresie wymogów jakie elementy powinna zawierać ocena Kolegium (art. 66a ust. 5 Projektu).	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.

				Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o

				uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
337.	PIIT	Art. 66a	1. Art. 66a 1.1. Art. 66a ust. 1 – uprawnienie Kolegium do dokonania oceny W myśl projektowanych przepisów organem uprawnionym do dokonywania oceny byłoby Kolegium, które jest działającym przy Radzie Ministrów organem opiniodawczo-doradczym. W jego skład wchodzą przedstawiciele administracji publicznej, tj. Pełnomocnik Rządu ds. Cyberbezpieczeństwa, określeni Ministrowie, Szef BBN, minister koordynator służb specjalnych. Oznacza to, że de facto Kolegium jest w wysokim stopniu gremium polityczno-administracyjnym. W jego składzie brakuje natomiast organów lub jednostek posiadających dogłębną wiedzę techniczną oraz doświadczenie w certyfikacji i ocenie urządzeń i oprogramowania. Takich można szukać dopiero wśród jednostek i organów podległych lub nadzorowanych, których udział w ocenie nie został jednak zaakcentowany w projekcie ustawy. Postulaty: • W naszej ocenie niezbędne jest, aby skład Kolegium, przynajmniej na potrzeby dokonywania ocen, o których mowa w art. 66a uzupełniany był o jednostki stricte techniczne, w tym certyfikacyjne, które w oparciu o przyjęte międzynarodowe standardy, mogłyby przedstawiać ocenę techniczno-inżynierską ocenianych dostawców. Jednostki te mogłyby być zarówno	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

			laboratoriami publicznymi, jak i prywatnymi niekoniecznie posiadającymi siedzibę na terytorium Polski. Taki element oceny byłby w naszej ocenie korzystny również dla bezpieczeństwa i trwałości samej decyzji, która posiadając wyraźne podstawy techniczne byłaby trudniejsza do późniejszego kwestionowania, w tym ramach ewentualnych postępowań w zakresie roszczeń. • Należy dodać możliwość zgłoszenia wniosku przez kilku członków Kolegium wspólnie. Zagadnienia w zakresie cyberbezpieczeństwa mają charakter międzysektorowy. W związku z tym, należy dopuścić możliwość składania wniosku, którego inicjatorem może być więcej podmiotów, niż jeden. • W związku z postulowanym brakiem włączania przedsiębiorców komunikacji elektronicznej do zakresu krajowego systemu cyberbezpieczeństwa, art. 66a ust. 1 należy uzupełnić o odwołanie do przedsiębiorców komunikacji elektronicznej, o których mowa w PKE. • W zakresie dokonywanych ocen należy uwzględniać także zagrożenia związane z aplikacjami. Warto bowiem zauważyć, że proponowana nowelizacja będzie nakładała na dostawców sprzętu czy operatorów telekomunikacyjnych bardzo wygórowane wymagania i środki wpływu/kontroli, natomiast pomijana jest zupełnie kwestia aplikacji, która ma fundamentalne znaczenie dla cyberbezpieczeństwa. Aplikacje mogą mieć dostęp do GPS/mikrofonu/wiadomości/plików. Już dziś są na rynku aplikacje, które w jawny sposób stosują podsłuch, umożliwiają nagrywanie nie tylko rozmów telefonicznych, ale i całego otoczenia, a same śledzą użytkownika włączając GPS-a. To zagrożenie dla cyberbezpieczeństwa powinno być adresowane w szerszym nawet zakresie niż ryzyko związane z samą siecią. • Niezbędne jest wprowadzenie przepisu wskazującego, że podmioty zobowiązane do dostosowania się do opinii Kolegium	sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast

			są zwolnione z wszelkiej odpowiedzialności cywilnoprawnej wobec dostawcy, którego urządzenia lub oprogramowanie zostały wskazane w ocenie ryzyka.	przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
338.	PIIT		1.2. Art. 66a ust. 1 – przedmiot oceny W projektowanym ust. 1 wskazano, że ocena może dotyczyć „ryzyka dostawcy sprzętu lub oprogramowania istotnego dla	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione.

			cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa”. Poza powyższymi uwagami zauważamy, że przepis nie jest wystarczająco precyzyjny. W szczególności nie jest jasne czy zwrot „istotnego” odnosi się do „ryzyka”, „dostawcy” czy do „sprzętu lub oprogramowania”. W naszej ocenie, powinien on wyraźnie referować do samego sprzętu lub oprogramowania. Tym samym postulujemy nadanie ust. 1 następującego brzmienia: 1. Kolegium może sporządzić, na wniosek członka lub członków Kolegium, ocenę ryzyka dostawcy dotyczącą sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa lub przedsiębiorców komunikacji elektronicznej. Ponadto zakres „istotnego sprzętu lub oprogramowania” powinien być w zakresie sieci telekomunikacyjnych, rozumiany zgodnie z koncepcją „kluczowych aktywów/zasobów” do których referuje 5G Toolbox (essential assets) oraz koncepcją kluczowej infrastruktury, której wykaz należy sporządzić zgodnie z par. 2 pkt 2 rozporządzenia do art. 175d PT także w odniesieniu do sieci 5G. Do tego samego zakresu powinny referować ewentualne restrykcje opisane w dalszej części projektu. W projekcie ustawy należy wyraźnie doprecyzować podstawę na której określany będzie zakres kluczowych zasobów, pod katem których dokonywana jest ocena ryzyka oraz nakładane restrykcje. W tym kontekście zwracamy bowiem uwagę na konkretne zapisy 5G Toolbox gdzie wskazano, że działanie to ma polegać na: • SM03 - Ocena profilu ryzyka dostawców i stosowanie ograniczeń dla dostawców uznawanych za obarczonych wysokim	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

			ryzykiem - w tym niezbędne wyłączenia w celu skutecznego ograniczenia ryzyka - dla kluczowych aktywów. o Ustanowić ramy z jasnymi kryteriami, biorąc pod uwagę czynniki ryzyka określone w pkt 2.37 skoordynowanej oceny ryzyka UE i dodając informacje specyficzne dla danego kraju (np. Ocena zagrożenia przeprowadzona przez krajowe służby bezpieczeństwa itp.), Dla właściwych organów krajowych i operatorów sieci ruchomej o Przeprowadzać rygorystyczne oceny profilu ryzyka wszystkich odpowiednich dostawców na poziomie krajowym i / lub UE (na przykład wspólnie z innymi państwami członkowskimi lub innymi operatorami sieci ruchomej); o Na podstawie oceny profilu ryzyka zastosować ograniczenia - w tym niezbędne wyłączenia w celu skutecznego ograniczenia ryzyka - dla kluczowych aktywów określonych jako krytyczne lub wrażliwe w skoordynowanym sprawozdaniu z oceny ryzyka UE (np. Funkcje sieci bazowej, funkcje zarządzania siecią i orkiestracji oraz funkcje dostępu do sieci); o Podjęcie kroków w celu zapewnienia, że operatorzy sieci ruchomej mają odpowiednie mechanizmy kontrolne i procesy zarządzania potencjalnym ryzykiem szczątkowym, takie jak regularne audyty łańcucha dostaw i oceny ryzyka, solidne zarządzanie ryzykiem Stąd uważamy, że ocena dostawcy nie może być oderwana od oferowanych przez niego urządzeń lub oprogramowania, które mogą lecz nie muszą stanowić kluczowych zasobów/aktywów i tym samym stanowić lub nie stanowić istotnego zagrożenia dla bezpieczeństwa. Wcześniejsze określenie, np. w rozporządzeniu zakresu aktywów uznawanych za kluczowe byłoby bardzo istotnym narzędziem również dla samych użytkowników, którzy dla takich przypadków	W ramach postępowania będą badane aspekty techniczne i nietechniczne, tak jak wymaga tego Toolbox 5G. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

			mogliby kierować się szczególnymi wymaganiami bezpieczeństwa. Zapewniłoby to również nieporównywalnie większą przewidywalność skutków potencjalnych wykluczeń.	do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.
339.	PIIT	Art. 66a ust 2 i 3	1.3. Art. 66a ust. 2 i 3 – zakres oceny i wniosku W ust. 2 zbyt ogólnie wskazano obligatoryjny zakres wniosku, który de facto mógłby być ograniczony do wskazania, że należy ocenić dostawcę X, który działa w zakresie np. telekomunikacji. Tymczasem spektrum oferowanych urządzeń lub oprogramowania może być tak szerokie, że skutki ewentualnego wydania oceny wobec całości działalności mogą prowadzić do całkowitego zablokowania telekomunikacji w Polsce, w tym w zakresie terminali abonenckich. W przypadku, więc gdyby ocenie miały podlegać urządzenia lub oprogramowanie dla sieci telekomunikacyjnych należałoby wyraźnie wskazać już we wniosku, że ocenie podlega dostawca w zakresie oferowanych	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być

			urządzeń lub oprogramowania dla sieci 5G Stand Alone, lub core 5G, a nie np. dla sieci 4G, sieci fix, czy terminali abonenckich. Jednocześnie wniosek nie powinien w naszej ocenie pozostawać bez uzasadnienia. Ponadto warto zauważyć, że projektowany system oceny będzie miał zastosowanie uniwersalne, nie tylko do dotychczas dyskutowanego obszaru sieci 5G, ale także wobec wszelkich innych zastosowań u podmiotów krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, tj. m.in. sektora energetyki, finansowego, ochrony zdrowia, wody, transportu. Tym samym brak precyzji wniosku może skutkować tym, że np. wykluczenie dokonane wobec danego dostawcy, będzie potencjalnie uzasadnione wobec jednego sektora, ale w drugim spowoduje istotne, niezbadane i nieoczekiwane reperkusje, które trudno będzie naprawić. Teoretyczny brak możliwości przedstawienia takich doprecyzowań na etapie wniosku nie powinien być argumentem przeciwko doprecyzowaniu przepisów. Ocena i jej skutki będą potencjalnie bardzo brzemienne w skutkach i nie mogą być realizowane bez odpowiedniego przygotowania, które powinno być wymagane od wszystkich członków Kolegium, a w szczególności od wnioskodawcy. Docelowo wniosek o wydanie opinii przez Kolegium powinien już w całości przedstawiać zagadnienie do rozstrzygnięcia przez Kolegium. Postulaty: • W ust. 2 postulujemy dodanie, jako obligatoryjnych elementów wniosku: o Identyfikacja urządzeń lub oprogramowania dostawcy, stanowiących kluczowe zasoby/aktywa, które mają podlegać ocenie ryzyka, a w przypadku dokonywania oceny w zakresie sieci	wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu

			lub usług komunikacji elektronicznej wskazanie konkretnych typów sieci i jej warstw lub usług, których ocena ryzyka i jej konsekwencje mają dotyczyć. Podobnie jak w przypadku procedur certyfikacji należy wyraźnie określać, co jest oceniane. Inne ryzyko rodzi wykorzystywanie Security Gateway, inne BTS'a, inne radiolinii, a inne anteny pasywne danego producenta. o Identyfikacja podmiotów, które wykorzystują lub mogą wykorzystywać urządzenia lub oprogramowanie dostawcy, które mają podlegać ocenie ryzyka, w tym wskazanie czy są to podmioty krajowego systemu cyberbezpieczeństwa czy przedsiębiorcy komunikacji elektronicznej, o których mowa w PKE. o Identyfikacja poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny. o Identyfikacja poziomu zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy. o Identyfikacja innych podmiotów działających na tym samym rynku co oceniany dostawca, w zakresie urządzeń i oprogramowania, w którego zakresie ma zostać dokonana ocena. o Określenie, jakiego zakresu dotyczy ocena, tj. czy np. powszechnego użycia (usługa masowa) czy np. użycia w określonych systemach czy usługach (np. rejestry państwowe, określone kategorie przemysłu, określone strategiczne lokalizacje). o Uzasadnienie wniosku, w tym przedstawienie potencjalnych ryzyk związanych z wykorzystaniem urządzeń lub oprogramowania danego dostawcy. o Identyfikacja zagrożeń w zakresie:	Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach

			- możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. - analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania; - prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą: a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, c) prawodawstwo w zakresie ochrony danych osobowych, nieosobowych oraz ochronie prywatności, zwłaszcza tam gdzie nie ma porozumień między UE i danym państwem, d) strukturę własnościową dostawcy sprzętu lub oprogramowania, e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania; - liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów dotyczących sprzętu lub oprogramowania danego dostawcy; - stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania, dostarczania i utrzymania sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;	- termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

			- treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy. o Identyfikacja rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy o Ocena skutków regulacji zawierająca: identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii; identyfikację skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów o Rekomendacje działań dla Kolegium - zakładany czas aktualizacji opinii; - rekomendacje działań dla Kolegium; - czas wdrożenia do 10 lat; - proponowany mechanizm refinansowania kosztów przedsiębiorców lub użytkowników, w tym konsumentów. • Ust. 3 powinien zostać włączony (po dostosowaniu) do ust. 2, jako obligatoryjny element wniosku. Tym samy ust. 3 powinien zostać usunięty.	
340.	PIIT	Art. 66a ust.4	1.1. Art. 66a ust. 4 – kryteria oceny Przedstawione kryteria oceny dostawcy wskazują, że ocena będzie dokonywana nie pod kątem technicznych zagrożeń związanych z wykorzystaniem sprzętu lub oprogramowania ocenianego dostawcy, ale pod kątem czynników ogólnych o charakterze potencjalnym i geopolitycznym. Wśród kryteriów brak jest takich, które w jasny sposób odnoszą się do sfery techniki, czy budowanego dorobku w zakresie certyfikacji, zarówno tej ogólnej, jak i tej, która będzie opierana na Cybersecurity Act, gdzie przecież bezpieczeństwo 5G jest jednym z kandydatów do wprowadzenia certyfikacji europejskiej. Decyzja o utrzymaniu takiego kształtu regulacji pozostaje oczywiście w	**Uwaga nieuzwględniona** Kryteria oceny są zgodne z Toolbox 5G.

			mocy ustawodawcy. Warto jednak zaznaczyć, że ani przepisy, ani uzasadnienie nie odnoszą się do potencjalnej sytuacji, w której ocena ryzyka na poziomie wysokim lub umiarkowanym musiałaby zostać wydana np. wobec dostawcy z kraju UE lub NATO. Wydaje się, więc, że dla zapewnienia niezbędnego obiektywizmu, oraz w celu uniknięcia ryzyka i zarzutu, jaki można postawić projektowanym obecnie przepisom należałoby doprecyzować, jakie skutki i jakie reguły kolizyjne będą stosowane w przypadku wpływu wydania oceny i np. faktycznego zablokowania wymiany handlowej w jakimś zakresie, na prawo międzynarodowe i zawarte umowy, traktaty czy porozumienia. Postulaty: • Za zasadne uznajemy (tak jak w pkt 1.1 powyżej) uzupełnienie zakresu oceny o dokonanie weryfikacji technicznej przez certyfikowane w odpowiednim zakresie laboratorium. Taka ocena będzie niezbędna także dla określenia poziomu ryzyka oraz możliwości wdrożenia odpowiednich środków technicznych i organizacyjnych na podstawie art. 66a ust. 5. • Prowadzona ocena ryzyka powinna zostać skorelowana z istniejącymi już schematami certyfikacji oraz odnosić się do ew. wykrytych niezgodnościami z dokumentacją standaryzacyjną dla danego typu urządzenia (np. 3GPP czy ITU). Ponadto należy w ramach mechanizmów oceny uwzględnić budowany na bazie rozporządzenia Cybersecurity Act system certyfikacji europejskiej, który ma dotyczyć również 5G. • Badaniu powinien również podlegać wpływ na konkurencję i konsumentów, a także możliwość utrzymania ciągłości usług, systemów i produktów, w których stosowane jest dane oprogramowanie lub urządzenie. Ocenie należy poddać czy wydanie oceny nie będzie skutkowało ograniczeniem możliwości świadczenia usług oraz faktycznym powstaniem na krajowym	

			rynku monopoli lub duopoli oraz związanym z tym realnym ryzykiem dla przedsiębiorstw i konsumentów. • Obowiązkiem Kolegium powinno być zidentyfikowanie podmiotów, których ocena ryzyka będzie dotyczyła (posiadających lub mogących planować zakup urządzeń lub oprogramowania ocenianego dostawcy) oraz zapoznanie się z ich opinią w sprawie dokonywanej oceny. • Należy rozważyć, czy w art. 66a ust. 4 nie uzupełnić zakresu o EOG/EFTA. Ponadto, należy odnieść się do faktu, że przynajmniej w zakresie sieci 5G istnieją, jeszcze nieobecni na polskim rynku dostawcy, którzy nie są formalnymi członkami NATO, ale z Sojuszem współpracują w ramach inicjatyw partnerskich. Kwestia ta może mieć fundamentalne znaczenie dla poziomu konkurencyjności rynku.	
341.	PIIT	Art. 66a ust. 5	1.5. Art. 66a ust. 5 – poziomy ryzyka Projektowany ust. 5 zawiera generalne wytyczne do sposobu określania poziomu ryzyka. Zastosowane sformułowania ogólne, tj. „poważne", „niewielkie", „znikome", a także brak informacji, w jaki sposób ma być dokonywana ocena czy możliwe jest wdrożenie środków technicznych i organizacyjnych w zasadzie uniemożliwiają dokonanie faktycznej oceny przepisu i jego potencjalnych skutków. Wynika to przede wszystkim z faktu, że kryteria te będą mogłyby być bardzo elastycznie stosowane i dopasowywane przez samo Kolegium w toku oceny. Tym samym, wydaje się, że niemal każda decyzja mogłaby w ich świetle znaleźć uzasadnienie formalnie odpowiadające kryteriom. Postulaty: • Należy doprecyzować kryteria, np. poprzez odwołanie się kategorii ryzyka wystąpienia incydentów o określonych poziomach istotności, w tym ciągłości działania lub naruszenia	**Wyjaśnienie** Zrezygnowano z poziomów ryzyka umiarkowany, niski, brak zidentyfikowanego poziomu ryzyka.

			bezpieczeństwa danych u podmiotów krajowego systemu cyberbezpieczeństwa oraz przedsiębiorstw komunikacji elektronicznej. • Wnioskujmy o dodanie doprecyzowania, które będzie mówiło, iż Kolegium wystawia ocenę ryzyka dostawcy tylko w obszarze, który został przeanalizowany i nie blokuje to możliwości współpracy w innych obszarach z takim dostawcą. Przykładowo np. telefony komórkowe dopuszczone standardami międzynarodowymi albo elementy pasywne jak anteny, światłowody, etc. – nie powinny podlegać restrykcjom.	
342.	PIIT	Art. 66a ust.6-8	**1.1. Art. 66a ust. 6 -8 - forma oceny** Proponowane rozwiązanie polega na nadaniu ocenie Kolegium formy „Komunikatu" publikowanego w Monitorze Polskim. Jednocześnie, dostawca w zależności od poziomu oceny ma możliwość przedstawienia środków zaradczych i planu naprawczego (niejasne, czym się faktycznie różnią) albo odwołania. Abstrahując od tego, że dotychczas nieupowszechniona jest praktyka procedury odwoławczej od publikacji Komunikatu w oficjalnym publikatorze (stosowanie KPA, dwuinstancyjność, właściwość sądu) należy szczegółowo rozpatrzyć ewentualne skutki tych środków „negocjacyjnych" i odwoławczych na podmioty obowiązane do stosowania się do treści Komunikatu i poziomu dokonanej oceny. Nie może bowiem dochodzić do sytuacji, w których ocena ryzyka wskazuje na ryzyko wysokie, a więc od publikacji Komunikatu nie jest możliwe np. wdrażanie urządzeń danego dostawcy (co ma swoje skutki organizacyjne, finansowe, techniczne i dla ciągłości usług), ale po rozpatrzeniu odwołania decyzja i treść Komunikatu się zmieniają. Tak doniosłe w skutkach	**Uwaga uwzględniona** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.

			dokumenty muszą być wydawane w formie ostatecznej i w pełni skutecznej. **Postulaty:** • Publikowany Komunikat musi mieć formę ostateczną. Wszelkie ustalenia, wymiana stanowisk, negocjacje i badanie stanu faktycznego muszą nastąpić w toku postępowania oceniającego. Finalny Komunikat musi mieć stabilną formułę i być zmieniany wyłącznie w przypadkach szczególnej wagi tj. trybie, o którym mowa w ust. 9. • Odpowiednią dla ogłoszenia oceny formą działania powinna być forma decyzji administracyjnej. • Komunikat powinien określać termin wejścia w życie oceny i jej skuteczności wobec konkretnych podmiotów, o których mowa w art. 66b ust. 1. Termin ten powinien być odpowiedni na dostosowanie się przedsiębiorców do jego treści, tj. być nie krótszy niż 12 miesięcy. • Podmiotem uprawnionym do odwołania od oceny powinien być również podmiot, którego dotyczą jego postanowienia, w tym ewentualnie przedsiębiorca telekomunikacyjny szczególnie, że jego skutki oceny będą dotyczyły w bardzo zbliżonym zakresie.	
343.	PIIT	66b ust 1	**2. Art. 66b ust. 1 – wysokie ryzyko** **Postulaty:** o W zdaniu pierwszym należy odwołać się do daty wejścia w życie Komunikatu, a nie „sporządzenia oceny”. Moment	**Wyjaśnienie** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone

			sporządzenia oceny nie jest równoznaczny z upublicznieniem Komunikatu, ani jego wejściem w życie. o W zdaniu pierwszym zwrot „podmioty krajowego systemu cyberbezpieczeństwa" należy uzupełnić o słowa „oraz przedsiębiorcy komunikacji elektronicznej". o Ocena nie powinna odwoływać się do „usług" które wg wcześniejszych przepisów nie są objęte oceną. o Skutki oceny powinny odnosić się do kluczowych zasobów/aktywów, zgodnie z naszymi wcześniejszymi uwagami. o Pkt 1) powinien otrzymać brzmienie: *„nie dokonują zakupów sprzętu lub oprogramowania określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji, kiedy dokonanie zakupów lub wdrożeń jest niezbędne dla funkcjonowania ich sieci, infrastruktury lub zapewnienia poziomu jakości oraz ciągłości świadczonych usług zgodnie z zapotrzebowaniem, w tym naprawy awarii lub uszkodzeń oraz następuje to w okresie nie dłuższym niż określony w opinii Kolegium;".* Propozycja ma na celu uniknięcie bardzo negatywnych skutków gospodarczych, w których ocena byłaby wydana i weszła w życie po dokonaniu zakupu, ale przed wdrożeniem, które jest procesem ciągłym i długotrwałym. Po drugie dokonywanie pewnych zakupów lub wdrożeń (aktualizacja oprogramowania, dokończenie procesu inwestycyjnego) jest konieczne dla utrzymania ciągłości świadczenia usług, przynajmniej w okresie wyznaczonym na dokonanie całkowitej wymiany, co miałoby znaczenie gdyby dana	przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję. Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres

			ocena miała zastosowanie do wykorzystywanego już sprzętu lub urządzeń. Jeśli byłoby to konieczne, o takich zakupach lub wdrożeniach podmiot mógłby informować Kolegium, natomiast samo ich dopuszczenie jest niezbędne. ○ Pkt 2) powinien otrzymać brzmienie: *„wycofują z użytkowania sprzęt lub oprogramowanie określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż w okresie określonym w opinii Kolegium, który nie może być jednak krótszy niż 10 lat od dnia wejścia w życie ogłoszenia komunikatu o ocenie*”. Przewidziany w pierwotnej propozycji przepisu 5 letni okres na wycofanie jest zdecydowanie krótszy niż podobne rozwiązania przyjmowane w innych krajach, np. we Francji licencje wydawane są na okres do 8 lat, a w Wielkiej Brytanii czas na wycofanie od momentu ogłoszenia decyzji ma wynieść ponad 7 lat. Jednocześnie realne okresy amortyzacji urządzeń są zdecydowanie dłuższe i sięgają okresu 9-10 lat, przy czym to i tak nie odpowiada technicznej użyteczności, która co do zasady jest dłuższa niż okres amortyzacji. Stąd postulujemy przyjęcie okresu 10 letniego, a w każdym przypadku efektywnie nie krótszego niż 8 lat. Dodatkowo w tym zakresie wyjaśniamy, że praktyczna realizacja opinii Kolegium: ▪ oznacza przeprowadzenie szerokich plac analitycznych oraz planistycznych po stronie przedsiębiorców telekomunikacyjnych, w zakresie przygotowania procedury wyboru nowego dostawcy i wdrożenia nowych elementów	użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

			sieciowych lub oprogramowania **– niezbędny jest czas na wdrożenie opinii!**; ▪ oznacza przeprowadzenie procedury przetargowej i dodatkowych negocjacji przeprowadzenia wyboru nowego dostawcę sprzętu lub oprogramowania **– niezbędny jest czas na wdrożenie opinii!**; ▪ oznacza przeprowadzenie procesu wdrożenia sprzętu lub oprogramowania oraz przeprowadzenia procesu odtwarzania dodatkowych funkcjonalności, w tym dodatkowych szkoleń pracowników **– niezbędny jest czas na wdrożenie opinii!**; ▪ istnieje ryzyko kumulacji przetargów zmiany dostawcy sprzętu lub oprogramowania po stronie wielu przedsiębiorców telekomunikacyjnych (w kraju i za granicą), przekraczających możliwości dostawców w danym okresie i w konsekwencji opóźnienia **– niezbędny jest czas na wdrożenie opinii!**; ▪ istnieje ryzyko kumulacji działań po stronie dostawców przedsiębiorców telekomunikacyjnych w zakresie integracji nowego sprzętu lub oprogramowania, co będzie powodować opóźnienia **– niezbędny jest czas na wdrożenie opinii!**; ▪ oznacza poniesienie dodatkowych opłat administracyjnych np. pozwoleń radiowych. Niezbędny jest czas na minimalizowanie nieprzewidzianych obciążeń przedsiębiorców telekomunikacyjnych;	

			▪ oznacza poniesienie dodatkowej marży dla dostawców „nowego” sprzętu i oprogramowania, którzy będą tworzyć i wykorzystywać presję czasową na przedsiębiorców telekomunikacyjnych **– niezbędny jest czas na wdrożenie opinii!** ▪ oznacza poniesienia dodatkowej marży dla dostawców „starego” sprzętu lub oprogramowania, którzy będą wykorzystywać wszelkie nieprzewidziane działania po stronie przedsiębiorców telekomunikacyjnych **– niezbędny jest czas na wdrożenie opinii!** ▪ oznacza kumulację dodatkowych kosztów przez przedsiębiorców telekomunikacyjnych związanych z utrzymywaniem sprzętu lub oprogramowania „starego” i „nowego” dostawcy, w okresie przejściowym; ▪ w przypadku złożonych usług telekomunikacyjnych na rynku B2B, zmiana dostawcy sprzętu lub oprogramowania oznaczać będzie przeprowadzenia dodatkowych ustaleń z klientami B2B w zakresie integracji; ▪ istnieje uzasadnione ryzyko pogorszenia jakości usług telekomunikacyjnych w okresie przejściowym, co może powodować dodatkowe finansowe reperkusje w stosunku do użytkowników końcowych; Podsumowując, oceniamy iż istnieje uzasadnione ryzyko, iż zmiana dostawcy sprzętu lub oprogramowania spowoduje kumulację zamówień do dostawców „nowego”	

			sprzętu, co w konsekwencji prowadzić będzie do opóźnień. Z reguły rynek telekomunikacyjny w Polsce w okresie 2 – 3 lat osiąga zdolność techniczną porównywalną do najbardziej wartościowych rynków telekomunikacyjnych (USA, Korea, Niemcy, Wlk Brytania). Czynnik ten musi być brany pod uwagę przy określaniu terminu wdrożenia opinii, w porównaniu do innych bogatszych rynków. Jednocześnie opinia Kolegium może mieć wpływ na konkurencyjność rynku telekomunikacyjnego, ponieważ przedsiębiorcy telekomunikacyjni w różnym stopniu będą posiadać sprzęt lub oprogramowanie określonego dostawcy. W celu uniknięcia tak dalece idących konsekwencji opinii Kolegium, niezbędne jest zastosowanie wydłużonego czasu na jej realizację.	
344.	PIIT	Art. 66b ust 2	2.1. Art. 66b ust. 2 – umiarkowane ryzyko Postulaty: o W zdaniu pierwszym należy odwołać się do daty wejścia w życie Komunikatu, a nie „sporządzenia oceny". Moment sporządzenia oceny nie jest równoznaczny z upublicznieniem Komunikatu ani jego wejściem w życie. o W zdaniu pierwszym zwrot „podmioty krajowego systemu cyberbezpieczeństwa" należy uzupełnić o słowa „oraz przedsiębiorcy komunikacji elektronicznej".	**Wyjaśnienie** Zrezygnowano z umiarkowanego poziomu ryzyka, do procedury zastosowane zostanie KPA.

			○ Ocena nie powinna odwoływać się do „usług” które wg wcześniejszych przepisów nie są objęte oceną. ○ Skutki oceny powinny odnosić się do kluczowych zasobów/aktywów, zgodnie z naszymi wcześniejszymi uwagami. ○ Pkt 1) powinien otrzymać brzmienie: *„nie dokonują zakupów sprzętu lub oprogramowania określonych w ocenie danego dostawcy sprzętu lub oprogramowania”* Uzasadnienie jak wyżej dla ryzyka wysokiego. ○ Pkt 2 powinien otrzymać brzmienie: *„mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu lub oprogramowania wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania, w tym dokonywać zakupów lub wdrożeń jest to niezbędne dla funkcjonowania ich sieci, infrastruktury lubzapewnienia poziomu jakości oraz ciągłości świadczonych usług zgodnie z zapotrzebowaniem, w tym naprawy awarii i uszkodzeń.”* Uzasadnienie jak wyżej dla ryzyka wysokiego.	
345.	Nanocoder	Art. 66a	Przepisy art. 66a niniejszego projektu nie zapewniają pełnych i równych praw dla podmiotów objętych postępowaniem oceniającym ryzyko, które gwarantuje chociażby Kodeks Postępowania Administracyjnego. Niniejsze przepisy nie umożliwiają odwołania się od decyzji kolegium dotyczącej oceny określającej średnie i niskie ryzyko, co jest niedopuszczalne. Nielogicznym jest umożliwienie podmiotom odwołania się	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z

			jedynie od oceny określającej ryzyko wysokie. Ponadto niespotykanym rozwiązaniem jest fakt, że odwołanie nie zawiesza wykonalności decyzji. Obecne zapisy pozbawiają stronę zainteresowaną obiektywnej i niezależnej ochrony podstawowych praw w postępowaniu	urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne

				związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
346.	T-Mobile Polska	Art. 66a	**Propozycja zmiany:** *Art. 66a. 1. Kolegium może sporządzić, na <u>wniosek jednego lub kilku członków</u> Kolegium, ocenę ryzyka dostawcy sprzętu lub*	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu

			oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. **<u>Uzasadnienie:</u>** Zagadnienia w zakresie cyberbezpieczeństwa mają charakter międzysektorowy. W związku z tym, należy dopuścić możliwość składania wniosku, którego inicjatorem może być więcej podmiotów, niż jeden.	cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania

				może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

347.	Signum Edward Kuś Marcin Kuś	Art. 66a ust. 1	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Ustanowienie warunków dla oceny ryzyka **Uzasadnienie** Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie wszystkich aktywów. Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego, zidentyfikowanego ryzyka a niezakładanego ryzyka. § 2 pkt 13 Rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych (...) przewiduje, że przedsiębiorcy telekomunikacyjni przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności **Przepisy** Art. 66a ust. 1 **Sugestie** Ocenę ryzyka przeprowadza się wyłącznie: 1) W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie. 2) , Gdy wystąpiły poważne naruszenia bezpieczeństwa lub podatności, których nie można załagodzić.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
348.	GBX Soft	Art. 66a ust. 1	Szczególnie kontrowersyjny w mojej ocenie jest art. 66a, który w ustępie 1 stanowi, że Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Przy czym podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka, a nie zakładanego ryzyka. Ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka. W związku z powyższym celowym wydaje się wprowadzenie zmiany zapisów, zgodnie z którymi ocenę ryzyka przeprowadza się wyłącznie w odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie lub w sytuacji gdy wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji.

				Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub

				oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
349.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Art. 66a ust. 1	**Uzasadnienie:** 1) Zestaw narzędzi UE dla działań ograniczających ryzyka dla skupienia analizy ryzyka na kluczowych aktywach zamiast wszystkich aktywach. 2) Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka a nie zakładanego ryzyka. 3) ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka. **Propozycja zmiany:** Ocenę ryzyka przeprowadza się wyłącznie: 1) W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie. 2) Wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

				Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
350.	Excogitate	Art. 66a ust. 1	Metody Kontroli Cyberbezpieczeństwa Ustanowienie warunków dla oceny ryzyka 1. Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie dla wszystkich aktywów. 2. Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka a nie zakładanego ryzyka. ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada, że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka. Ocenę ryzyka przeprowadza się wyłącznie: 1. W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za

			Wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić	wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę

				wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
351.	KIGEIT	Art. 66a ust. 1	**Propozycja zmiany**: ***„****Kolegium, a w stosunku do przedsiębiorców komunikacji elektronicznej Prezes UKE, może sporządzić, ~~na wniosek członka Kolegium,~~ ocenę ryzyka ~~dostawcy~~ związaną ze sprzęt~~u~~em lub oprogramowani~~a~~em ~~istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa~~ o znaczeniu krytycznym, decydującym o sposobie zarządzania: przetwarzaniem informacji i przesyłania danych, mechanizmami kryptograficznymi, mechanizmami zarządzania wirtualizacją oraz interfejsami zapewniającymi uprawnionym podmiotom dostęp do przekazów nadawanych lub odbieranych w sieci podmiotów krajowego systemu bezpieczeństwa cybernetycznego. Ocena ta jest dokonywana:* ***a)*** *po stwierdzonym istotnym naruszeniu bezpieczeństwa lub integralności usług kluczowych o istotnym wpływie na funkcjonowanie tych usług na poziomie krajowym i spowodowanym przez sprzęt i oprogramowanie danego dostawcy, w zakresie objętym naruszeniem, lub*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka

			b) *wykryciu wysokiej podatności sprzętu lub oprogramowania zwiększającej istotnie poziom ryzyka wystąpienia naruszenia bezpieczeństwa lub integralności usług kluczowych o istotnym wpływie na funkcjonowanie tych usług na poziomie krajowym, w zakresie objętym wykrytą podatnością i kiedy operator usługi kluczowej, którego dotyczy podatność oraz dostawca tego sprzętu i oprogramowania, poinformują Kolegium lub odpowiednio Prezesa UKE w przypadku przedsiębiorców komunikacji elektronicznej o braku możliwości ograniczenia ryzyka."* **Uzasadnienie:** 1) Jak zostało wskazane we wstępie, sektor powszechnych usług komunikacji elektronicznej z uwagi na specyfikę powinien pozostać kompleksowo regulowany w osobnych przepisach jego dotyczących (tj. w ustawie Prawo komunikacji elektronicznej, które zastąpi ustawę Prawo telekomunikacyjne) i poddany kompleksowemu nadzorowi jednego organu regulacyjnego (Prezes Urzędu Komunikacji Elektronicznej - UKE), z zastrzeżeniem realizowanych przez niektórych przedsiębiorców zadań kluczowych z punktu widzenia bezpieczeństwa publicznego, podobnie jak ma to miejsce obecnie. Dlatego proponujemy, by w stosunku do przedsiębiorców telekomunikacyjnych ocenę przeprowadzał Prezes UKE. Rozwiązanie to jest zgodne z postanowieniami tytułu V EKŁE, zatytułowanego „Bezpieczeństwo" (art. 40-41 EKŁE). Zgodnie z motywem 5 EKŁE, celem tej dyrektywy jest stworzenie ram prawnych dla zapewnienia swobody w zakresie dostarczania sieci i usług łączności elektronicznej, podlegających wyłącznie warunkom określonym w niniejszej dyrektywie oraz ograniczeniom zgodnie z art. 52 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej, a w szczególności środkom podejmowanym w	zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

			związku z polityką państwową, bezpieczeństwem publicznym oraz zdrowiem publicznym, oraz spójne z art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej. Zgodnie z art. 1 ust. 3 lit c) EKŁE, postanowienia tej dyrektywy pozostają bez uszczerbku dla działań podejmowanych przez państwa członkowskie do celów zachowania porządku publicznego i bezpieczeństwa publicznego oraz obronności. Nie mogą być jednak sprzeczne z art. 1 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (Dz. Urz. UE L Nr 194, s. 1), który stanowi, że wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz. Urz. UE. L Nr 108, str. 33), ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014. Zgodnie więc z tymi przepisami problematyka dotycząca realizacji bezpieczeństwa powinna być uregulowana w odpowiednim akcie prawnym, regulującym rynek sieci i usług łączności elektronicznej, którym obecnie jest ustawa Prawo telekomunikacyjne a przyszłości będzie ustawa Prawo komunikacji elektronicznej. Organem właściwym na rynku usług łączności elektronicznej w zakresie spraw dotyczących m.in. bezpieczeństwa, zgodnie z art. 192 ust. 1 pkt 9 obowiązującej ustawy Prawo telekomunikacyjne, jest Prezes Urzędu Komunikacji Elektronicznej. Zgodnie z tym przepisem, do zakresu działania Prezesa UKE należy w szczególności wykonywanie obowiązków na rzecz obronności,	Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			bezpieczeństwa państwa i porządku publicznego (w tym dział VIIA Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych – art. 175-175e). Analogiczne rozwiązania przewiduje projekt ustawy Prawo komunikacji elektronicznej. Wprost o kompetencji Prezesa UKE w zakresie zapewnienia bezpieczeństwa publicznej sieci telekomunikacyjnej stanowi art. 375 ust. 2 pkt 5 lit f) PKE. Rozdział 5 PKE zatytułowany jest Bezpieczeństwo sieci i usług oraz zadania i obowiązki na rzecz obronności, bezpieczeństwa państwa i porządku publicznego. W rozdziale 5 znajduje się oddział 1, w którym uregulowane zostały kwestie dotyczące obowiązku stosowania przez przedsiębiorców telekomunikacyjnych środków zapewniających bezpieczeństwo sieci lub usług oraz obowiązku sporządzania planu działań w sytuacjach szczególnych zagrożeń (art. 39-49 PKE). Organem kompetencyjnym w zakresie spraw tam wymienionych jest Prezes UKE. W szczególności to Prezes UKE dokonuje oceny podjętych przez przedsiębiorcę komunikacji elektronicznej środków technicznych i organizacyjnych, o których mowa w art. 39 ust. 2 pkt 2 PKE, kierując się rekomendacjami Agencji Unii Europejskiej do spraw cyberbezpieczeństwa (art. 40 ust. 1 PKE). Następnie, „może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek: 1) zastosowania dodatkowych środków technicznych i organizacyjnych lub 2) w przypadku powstania uzasadnionych wątpliwości co do stosowania właściwych środków bezpieczeństwa, poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę podmiot i udostępnienia Prezesowi UKE wyników takiego audytu” (art. 40 ust. 3 PKE). Szczegółowe wymagania dla podmiotu, który mógłby przeprowadzić wskazany audyt oraz podstawowe obowiązki	

			audytora określa art. 41 PKE. W uzasadnieniu PKE, dotyczącym art. 40 ust. 3 wyjaśniono, że art. 40 ust. 3 pkt 1 PKE stanowi właśnie implementację art. 41 ust. 1 EKŁE, a art. 40 ust. 3 pkt 2 PKE stanowi implementację art. 41 ust. 2 lit b PKE. Kompetencje Prezes UKE w zakresie dokonywania ocen jest więc zbieżna w zakresie kompetencji z dotychczasowymi postanowieniami obowiązującej ustawy Prawo telekomunikacyjnej, opartej na europejskich dyrektywach w zakresie łączności elektronicznej oraz obowiązujący już EKŁE oraz projektowanej ustawy PKE, stanowiącej wdrożenie do polskiego porządku prawnego EKŁE. 2) Zgodnie z Toolbox 5G, (str. 12)."Ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka — ma następować w odniesieniu do kluczowych aktywów", projekt nie bierze pod uwagę kategorii aktywów z punktu widzenia bezpieczeństwa, wraz z poziomem wrażliwości i listą kluczowych elementów (kategorie elementów i funkcji). Niewłaściwe jest nakładanie takich samych zobowiązań na wszystkie aktywa. 3) Niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), również dlatego, że przewiduje całościowe wyłączenie dostawcy, np. z wyłączeniem określonego dostawcy. Toolbox 5G SM03 przewiduje możliwość wyłączenia, ale z wyłączeniem dostaw określonej infrastruktury (aktywa kluczowe). Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox'ie	
352.	Unia Metropolii Polskich	Art. 66a. 1	Wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa.	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy

			Oznacza to, że rząd mógłby zablokować przetarg z konkretnymi podmiotami, jeżeli specjalne Kolegium, w wyniku analizy wielu czynników, wykazałoby np. zbyt duże powiązanie firmy z rządem innego kraju, zwłaszcza spoza Unii Europejskiej i NATO (lex Huawei). W przepisie nie ma wskazania mechanizmu kontroli niezależnych sądów. W projekcie można przeczytać, że można się odwołać od oceny Kolegium do … Kolegium.	Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji

				na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
353.	KIGEIT	Art. 66a ust 2-3	**Propozycja** zmiany:	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione.

			2. Wniosek o ~~sporządzenie~~ wydanie opinii ~~oceny~~ zawiera wskazanie: *1) danych identyfikujących dostawcę sprzętu lub oprogramowania;* *2) możliwych obszarów działalności, w których ~~dostawca~~ sprzęt~~u~~ lub oprogramowani~~a~~e może stanowić zagrożenie dla bezpieczeństwa narodowego.* *3) ocena skutków regulacji zawierająca:* *a) identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii;* *b) identyfikacja skali działań mających zostać podjętych przez przedsiębiorstwa komunikacji elektronicznej, podmioty publiczne i użytkowników końcowych, w tym kosztów związanych ze skutkami ewentualnej opinii;* *c) oczekiwany harmonogram działań;* *4) rekomendacje działań dla Kolegium lub odpowiednio Prezesa UKE w stosunku do przedsiębiorców komunikacji elektronicznej* *5) proponowany mechanizm refinansowania kosztów przedsiębiorców komunikacji elektronicznej lub użytkowników końcowych;* *6) czas wdrożenia nie krótszy niż 10 lat,* *7) zakładany czas aktualizacji opinii;* *3. Wniosek o sporządzenie oceny może określać:* *1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub,* *2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa* *- które uwzględnia się przy sporządzeniu oceny ~~dostawcy~~ sprzętu lub oprogramowania.* **Uzasadnienie:**	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

			Z punktu widzenia bezpieczeństwa sieci i usług głównym źródłem ryzyka są konkretne rozwiązania techniczne oferowane przez tych dostawców. W konsekwencji ocena ryzyka powinna być przeprowadzana dla danego typu sprzętu lub oprogramowania, ale nie charakterystyki dostawcy. Z kolei ocenę bezpieczeństwa dostawcy należy oceniać z punktu widzenia bezpieczeństwa procesu produkcji i zapewnienia ciągłości dostaw. Należy podkreślić, że na obecnym rynku wielu dostawców funkcjonuje w modelu zintegrowanym pionowo (np. Samsung, Huawei), w którym dostarczane przez nich rozwiązania funkcjonują w różnych obszarach sieci i maja zróżnicowany wpływ na bezpieczeństwo sieci i usług. Przykładowo jeden dostawca może być producentem zarówno terminali użytkownika, jak również inwerterów elektrycznych w instalacjach fotowoltaicznych przy stacjach bazowych, infrastruktury radiowej oraz oprogramowania w sieci szkieletowej. Każdy z tych elementów powinien być oceniany z punktu widzenia roli, jaką pełni w świadczeniu usług telekomunikacyjnych, a nie z punktu widzenia rodzaju dostawcy	W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

354.	T-Mobile Polska	Art. 66a ust. 3, 8	**Propozycja zmiany zakresu wniosku art. 66a ust. 3 [opis w nawiasach ma wyjaśnić cel zapisu]** *2. Wniosek o sporządzenie oceny zawiera wskazanie:* ***[cel: identyfikacja dostawcy]*** *1) danych identyfikujących dostawcę sprzętu lub oprogramowania;* ***[cel: identyfikacja produktu]*** *2) produktu lub grupy produktów dostawcy, w tym obszar ich lokalizacji, realizowanych funkcji w sieciach teleinformatycznych, świadczonych usługach w oparciu sprzęt lub oprogramowanie;* ***[cel: identyfikacja odbiorców]*** *3) odbiorców sprzętu lub oprogramowania* ***[cel: identyfikacja poziomu wykorzystywania w sektorze prywatnym i publicznym]*** *3) poziomu wykorzystania sprzętu lub oprogramowania przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych;* *5) poziomu wykorzystania sprzętu lub oprogramowania w realizacji przez przedsiębiorców telekomunikacyjnych obowiązków wynikających ze stanów nadzwyczajnych i stanu wojny;* *4) poziom zobowiązań przedsiębiorców telekomunikacyjnych i użytkowników końcowych wobec dostawcy;* ***[cel: identyfikacja zagrożeń]*** *6) możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego.*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie

			7) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania; *8) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą:* *a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,* *b) ~~prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka~~,* *c) prawodawstwo w zakresie ochrony danych osobowych, <u>nieosobowych oraz ochronie prywatności</u>, zwłaszcza tam gdzie nie ma porozumień między UE i danym państwem,* *d) strukturę własnościową dostawcy sprzętu lub oprogramowania,* *e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;* *9) liczbę i rodzaje oraz sposób i czas eliminowania wykrytych podatności i incydentów dotyczących sprzętu lub oprogramowania danego dostawcy;* *10) stopień, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania, dostarczania <u>i utrzymania</u> sprzętu lub oprogramowania oraz ryzyka dla procesu wytwarzania, dostarczania i utrzymania sprzętu lub oprogramowania;* *11) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.*	przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla

			[cel: identyfikacja rozwiązań alternatywnych] *12) rozwiązań alternatywnych działań w stosunku do sprzętu lub oprogramowania danego dostawcy* ***[cel: ocena skutków opinii]*** *13) ocena skutków regulacji zawierająca:* *a) identyfikację podmiotów lub grupy podmiotów ponoszących koszty ewentualnej opinii;* *b) identyfikacja skali działań mających zostać podjętych przez przedsiębiorstwa telekomunikacyjne, podmioty publiczne i użytkowników końcowych, w tym kosztów związanych ze skutkami ewentualnej opinii;* *c) oczekiwany harmonogram działań;* ***[cel: rekomendowane działania dla Kolegium]*** *14) rekomendacje działań dla Kolegium* *15) proponowany mechanizm refinansowania kosztów przedsiębiorców telekomunikacyjnych lub użytkowników końcowych;* *16) czas wdrożenia nie krótszy niż 10 lat,* *17) zakładany czas aktualizacji opinii;* <u>Uzasadnienie:</u> Zgodnie z uwagami przedstawionymi w części ogólnej, wniosek o wydanie opinii powinien już w całości przedstawiać w pełnym wymiarze zagadnienie dla Kolegium, w tym konsekwencje jakie będą związane z podjęciem decyzji przez Kolegium i wdrożeniem w życie jej postanowień.	bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

			Uzasadnienia dla przyjęcia okresu „10 lat” na wdrożenie opinii. Praktyczna realizacja opinii Kolegium: a) oznacza przeprowadzenie szerokich plac analitycznych oraz planistycznych po stronie przedsiębiorców telekomunikacyjnych, w zakresie przygotowania procedur wyboru nowego dostawcy i wdrożenia nowych elementów sieciowych lub oprogramowania; b) oznacza przeprowadzenia procedur przetargowych i dodatkowych negocjacji oraz przeprowadzenia wyboru nowego dostawcy sprzętu lub oprogramowania; c) oznacza przeprowadzenie procesu wdrożenia sprzętu lub oprogramowania oraz przeprowadzenia procesu odtwarzania dodatkowych funkcjonalności (tzw. ‘features’), w tym dodatkowych szkoleń pracowników. W tym miejscy zaznaczamy, iż oferta dostawców sprzętu i oprogramowania jest zazwyczaj zróżnicowana w zakresie dostępności różnych funkcjonalności dla operatora. Zazwyczaj dostępność konkretnych funkcjonalności na ‘roadmapach’ poszczególnych dostawców jest na tyle różna, że ponowne ich odtworzenie w sieci operatora – po usunięciu sprzętu innego dostawcy – może zająć nawet kilka lat, a niektóre z funkcjonalności mogą okazać się trwale niedostępne dla operatora, powodując brak możliwości świadczenia niektórych usług; d) istnieje ryzyko kumulacji przetargów zmiany dostawcy sprzętu lub oprogramowania po stronie wielu przedsiębiorców telekomunikacyjnych (w kraju i za granicą), przekraczających możliwości dostawców w danym okresie i w konsekwencji opóźnienia daleko większe niż standardowo możliwe do akceptacji na rynku;	

			e) istnieje ryzyko kumulacji działań po stronie dostawców przedsiębiorców telekomunikacyjnych w zakresie integracji nowego sprzętu lub oprogramowania, co będzie powodować opóźnienia; f) oznacza poniesienie dodatkowych opłat administracyjnych np. konieczność sfinansowania przez operatora opłat związanych z wydaniem nowych pozwoleń radiowych. Niezbędny jest czas na minimalizowanie nieprzewidzianych obciążeń przedsiębiorców telekomunikacyjnych; g) oznacza poniesienie dodatkowej marży dla dostawców „nowego" sprzętu i oprogramowania, którzy traktując tę sytuację jako szansę rynkową będą podwyższać ceny i wykorzystywać presję czasową na przedsiębiorców; h) oznacza poniesienia dodatkowej marży dla dostawców „starego" sprzętu lub oprogramowania, którzy będą wykorzystywać wszelkie nieprzewidziane działania po stronie przedsiębiorców telekomunikacyjnych; i) oznacza kumulację dodatkowych kosztów przez przedsiębiorców telekomunikacyjnych związanych z utrzymywaniem i integracją sprzętu lub oprogramowania „starego" i „nowego" dostawcy, w okresie przejściowym; j) w przypadku złożonych usług telekomunikacyjnych na rynku B2B, zmiana dostawcy sprzętu lub oprogramowania oznaczać będzie przeprowadzenia dodatkowych ustaleń z klientami B2B w zakresie integracji; k) istnieje uzasadnione ryzyko pogorszenia jakości usług telekomunikacyjnych w okresie przejściowym, co może powodować dodatkowe finansowe reperkusje w stosunku do użytkowników końcowych;	

			l) w ramach cyklu życia danego produktu/usługi, zdolność sieci musi być stale rozwijana, przynajmniej pod kątem pojemności, aby zapewnić zdolność do bieżącego reagowania na wzrastające zapotrzebowanie. Oznacza to, iż w okresie przejściowym operator będzie musiał realizować inwestycje z obecnym dostawcą. Wydatek inwestycyjny może mieć związek z np. zakupem dodatkowej pojemności/funkcjonalności, aż do ostatecznego wycofania danego elementu sieciowego. Oznacza to, iż należy rozszerzyć okres 5 lat o dodatkowy czas (tj. w sumie do 8-10 lat), uwzględnić okres amortyzacji funkcjonowania elementu sieciowego, wraz z dodatkową pojemnością/funkcjonalnością, która została zakupiona w pierwszym okresie 5 lat. Podsumowując, oceniamy iż istnieje uzasadnione ryzyko, iż zmiana dostawcy sprzętu lub oprogramowania spowoduje kumulację zamówień do dostawców „nowego" sprzętu, co w konsekwencji prowadzić będzie do opóźnień i wzrostu cen. Z reguły rynek telekomunikacyjny w Polsce w okresie 2 – 3 lat osiąga zdolność techniczną porównywalną do najbardziej wartościowych rynków telekomunikacyjnych (USA, Korea, Niemcy, Wlk Brytania). Czynnik ten musi być brany pod uwagę przy określaniu terminu wdrożenia opinii, w porównaniu do innych bardziej rozwiniętych rynków. 1. Propozycja uwzględnienie procesu konsultacji *2a Wniosek przed złożeniem do Kolegium jest konsultowany z przedsiębiorcami telekomunikacyjnymi, stosuje się przepisy o ochronie informacji niejawnych.* <u>Uzasadnienie:</u>	

			Z uwagi na daleko idące konsekwencje dla gospodarki, niezbędne jest konsultacja wniosku przed przedłożeniem do Kolegium, aby uwzględnić istotne zagadnienia w procesie decyzyjnym, zwiększyć pewność prawną zaangażowanych stron. Proponujemy zmianę ust. 8 *8. Dostawca sprzętu lub oprogramowania <u>oraz przedsiębiorca komunikacji elektronicznej</u>, którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.* <u>Uzasadnienie:</u> Koszty wdrożenia opinii Kolegium ponosi dostawca sprzętu lub oprogramowania, ponieważ traci potencjalne przychody z tytułu sprzedaży sprzęty lub oprogramowania. Dodatkowo koszty ponosi też przedsiębiorca telekomunikacyjny, który będzie musiał ponieść dodatkowe koszty związane ze zmianą dostawy sprzętu lub oprogramowania. W związku z tym, zarówno dostawca sprzętu lub oprogramowania oraz przedsiębiorstwa komunikacji elektronicznej ponoszą koszty opinii Kolegium. Oznacza to, iż powinni mieć uprawnienie do weryfikacji decyzji Kolegium.	
355.	Związek Cyfrowa Polska	Art. 66a ust. 4	W art. 66a ust 4 (kryteria oceny ryzyka) dodanie punktów 6 i 7 w brzmieniu: *6) udział danego dostawcy sprzętu lub oprogramowania przekraczający 50% w:* *a)krajowym rynku infrastruktury telekomunikacyjnej, w tym w szczególności LTE i 5G*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z

			b)infrastrukturze sieci telekomunikacyjnych poszczególnych operatorów *7) stosowanie rozwiązań uniemożliwiających dywersyfikację, interoperacyjnośći kompatybilność z innymi dostawcami na pozostawienie w sieci już zbudowanej elementów infrastruktury niekrytycznej, pod warunkiem otwarcie interfejsów przez ich dostawców i wycofania elementów infrastruktury krytycznej w celu zastąpienia ich dostawcą o niskim lub zerowym poziomie ryzyka.* 3. Przyznanie Ministrowi właściwemu do spraw informatyzacji, po zasięgnięciu opinii Kolegium, kompetencji do określania, w drodze rozporządzenia, maksymalnego parytetu udziału jednego dostawcy w sieci publicznej (czyli w skali sieci jednego operatora lub sieci narodowej), przynajmniej w zakresie infrastruktury krytycznej. 4. Wskazanie wprost w art. 66a ust. 7 stosowania otwartych interfejsów dla poszczególnych elementów infrastruktury sieciowej jako środka pozytywnie wpływającego na ocenę ryzyka.	urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne

				związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
356.	Związek Banków Polskich	Art. 66a ust. 4	Poprawka językowa. Art. 66a ust. 4 Przy sporządzaniu oceny przeprowadza się w szczególności: (…)	**Uwaga uwzględniona**

357.	KIGEIT	art. 66a ust. 4 pkt 1	**Propozycja** zmiany: *„4. W ramach sporządzania oceny przeprowadza się w szczególności:* *1)analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich jakie stanowi ~~dostawca~~ dany typ sprzętu ~~i~~ lub oprogramowania*". **Uzasadnienie:** Analiza winna mieć charakter przedmiotowy, a nie podmiotowy – dotyczyć samego sprzętu i oprogramowania zamiast ich dostawcy. Pod względem podmiotowym ewentualne zagrożenie jest bardziej uzależnione od tego, kto używa sprzętu w taki sposób, aby stwarzać takie zagrożenie niż od tego, kto ten sprzęt sprzedaje.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
358.	Polska Izba Handlu	art. 66a ust. 4 pkt 1	**Propozycja zmiany:** W art. 66a ust. 4 pkt 1 („analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania") usunąć słowa „jakie stanowi dostawca sprzętu i oprogramowania": *„analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich.* **Uzasadnienie:** Polska Izba Handlu jako organizacja branżowa współpracująca podmiotami, które na co dzień konkurują ze sobą doskonale rozumie jak ważna jest etyka konkurencji. Z drugiej strony zachowanie różnorodności tak zakresie obszarów, którymi zajmujemy się bezpośrednio jak i dostawców innych usług z których zarówno handel jak i inne branże będą szeroko korzystać jest niezbędne dla zapobiegania działaniom quasi monopolistycznym. Jako, że naszym mottem **jest zachowanie różnorodności handlu i usług na rynku wewnętrznym** wierzymy, że zapewnienie równych możliwości prowadzenia walki konkurencyjnej wszystkim podmiotom rynku jest kluczowe dla jego rozwoju. Pozwalamy sobie mieć nadzieję iż jedyne kryteria według jakich oceniane są lub będą oferty to spójność z oczekiwaniami biznesowymi inwestora oraz warunki współpracy, co wynika z zasad swobody prowadzenia działalności gospodarczej. Podsumowując liczymy, że ocena proponowanych rozwiązań oparta będzie na tym czym rozwiązania są, a nie czym mogłby być	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji.

			gbyby korzystano z nich w złej woli, ponieważ żadne usługi ani produkty nie są ze swej natury dobre ani złe.	Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub

				oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
359.	KIGEIT	Art. 66a ust. 4 pkt 2	**Propozycja**: przepis powinien zostać usunięty ~~*Prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą:*~~ ~~*a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,*~~ ~~*b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka,*~~ ~~*c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,*~~ ~~*d) strukturę własnościową dostawcy sprzętu lub oprogramowania,*~~ ~~*e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania)*~~ **Uzasadnienie:** 1) Ocena musi być przeprowadzana na podstawie jasno określonych, jednoznacznych i możliwych do zweryfikowania kryteriów. W przeciwnym razie nie będzie to obiektywna ocena, lecz ocena uznaniowa, bez uzasadnienia merytorycznego, prowadząca do błędnych wniosków; 2) Ocena na podstawie kraju pochodzenia niesie ze sobą istotną dyskryminację; 3) Jest to sprzeczne z przepisami §6 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			prawodawczej" (t.j. Dz.U. z 2016 r., poz. 283 z późniejszymi zmianami): *„Przepisy ustawy redaguje się tak, aby dokładnie i w sposób zrozumiały dla adresatów zawartych w nich norm wyrażały intencje prawodawcy."* Przepisy prawa winny być tak sformułowane, aby intencje prawodawcy były dokładnie wyrażone adresatom zawartych w nich norm. Projektowane normy naruszają przepisy rozporządzenia, ponieważ są one niezrozumiałe i nie jest możliwe określenie ich treści. Wiele niepewności i wątpliwości interpretacyjnych przewiduje przykładowo "prawdopodobieństwo wpływu dostawcy sprzętu lub oprogramowania na kraj spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego" – jest niejasne i rodzi następujące pytania: Jaki stopień prawdopodobieństwa? Co to znaczy „być pod wpływem państwa"? Jak należy rozumieć "wpływ" – czy chodzi o politykę, ekonomię itp.? Czy wpływ państwa powinien zawsze być oceniany negatywnie?	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
360.	GBX Soft	Art. 66a ust. 4 pkt 2-5	Patrząc dalej, ten sam art. 66a, ust. 4, pkt 2)-5) powinien zawierać jasne, bezstronne i obiektywne kryteria oceny ryzyka. Co gwarantuje poprawność wyników zastosowanych kryteriów oceny, bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. W tym wypadku celową wydaje się propozycja ustanowienia wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania, a także wymaganie od dostawców posiadania oświadczenia o wiarygodności, ustawienia wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT oraz wprowadzenie odniesienia do modelu niemieckiego.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za

				wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę

				wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
361.	Polska Izba Handlu	art. 66a ust. 4 pkt 2-5	**Propozycja zmiany: Art. 66a ust. 4 pkt 2-5 otrzymuje następujące brzmienie:** *„Do sporządzania oceny przeprowadza się analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami”, w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności:* *a)uzyskanie certyfikatu dla sprzętu lub oprogramowania o znaczeniu krytycznym, o którym mowa w art. 66 a ust. 1 KSC*; *b)posiadanie deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, która powinna w szczególności zawierać :* *ba) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka

			bb) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim; *bc) obowiązek producenta lub dostawcy infrastruktury telekomunikacyjnej polegający na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;* *bd) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej;* *be) deklaracje gotowości producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;* *bf) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;* *bg) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa.* *c)zapewnienie integralności dostarczanych krytycznych składników infrastruktury, a w szczególności:* *ca) zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu;*	zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

			cb) sprawdzenie w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione. *d)prowadzenie monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;* *e)zatrudnianie tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie;* *f)zapewnienie w odpowiednim zakresie redundacji, wskazanym w procedurze bezpieczeństwa, krytycznych składników infrastruktury;* *g)uzyskanie przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego.* **Uzasadnienie:** Zaproponowany powyżej model charakteryzuje się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewnia poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologiczne są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków.	Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
362.	Excogitate	Art. 66a ust. 4 pkt 2)-5)	Metody Kontroli Cyberbezpieczeństwa Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne 1. Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. 2. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji

			wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. 1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2. Wymaga się od dostawców posiadania oświadczenia o wiarygodności. 3. Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT. Wprowadzenie odniesienia do modelu niemieckiego	lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in.

				prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
363.	Polsko-Chińska Główna Izba	Art. 66a ust. 4 pkt 2-5	**Uzasadnienie:** 1) Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy

	Gospodarcza SinoCham		2) Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. 3) Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. **Propozycja zmiany:** 1) Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2) wymaga się od dostawców posiadania oświadczenia o wiarygodności. 3) Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT. 4) Wprowadzenie odniesienia do modelu niemieckiego	Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji

				na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

364.	KIGEIT	Art. 66a ust. 4 pkt 2-5	*„Do sporządzania oceny przeprowadza się analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami", w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności:* *a)uzyskanie certyfikatu dla sprzętu lub oprogramowania o znaczeniu krytycznym, o którym mowa w art. 66 a ust. 1 KSC. Prezes UKE ustala z odpowiednim CSRIT oraz przedsiębiorcami komunikacji elektronicznej świadczącymi usługi w ruchomej publicznej sieci telekomunikacyjnej oraz ich stowarzyszeniami, producentami i dostawcami infrastruktury telekomunikacyjnej oraz ich stowarzyszeniami, listę funkcji i składników sprzętu oraz oprogramowania o znaczeniu krytycznym, w ruchomej publicznej sieci telekomunikacyjnej, którą publikuje na swojej stronie internetowej;* *b)posiadanie deklaracji wiarygodności od producentów i dostawców infrastruktury telekomunikacyjnej, która powinna w szczególności zawierać;* *ba) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do współpracy z przedsiębiorcą w zakresie techniki bezpieczeństwa, a w szczególności do wczesnego informowania o nowych produktach, technologiach i aktualizacjach istniejących linii produktów;* *bb) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że żadne informacje pochodzące z jego relacji umownych z przedsiębiorcą nie zostaną przekazane osobom trzecim;* *bc) obowiązek producenta lub dostawcy infrastruktury telekomunikacyjnej polegający na niezwłocznym poinformowaniu przedsiębiorcy, że nie może już zagwarantować dotrzymania zadeklarowanego zobowiązania;*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

			bd) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do posługiwania się wyłącznie godnymi zaufania pracownikami przy opracowywaniu i produkcji krytycznych pod względem bezpieczeństwa części infrastruktury telekomunikacyjnej; *be) deklaracje gotowości producenta lub dostawcy infrastruktury telekomunikacyjnej do wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie;* *bf) zapewnienie producenta lub dostawcy infrastruktury telekomunikacyjnej, że produkt, którego dotyczy składana deklaracja, nie posiada celowo wdrożonych wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie;* *bg) zobowiązanie producenta lub dostawcy infrastruktury telekomunikacyjnej do niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa.* *c)zapewnienie integralności dostarczanych krytycznych składników infrastruktury, a w szczególności:* *ca) zapewnienie możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie, począwszy od ich odbioru a skończywszy na uruchomieniu;* *cb) sprawdzenie w czasie odbioru, czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione.* *d)prowadzenie monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;*	zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

			e)zatrudnianie tylko przeszkolonych specjalistów w obszarach związanych z bezpieczeństwem, posiadających stosowne kompetencje i doświadczenie; *f)zapewnienie w odpowiednim zakresie redundacji, wskazanym w procedurze bezpieczeństwa, krytycznych składników infrastruktury;* *g)uzyskanie przez producenta sprzętu telekomunikacyjnego międzynarodowych lub uznanych przez UE norm bezpieczeństwa cybernetycznego, takich jak ISO27001, Common Criteria, Network Equipment Security Scheme, unijny program certyfikacji cyberbezpieczeństwa.* **Uzasadnienie:** Zaproponowany powyżej model charakteryzuje się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewnia poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologiczne są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków.	do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
365.	Signum Edward Kuś Marcin Kuś	Art. 66a ust. 4 pkt 2-5	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne **Uzasadnienie** Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania

			niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny. **Przepisy** Art. 66a ust. 4 pkt 2)-5) **Sugestie** 1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2. Wymaganie od dostawców posiadania oświadczenia o wiarygodności. 3. Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT. Skorzystanie z wzorca modelu niemieckiego	dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa

				dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
366.	KIGEIT	art. 66a ust. 5	**Propozycja zmiany:** doprecyzowanie definicji w zakresie gradacji ryzyk i usunięcie odniesień do dostawców. **Przepis art. 66a ust. 5 Projektu otrzymuje następujące brzmienie:** **„**5. *Sporządzona ~~przez Kolegium~~ ocena ~~ryzyka dostawcy sprzętu lub oprogramowania~~ określa:* *a) wysokie ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowanie~~a~~ stanowi bardzo poważne zagrożenia dla cyberbezpieczeństwa*	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W

			państwa ~~i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe”.~~ *b) umiarkowane ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowani~~e~~~~a~~ stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo* *c) niskie ryzyko, jeżeli ~~dostawca~~ sprzęt~~u~~ lub oprogramowani~~e~~~~a~~ stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo* *d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.* **Uzasadnienie** Niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), dlatego, że przewiduje całościowe wyłączenie dostawcy bez odniesienia do konkretnych „krytycznych aktywów”. Toolbox istotnie przewiduje możliwość wyłączenia, ale to wyłączenie dotyczy określonej infrastruktury. Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox’ie. Wątpliwości budzi także przyjęta w art. 66a ust. 5 Projektu gradacja ryzyk, a ściśle ich definiowanie. Chodzi o różnicę pomiędzy wysokim ryzykiem a ryzykiem umiarkowanym. W przypadku bowiem obu definicji jest to poważne zagrożenie a różnica polega na tym, że w przypadku wysokiego ryzyka zmniejszenie tego ryzyka nie jest możliwe a w przypadku umiarkowanego jest możliwe. Tymczasem powinny te definicje (art. 66a ust. 5 lit a-b Projektu) różnić się gradacją, tak jak się różnią ryzyka opisane w art. 66a ust. 5 lit b-d Projektu, a nie tym czy można to ryzyko zmniejszyć czy też nie, gdyż należy przyjąć,	ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub

			że zawsze można poziom takiego ryzyka zmniejszyć a przynajmniej powinno się stworzyć możliwość dla dostawcy podjęcia próby jego zmniejszenia. Poważne więc zastrzeżenia budzi przyjęcie z góry założenia, że w przypadku „wysokiego ryzyka" zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe. W kontekście zaproponowanych zmian polegających na bezpośrednim powiązaniu oceny z dostawcą, po raz kolejny wskazujemy, że analiza powinna mieć charakter przedmiotowy (dotyczyć sprzętu), a nie podmiotowy (dotyczyć charakterystyki samego dostawcy).	oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
367.	Signum Edward Kuś Marcin Kuś	Art. 66a ust. 7	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Możliwość zmiany wyniku oceny powinna mieć również zastosowanie do sprzętu lub oprogramowania wysokiego ryzyka. **Uzasadnienie**	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego.

			Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku **Przepisy** Art. 66a ust. 7 **Sugestie** Dostawca sprzętu lub oprogramowania wysokiego ryzyka może również przedłożyć Kolegium środki zaradcze i plan naprawczy. Jeżeli te środki zaradcze oraz plan naprawczy zostaną zaakceptowane, Kolegium może zmienić ocenę.	Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie

				podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
368.	KIGEIT	art. 66a ust. 7	**Propozycja zmiany:** **Art. 66a ust. 7 Projektu** powinien otrzymać następujące brzmienie:	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione.

			7. *W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca ~~sprzętu lub oprogramowania~~, którego sprzętu lub oprogramowania dotyczy ~~ta~~ ocena ~~dostawcy sprzętu lub oprogramowania~~, może przedstawić Kolegium lub Prezesowi UKE w przypadku przedsiębiorców komunikacji elektronicznej środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium, a w stosunku do przedsiębiorców komunikacji elektronicznej Prezes UKE, zmienia ~~może zmienić~~ ocenę*. **Uzasadnienie:** Zmiana art. 66a ust. 7 Projektu jest konsekwencją ewentualnej zmiany art. 66a ust. 5 lit a Projektu.	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

				W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

369.	GBX Soft	Art. 66a ust. 7	Ponadto w odniesieniu do ust. 7 omawianego art. 66a należy podkreślić, że możliwość zmiany wyniku oceny powinno mieć zastosowanie również do sprzętu lub oprogramowania wysokiego ryzyka. Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku. Tego rodzaju argumentacja wymagałaby zmiany zapisów, które z wyjątkiem umiarkowanego lub niskiego poziomu ryzyka umożliwią dostawcy sprzętu lub oprogramowania wysokiego ryzyka przedłożenie Kolegium środków zaradczych i planu naprawczego. Jeżeli te środki zaradcze oraz plan naprawczy zostaną zaakceptowane, Kolegium może zmienić ocenę.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie

				przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla

				bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
370.	Polska Izba Handlu	Art. 66a ust. 7	**Propocycja zmiany:** **Art. 66a ust. 7 Projektu** powinien otrzymać następujące brzmienie: 7. W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ocena dostawcy, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ocenę. **Uzasadnienie:** Zmiana art. 66a ust. 7 Projektu jest konsekwencją ewentualnej zmiany art. 66a ust. 5 lit a Projektu.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.

				Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o

				uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
371.	Liquid Systems	Art. 66a ust. 7	Metody Kontroli Cyberbezpieczeństwa Możliwość zmiany wyniku oceny powinna mieć zastosowane również do sprzętu lub oprogramowania wysokiego ryzyka. Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku. Sugestie: Z wyjątkiem umiarkowanego lub niskiego poziomu ryzyka dostawca sprzętu lub oprogramowania wysokiego ryzyka może również przedłożyć Kolegium środki zaradcze i plan naprawczy. Jeżeli te środki zaradcze oraz plan naprawczy zostaną^ zaakceptowane, Kolegium może zmienić ocenę.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący

				sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast

				przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
372.	Związek Banków Polskich	Art. 66a ust. 8	**art. 66a ust. 8:** Dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko lub **podmiot krajowego systemu bezpieczeństwa użytkujący sprzęt lub oprogramowania** którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania **w formie decyzji administracyjnej**. Wniesienie odwołania **wstrzymuje działania** określone w art. 66b. **Od decyzji Kolegium przysługuje skarga do sądu administracyjnego.** Z uwagi na istotne konsekwencje organizacyjne i finansowe (konieczność wycofania użytkowanego sprzętu lub oprogramowania) prawo wniesienia odwołania powinno przysługiwać również podmiotowi użytkującemu taki sprzęt lub oprogramowanie. Wniesienie odwołania powinno wstrzymywać wskazane działania gdyż mogą one wywołać nieodwracalne skutki dla podmiotu krajowego systemu bezpieczeństwa. Postulowane byłoby również wprowadzenie wskazania, iż	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania.

			rozstrzygnięcie kolegium następuje w formie decyzji oraz, iż od takiej decyzji przysługuje odwołanie do sądu, co umożliwiłoby ostateczne rozstrzygnięcie sprawy przez niezależny organ.	Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

				Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
373.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Art. 66a ust. 8	**Uzasadnienie:** 1) Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania. 2) Odwołanie nie zawiesza wykonalności decyzji 3) Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia strony zainteresowanej obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu. **Propozycja zmiany:** 1) Ocena określająca średnie i niskie ryzyko powinna również upoważniać do wniesienia odwołania. 2) Wniesienie odwołania powinno zawieszać wykonalność decyzji.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla

			3) Wynik oceny ryzyka może być przedmiotem odwołania do sądu zgodnie z postanowieniami Kodeksu Postępowania Administracyjnego. 4) Wykonalność decyzji powinna zostać zawieszona do czasu prawomocnej decyzji sądu.	bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania.

				Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
374.	SmartWeb Media	Art. 66a ust. 8	Negatywne implikacje biznesowe niesie za sobą również projektowana regulacja art. 66a ust. 8 zd. trzecie ustawy o krajowym systemie cyberbezpieczeństwa, w myśl którego wniesienie odwołania nie wstrzymuje działań określonych w art. 66b tejże ustawy, tj. zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz obowiązku wycofania z użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o tej ocenie. W celu zapewnienia stabilności	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania

			gospodarczej, wykonalność decyzji powinna zostać zawieszona do czasu uprawomocnienia się oceny ryzyka	dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa

				dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
375.	KIGEIT	Art. 66a ust. 8	**Propozycja zmiany:** *„8. ~~Dostawca sprzętu lub oprogramowania którego dotyczy~~ Od ocen~~a~~y określającae**j** ~~wysokie~~ ryzyko ~~może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium~~ przysługuje wniosek o ponowne rozpatrzenie sprawy; do wniosku tego stosuje się odpowiednio przepisy dotyczące odwołań od decyzji. Kolegium rozpatruje ~~odwołanie~~ wniosek o ponowne rozpatrzenie sprawy w ciągu 2 miesięcy od otrzymania.*	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W

			~~*Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.*~~ **Uzasadnienie:** Od rozstrzygnięcia, stanowiącego decyzję administracyjną, powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka sprzętu lub oprogramowania ocenianego dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mnie dotkliwa. Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie", nie stanowi w istocie odwołania, ale wniosek o ponowne rozpatrzenie sprawy, o którym mowa w art. 127 § 3 KPA. Z uwagi na fakt, że Kolegium nie należy do organów wskazanych w powyższym przepisie, konieczne jest ujęcie wprost odniesienia do przepisów dotyczących odwołań od decyzji, za wyjątkiem przedsiębiorców komunikacji elektronicznej, dla których organem właściwym do rozpatrywania odwołań będzie Prezes UKE. Ostatnie zdanie winno zostać wykreślone, gdyż pozostaje w sprzeczności z art. 130 § 1 KPA. W praktyce oznaczałoby również, że przewidziane w tym przepisie „odwołanie" nie miałoby żadnego praktycznego znaczenia, skoro pomimo jego wniesienia byłyby podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontraktu na sprzedaż infrastruktury telekomunikacyjnej.	ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub

				oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
376.	Excogitate	Art. 66a ust.8	**Mechanizm odwołań od decyzji kolegium** Zapewnić zakres pełnych i równych praw zgodnie z Kodeksem Postępowania Administracyjnego 1. Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego.

			2. Odwołanie nie zawiesza wykonalności decyzji Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia stronę zainteresowaną obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu. 1. Ocena określająca średnie i niskie ryzyko powinna również upoważniać do wniesienia odwołania. 2. Wniesienie odwołania powinno zawieszać wykonalność decyzji. 3. Wynik oceny ryzyka może być przedmiotem odwołania do sądu zgodnie z postanowieniami Kodeksu Postępowania Administracyjnego. Wykonalność decyzji powinna zostać zawieszona do czasu prawomocnej decyzji sądu.	Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie

				podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
377.	Polska Izba Handlu	Art. 66a ust. 8	**Propozycja:** Przepis art. 66a ust. 8 Projektu otrzymuje brzmienie: *„Dostawcy sprzętu lub oprogramowania, którego dotyczy ocena, przysługuje wniosek do Kolegium o ponowne rozpoznanie sprawy*	**Uwaga uwzględniona** Przepisy art. 66a-66c zostaną zmienione.

			w zakresie oceny. Przepisy działu 2 rozdziału 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego w zakresie odwołań od decyzji stosuje się odpowiednio. Od decyzji Kolegium wydanej po rozpoznaniu wniosku o ponowne rozpoznanie sprawy przysługuje skarga do Wojewódzkiego Sądu Administracyjnego. **Uzasadnienie:** Od rozstrzygnięcia Kolegium powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mnie dotkliwa. Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie" jest pozorowana, pozbawiająca podstawowych praw podmiotów zainteresowanych weryfikacją dokonanej oceny przez Kolegium w sposób obiektywny i niezależny przez sąd. Przyjęta konstrukcja pozwala na to, że Kolegium będzie „sędzią we własnej sprawie" tj. będzie sprawdzało własną decyzję. W prawie przewidziana jest konstrukcja złożenia wniosku o ponowne rozpoznanie sprawy przez organ, który wydał decyzję, ale zawsze przysługują środki odwoławcze do sądu od takiego ponownego rozpoznania sprawy. Potwierdzeniem tezy o pozorowanej konstrukcji odwołania, a wręcz o jej fikcyjności jest dodatkowo to, że zgodnie z obecnym brzmieniem art. 66a ust. 8 Projektu, zdanie ostatnie: *Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b.* W praktyce oznacza to więc, że przewidziane w tym przepisie	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii.

			„odwołanie” nie ma żadnego praktycznego znaczenia, skoro pomimo jego wniesienia będą podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontaktu na sprzedaż infrastruktury telekomunikacyjnej.	W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.

378.	Narodowy Bank Polski	Art. 66a ust. 10	**Dodanie w projektowanym art. 66a ust. 10 o treści:** „10. Sporządzana przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania wskazująca wysokie lub umiarkowane ryzyko ma zastosowanie wobec Narodowego Banku Polskiego jedynie w zakresie w jakim nie wywiera wpływu na realizację zadań NBP. Po ogłoszeniu komunikatu, o którym mowa w ust. 6, NBP przekazuje Kolegium informację o ewentualnym ograniczeniu stosowania oceny ryzyka dostawcy sprzętu lub oprogramowania.”.	**Uwaga nieuwzględniona** Obowiązek wycofania sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych.
379.	Excogitate	Art. 66b	Operatorzy telekomunikacyjni powinni otrzymać rekompensatę za koszty poniesione w związku z wymianą sprzętu lub oprogramowania, a rekompensatę powinno obliczać się na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE.	
380.	Business Centre Club	Art. 66b	BCC zwraca uwagę na finansowe konsekwencje projektowanej regulacji art. 66b Noweli Ustawy zarówno w przypadku oceny wysokiego, jak i umiarkowanego ryzyka. Ustawodawca wprowadzając w przypadku oceny wysokiego ryzyka nakaz wycofania z użytkowania sprzętu lub oprogramowania nie później niż w terminie 5 lat od dnia ogłoszenia komunikatu o ocenie, nie uwzględnia realiów biznesowych i technicznych, w tym amortyzacji sprzętu lub oprogramowania, zasad projektowania sieci, jej remontów, konserwacji i usuwania awarii,	Wyjaśnienie Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu

			co często nie będzie możliwe przy użyciu innych części niż części oryginalne, a w przypadku użycia zamienników może się wiązać z utratą gwarancji na sprzęt. Brak możliwości naprawy takiego sprzętu (art. 66b ust. 1 pkt 1)) bądź obowiązek pozbycia się go przed upływem okresu amortyzacji (art. 66b ust. 1 pkt 2)) będzie skutkować w najczarniejszym scenariuszu pogorszenie działania sieci, jej czasowe wyłączenia i spadek przychodów sektora telekomunikacyjnego oraz wzrost cen usług detalicznych. Realny czas eksploatacji/zwrotu inwestycji to 10-12 lat.	dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
381.	KIGEIT	Art. 66b	**Propozycja: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2:** *„3. operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;* *4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających”* **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury,

				która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
382.	T-Mobile Polska	Art. 66b ust. 1	**Proponujemy zmianę at. 66b ust. 1** *Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:* *1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;* *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż czas określony w opinii Kolegium~~; 5 lat od dnia ogłoszenia komunikatu o ocenie~~.* **Uzasadnienie:** Czas na wycofanie sprzętu lub oprogramowania ma być określony w opinii Kolegium, ponieważ musi uwzględniać specyficzną sytuację każdego dostawcy sprzętu, przedsiębiorców telekomunikacyjnych oraz użytkowników końcowych	**Uwaga nieuwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
383.	Związek Banków Polskich	Art. 66b ust. 1	Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1)nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; 2) **w miarę istnienia możliwości organizacyjnych i finansowych** wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie.	**Uwaga nieuwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach

			Nakazanie podmiotowi krajowego systemu bezpieczeństwa wycofanie sprzętu i oprogramowania naraża go na poniesienie istotnych kosztów finansowych. Biorąc pod uwagę wskazany okres 5 lat na wycofanie sprzętu lub oprogramowania skuteczność wskazanego instrumentu dla zapewnienia cyberbezpieczeństwa wydaje się i tak iluzoryczna. Postulowane byłoby zatem aby wskazany obowiązek był uzależniony od możliwości danego przedsiębiorcy i powiązany np. z planowanymi postępowaniami zakupowymi sprzętu i oprogramowania.	kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
384.	S4IT Michał Podgórski	Art. 66b ust. 1 pkt 2	Okres 5 lat na wymianę sprzętu jest zbyt krótki. Wymiana sprzętu i oprogramowania uznanego za wysoce ryzykowny będzie wiązała się z koniecznością nabycia nowych komponentów i przystosowania ich do obecnej infrastruktury. Należy mieć na uwadze zarówno koszty wymiany sprzętu, jak i przeszkolenia użytkowników. **Propozycja** Czas wycofania sprzętu z eksploatacji: 10 lat od daty opublikowania ogłoszenia o uznaniu produktu za wysoce ryzykowny.	**Uwaga częściowo uwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
385.	Liquid Systems	Art. 66b ust. 1 pkt 2	Artykuł 66b doprowadzi do powstania istotnych kosztów dla operatorów telekomunikacyjnych, których nie powinni ponosić, a które powinny być pokryte przez Skarb Państwa. **Sugestia**:	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem

			Operatorzy telekomunikacyjny powinni dostać odszkodowanie za koszty poniesione w związku z wymianą sprzętu lub oprogramowania. Odszkodowanie to powinno być naliczone na podstawie kosztów poniesionych na zakup infrastruktury i oprogramowania, przy uwzględnieniu amortyzacji oraz kosztu usunięcia.	sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
386.	Liquid Systems	Art. 66b ust. 1 pkt 2	Okres karencji powinien wynosić 10 lat zamiast 5 lat. Wymiana związana z krytycznym sprzętem i oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci. Zajmie to dużo czasu, a jakikolwiek pospiech w tym zakresie wpłynie negatywnie na stabilność sieci. Również wysokie koszty przemawiają za rozłożeniem procesu wycofania w dłuższym przedziale czasu. Sugestie: Czas wycofania sprzętu: 10 lat od daty opublikowania ogłoszenia o ocenie.	**Uwaga częściowo uwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie

				wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
387.	Polska Izba Handlu	Art. 66b ust. 1 pkt 2	**Projekt przepisu***: „W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:* *1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług infrastruktury krytycznych określonych w ocenie danego sprzętu lub oprogramowania;* *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego sprzętu lub oprogramowania nie później niż ~~5~~ 10 lat od dnia ogłoszenia komunikatu o ocenie."* **Uzasadnienie** Pięcioletni okres na wycofanie jest zdecydowanie za krótki i powinien zostać przedłużony do 10 lat, a wymiana powinna odnosić się do określonego sprzętu i oprogramowaniu zamiast do dostawcy. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz". Przepis nakazujący wycofywanie sprzętu zakupionego wiele lat wcześniej stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu w oparciu o obowiązujące wówczas przepisy. Tym bardziej więc powinien być uwzględniony postulat wycofywania sprzętu z użytkowania	**Uwaga częściowo uwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
388.	Polska Izba Handlu	Art. 66b sekcja 1 pkt 2	**Propozycja: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2:** *3. operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;*	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii

			4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie" operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.	sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
389.	S4IT Michał Podgórski	Art. 66b ust. 1 i ust. 2	**Postulowane wprowadzenie rekompensat.** Artykuł 66b doprowadzi do powstania istotnych kosztów dla operatorów telekomunikacyjnych, których nie powinni ponosić, spowodowanych nowymi regulacjami, które powinny być pokryte przez Skarb Państwa reprezentowany przez Prezesa UKE. **Propozycja:** Przedsiębiorcy telekomunikacyjni powinni otrzymać odszkodowanie z tytułu poniesionych kosztów wymiany sprzętu lub oprogramowania.	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu

				wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
390.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Art. 66b ust. 1 pkt 2	**Przepisy projektu:** brak przepisów dotyczących mechanizmu rekompensat **Propozycja zmiany:** należy dodać ust. 3 oraz 4 w art. 66b po ust. 2.: „3. Operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania; 1. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających.” **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w

			zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie" operatorów z posiadanego sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby niewprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.	tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
391.	Signum Edward Kuś Marcin Kuś	Art. 66b ust. 1 pkt 2	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Okres karencji powinien wynosić 10 lat zamiast 5 lat **Uzasadnienie** Wymiana związana z krytycznym sprzętem i oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci. Zajmie to dużo czasu, a wszelki pośpiech negatywnie wpłynie to na stabilność sieci. Również koszty zmiany będą bardzo wysokie. Dlatego powinny zostać rozłożone w dłuższym okresie czasu. **Przepisy** Art. 66 b ust. 1 pkt 2 **Sugestie** Czas wycofania sprzętu z eksploatacji: 10 lat od daty opublikowania ogłoszenia o ocenie.	**Uwaga częściowo uwzględniona** Zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
392.	Excogitate	art. 66b ust. 1 pkt 2: „Konsekw	**Przepisy projektu**: brak zapisów dotyczących mechanizmu rekompensat Propozycja zmiany: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2.:	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem

		encje oceny”	„3. Operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania; 4. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających.” **Uzasadnienie:** Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby niewprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.	sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G
393.	KIGEIT	Art. 66b ust. 1 pkt 1 i ust. 2 pkt 1	**Propozycja zmiany:** wykreślenie *„Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko ~~dostawcy~~ określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:* *~~1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;~~* *(…)*	**Uwaga nieuwzględniona** Zrezygnowano z poziomu umiarkowanego. Z kolei decyzja o uznaniu za dostawcę wysokiego ryzyka nie powinna być przesłanką do zakończenia wsparcia eksploatacyjnego przez dostawcę tego sprzętu do momentu wycofania danego sprzętu lub oprogramowania z użytkowania.

			2. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: ~~*1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania;*~~ **Uzasadnienie:** Niezmiernie istotne jest uwzględnienie faktu, iż w przypadku kilkuletniego procesu wycofywania sprzętu, oprogramowania i usług określonego dostawcy (wskazanego w pkt 2)) niezbędne będzie realizowanie procesów utrzymaniowych istniejącego sprzętu w tym okresie. Procesy utrzymaniowe mogą m.in. obejmować niezbędną wymianę sprzętu na stacjach bazowych (uszkodzonego w wyniku awarii, wandalizmu, zjawisk atmosferycznych itp.) lub instalację nowego oprogramowania niezbędnego dla funkcjonowania sieci (np. adresującego zidentyfikowane luki w zakresie bezpieczeństwa lub możliwość korzystania z nowych urządzeń sieciowych w bezpieczny sposób), czy też zwiększenie pojemności danego sprzętu. Jednocześnie podmioty, na których będzie ciążył obowiązek wycofania sprzętu, oprogramowania i usług danego dostawcy w ciągu 5 (lub 10 – jak postulujemy) lat nie będą miały ekonomicznego interesu w zwiększaniu współpracy z danym dostawcom powyżej niezbędnego minimum. W konsekwencji postulujemy wykreślenie niniejszego punktu w całości. Gdyby uwaga Izby nie została rozpatrzona pozytywnie, alternatywnym – jednakże dużo mniej elastycznym i nie w pełni przystającym do wieloletniego okresu wycofywania sprzętu, oprogramowania i usług – rozwiązaniem byłoby poniższe doprecyzowanie niniejszego punktu:	

			„1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji niezbędnych dla realizacji funkcji utrzymania oraz niezbędnego rozwoju istniejącego sprzętu, oprogramowania i usług, w odpowiedzi na zgłaszane zapotrzebowanie;"	
394.	KIGEIT	Art. 66b ust. 1 pkt 2	Projekt przepisu*: „Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko ~~dostawcy~~ określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa:* *2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego ~~dostawcy~~ sprzętu lub oprogramowania na obszarze gmin określonych jako najbardziej istotne dla funkcjonowania krajowego systemu cyberbezpieczeństwa nie później niż ~~5~~ 10 lat od dnia ogłoszenia komunikatu o ocenie."* **Uzasadnienie** Ze względu na to, iż obowiązek wycofania sprzętu z użytkowania stanowi poważną ingerencję w swobodę prowadzenia działalności gospodarczej powinien być on ograniczony jedynie do obszarów gmin, które mogą mieć strategiczne znaczenie dla funkcjonowania krajowego systemu cyberbezpieczeństwa, np. obszarów poligonów wojskowych, kluczowych węzłów komunikacyjnych np. lotnisk, terenów związanych z wytwarzaniem i magazynowaniem energii elektrycznej, miejsc składowania rezerw żywności itp. Należy podkreślić, że obowiązek wycofania sprzętu z użytkowania nie powinien mieć zastosowania do obszarów gmin, gdzie w zdecydowanej przewadze prowadzona jest działalność cywilna, w tym gospodarcza. Obszary te nie mają istotnego znaczenia dla funkcjonowania krajowego systemu cyberbezpieczeństwa.	**Uwaga nieuwzględniona** Podmioty krajowego systemu cyberbezpieczeństwa, będą musiały wycofać sprzęt lub oprogramowanie od dostawcy wysokiego ryzyka w terminie do 7 lat**.**

			W konsekwencji pożądanym jest stworzenie listy gmin najbardziej istotnych dla funkcjonowania krajowego systemu cyberbezpieczeństwa, do której będą odnosić się obowiązki wycofania z użytkowania sprzętu, oprogramowania i usług dostawców wysokiego ryzyka. Lista ta może podlegać okresowym przeglądom weryfikującym jej aktualność. Pięcioletni okres na wycofanie jest zdecydowanie za krótki i powinien zostać przedłużony do 10 lat, a wymiana powinna odnosić się do określonego sprzętu i oprogramowania zamiast do dostawcy. Typowy okres eksploatacyjny aktywnej infrastruktury telekomunikacyjnej wynosi co najmniej 7 lat kalendarzowych. Okres 7-letni jest również przyjmowany na potrzeby księgowe jako czas życia aktywów radiowych na potrzeby wyznaczenia odpisów amortyzacyjnych (mimo, iż w praktyce często są one wykorzystywane również po upływie tego okresu). Jednakże amortyzacji będzie podlegał również dodatkowy sprzęt, który został zakupiony w okresie do 7 roku, którego czas amortyzacji będzie wykraczał poza okres 7 letni. Dlatego wskazane jest przyjęcie okresu 10 lat. Okres 7-letni na wycofanie z użytkowania sprzętu i oprogramowania danego dostawcy jest również wskazywany w rozwiązaniach regulacyjnych stosowanych na rynkach międzynarodowych, w szczególności w Wielkiej Brytanii. Konstrukcja wycofywania sprzętu z użytkowania wywołuje poważne wątpliwości z uwagi na obowiązywanie jednej z kardynalnych zasad prawa, tj. zasady „niedziałania prawa wstecz”. Przepis nakazujący wycofywanie sprzętu stanowi objęcie regulacją zdarzeń wcześniejszych, sprzed kilku lat, które dotyczyły zawierania umów o zakup sprzętu w oparciu o obowiązujące	

			wówczas przepisy. Tym bardziej więc powinien być uwzględniony postulat przedłużenia okresu wycofywania sprzętu z użytkowania	
395.	Excogitate	Art. 66c section 1	Metody Kontroli Cyberbezpieczeństwa Okres na dostarczenie planu wycofania wynosi 1 rok zamiast 3 miesięcy. Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania w jest praktycznie niemożliwy do wdrożenia. Okres przygotowania i przedstawienia planu oraz harmonogramu powinien został wydłużony do jednego roku.	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
396.	T-Mobile Polska	Art. 66c ust. 1	**Proponujemy zmianę art. 66c ust. 1** *Art. 66c 1. W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 6~~3~~ miesięcy planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.* *2. Plan i harmonogram podlega zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora, a w przypadku przedsiębiorcy komunikacji elektronicznej z Prezesem UKE.* *3. Zmiana planu i harmonogramu wymaga zatwierdzeniu przez Pełnomocnika po uzgodnieniu z organem właściwym dla danego sektora, a w przypadku przedsiębiorcy komunikacji elektronicznej z Prezesem UKE* **Uzasadnienie:** Okres 3 miesięcy jest zbyt krótkim okresem, aby opracować plan i harmonogram planofwanych zmian, w szczególności, gdy plan/harmonogram będzie w przyszłości podstawą weryfikacji działań prowadzonych przez przedsiębiorców	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

			telekomunikacyjnych, którzy uzależnienie są od podmiotów zewnętrznych „starego” i „nowego” dostawcy.	
397.	Excogitate	art. 66c pkt. 1 “Plan naprawczy”	**Przepis projektu:** W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, sporządzenia i dostarczenia w terminie 3 miesięcy planu i harmonogramu odstąpienia od dostawcy usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Propozycja zmiany: cyfrę i słowo „3 miesięcy” zastępuje się cyfrą i słowem „1 roku”, skreślić „dostawca” tak, aby plan dotyczył konkretnego sprzętu i oprogramowania zamiast dostawcy. „W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, do sporządzenia i dostarczenia w terminie 1 roku planu i harmonogramu odstąpienia od usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.” **Uzasadnienie:** Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do dostawcy.	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
398.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Art. 66c pkt 1	**Przepis projektu:** W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, sporządzenia i dostarczenia w terminie 3 miesięcy planu i harmonogramu odstąpienia od dostawcy usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. **Propozycja zmiany:** cyfrę i słowo „3 miesięcy” zastępuje się cyfrą i słowem „1 roku", skreślić „dostawca" tak, aby plan dotyczył	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

			konkretnego sprzętu i oprogramowania zamiast dostawcy. „W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, do sporządzenia i dostarczenia w terminie 1 roku planu i harmonogramu odstąpienia od usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.” **Uzasadnienie:** Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do dostawcy.	
399.	Liquid Systems	Art. 66c ust. 1	Okres na dostarczenie planu wycofania wynosi rok zamiast 3 miesięcy**.** Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług, sprzętu i oprogramowania jest praktycznie niemożliwy do odtrzymania. **Sugestie:** **Okres przygotowania i przedstawienia planu oraz harmonogramu powinien zostać wydłużony do jednego roku.**	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
400.	Polska Izba Handlu	Art. 66c pkt 1	**3 miesiące na dostarczenie harmonogramu** **Propozycja zmiany:** „W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu roku planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.”	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

			Uzasadnienie: Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do przymiotów	
401.	KIGEIT	Art. 66c ust. 1	**3 miesiące na dostarczenie harmonogramu** **Propozycja zmiany:** *„W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu ~~3 miesięcy~~ roku planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług ~~dostawcy~~ sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko*." **Uzasadnienie:** Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do podmiotów.	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
402.	Signum Edward Kuś Marcin Kuś	ART. 66C UST.1	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Okres na dostarczenie planu wycofania wynosi rok zamiast 3 miesięcy **Uzasadnienie** Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług	**Wyjaśnienie** Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

			sprzętu i oprogramowania jest praktycznie niemożliwy do dochowania. **Przepisy** Art.. 66c ust. 1 **Sugestie** Okres przygotowania i przedstawienia planu oraz harmonogramu powinien zostać wydłużony do jednego roku.	
403.	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM Reprezentowany przez adw. Annę Gąsecką	Art. 66a, 66b, 66c	Odnosząc się do planowanej zmiany polegającej na dodaniu przepisów art. 66a, 66b i 66c Mediakom wskazuje, że nie popiera proponowanych zmian w zakresie w jakim uprawniają one do wydawania wiążących rozstrzygnięć skutkujących powstaniem zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług danego dostawcy oraz obowiązku wycofania ich z obrotu. Mediakom rozumie potrzebę kontroli bezpieczeństwa i jakości sprzętu, oprogramowania i usług dostawców, jednak w jego ocenie proponowana procedura może prowadzić de facto do wykluczenia z rynku dowolnych dostawców i będzie wiązać się z poważnymi kosztami dla przedsiębiorców komunikacji elektronicznej, którzy będą zmuszeni do wymiany być może znacznej części wykorzystywanych urządzeń. Jednocześnie okres wymiany tych urządzeń (5 lat od ogłoszenia komunikatu o ocenie) nie pokrywa się z okresem amortyzacji urządzeń, co dodatkowo wpływa na zwiększenie kosztów nowych urządzeń. Jeśli więc możliwość wydawania wiążących ocen miałaby pozostać, to należy postulować wydłużenie okresu czasu na wymianę urządzeń do 7-8 lat.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

				Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
404.	1Innosystem	Art. 66a-66c	Przepisy ustawy w art. 66a - 66c łączą zagrożenia gospodarcze, kontrwywiadowcze i terrorystyczne z dostawcą sprzętu i oprogramowania, co jest w dużej mierze nieprawdziwe w realnym odniesieniu. Dużo ważniejsze w tej kwestii jest to, kto sprzęt produkuje oraz jakie elementy hardware np.: „chipsety" zainstalował na pokładzie, a co za tym idzie, co się może dziać po upgrade'dzie software, jakie dane przez łącza Internetu, a potem routery brzegowe są wysyłane za granicę, a co za tym idzie, dane te mogą nadrzędnie być monitorowane i wychwycone. Znacząca rola tu jest po stronie Instytucji Teletechnicznych i badań, zanim zostanie dany sprzęt wprowadzony na rynek Polski. Pokazuje to przykład otrzymanych telefonów Huawei, gdzie ta kontrola powinna być znacząco większa.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka

				zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

				Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
405.	1Innosystem	Art. 66a, 66b, 66c	Ponadto analiza art. 66a, 66b i 66c pokazuje, że w systemie cyberbezpieczeństwa wprowadza się jednostronną, uznaniową i subiektywną procedurę oceny działalności dostawców sprzętu, oprogramowania i usług. Taka ocena podaje w wątpliwość, że kontrola zostanie wszczęta z zachowaniem zasady równości i niedyskryminacji dostawców usług czy sprzętu. Dobrze byłoby do tego zaprząc jednostki naukowe, inne firmy IT oraz niezależnych ekspertów (programiści), a także stworzyć bardzo dokładne ramy sposobu badania i elementów analizy kodu, które będą traktowane jako zagrożenie.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania

			Sam sposób możliwości reakcji budzi wiele wątpliwości, zanim przedsiębiorca dowie się o ocenie, nie ma możliwości wytłumaczyć „wątpliwości”, bo nie dostanie szansy odwołania czy wybronienia swojej racji, jedynie już z MONITORA POLSKIEGO dowiaduje się o orzeczonej winie. Będzie to z wielką szkodą jaką wyrządzą w majątku przedsiębiorców po publikacji komunikatu. Zauważmy też, iż w legislacji nie przewidziano odpowiedzialności i prawa do odszkodowania za naruszenie przepisów przez organ oceniający w przypadku pomyłek, a zapewne się zdarzą.	dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa

				dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
406.	Excogitate	Art. 66a - 66c	**Metody Kontroli Cyberbezpieczeństwa** Przedmiotem oceny ryzyka jest sprzęt lub oprogramowanie, a nie dostawca, 1. Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego.

			nieracjonalne i nielogiczne. 2. Istotą regulacji powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje. Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE.' Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny **sprzęt lub oprogramowanie**" w artykule. 66a -66c.	Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie

				podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

407.	Signum Edward Kuś Marcin Kuś	Art. 66 a-c	**Przedmiot** Metody Kontroli Cyberbezpieczeństwa **Ustawa** Przedmiotem oceny ryzyka powinien być sprzęt lub oprogramowanie, a nie dostawca. **Uzasadnienie** Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzęt i oprogramowania jest nieracjonalne i nielogiczne. Ważniejszym pytaniem, od tego, kto jest sprzedawcą, powinno być pytanie, jak korzystać z sprzętu tak, aby nie stanowił onzagrożenia. Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania Zestawu Narzędzi UE **Przepisy** Art. 66a -66c **Sugestie** Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a -66c.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto

				zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku

				do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
408.	Polsko-Chińska Główna Izba Gospodarcza SinoCham	Art. 66 a-c	Uzasadnienie: 1) Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne. 2) Ważniejszym pytaniem powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje. 3) Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE.. **Propozycja zmiany:** Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a - 66c.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

				Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
409.	Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o.	Art. 66 a-c	**Rola, zadania, obowiązki Kolegium** W zapisach brak informacji czy w ramach pracy Kolegium zostanie wypracowana metodyka oceny ryzyka dostawców systemów i usług, w zakresie cyberbezpieczeństwa – np. w formie aktu wykonawczego - rozporządzenia ? Metodyka oceny ryzyka pozwoliłaby na możliwość wstępnego szacowania ryzyka przez podmioty OUK, DUC, na etapie wyboru technologii i dostawców, nie czekając na ocenę Kolegium i konieczność wycofania wybranej technologii.	**Wyjaśnienie** Postępowanie administracyjne będzie prowadził minister właściwy do spraw informatyzacji.
410.	ETOB-RES	Art. 66 a-c	W omawianym projekcie przedmiotem oceny ryzyka jest sprzęt lub oprogramowanie, a nie dostawca. Sugeruję zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a -66c.	**Uwaga nieuwzględniona** W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania.

				Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
411.	Digital Poland	Art. 66a-66c	Pragniemy zauważyć że w większości Państw unijnych sektor telekomunikacyjny nie stanowi elementu KSC. Nie ma go również w tzw. NIS - dyrektywnie unijnej. Wnosimy stąd o usunięcie zatem zapisów dotyczących tego sektora telekomunikacyjnego by zapewnić spójność prawa krajowego z unijnym. W artykule 66a przedstawiono szereg nie merytorycznych kryteriów oceny dostawców. Pozwala to stwierdzić, że w wyniku zmian KSC **wcale nie ulegnie polepszeniu system cyberbezpieczeństwa w Polsce**. To tak jakby z Polskiego rynku wyeliminować samochody produkowane w Meksyku czy Chinach. Wyeliminowanie tych samochodów na bazie czysto politycznych decyzji, nie zwiększy bezpieczeństwa poruszania się po krajowych drogach. Kluczem jest bowiem homologacja czy ocena **testów zderzeniowych Euro NCAP**. Innymi słowy brak jakichkolwiek merytorycznych analiz, brak centra certyfikującego sprzęt, powoduje, że de facto w wyniku proponowanych decyzji osłabimy KSC w Polsce. Zwracamy uwagę, że takie kraje jak Wielka Brytania (uznany sojusznik Stanów Zjednoczonych), ma swoje centrum certyfikacji oraz dokonuje merytorycznej oceny dostawców. Wnosimy się zatem prośbę o podobne zapisy i zmianę, obecnie głównie politycznych, zapisów w zakresie oceny dostawców. **Uważamy, że najwyższym celem jest zwiększenie realnego bezpieczeństwa Polski, a nie** „**papierowe**”. Wnosimy o zmianę **okresu usunięcia dostawców wysokiego ryzyka z sieci** (obecnie 5 lat) – tak złych zapisów nie znajdujemy w Stanach Zjednoczonych, Wielkiej Brytanii czy każdym innym kraju sojuszniczym, a nie w Unii Europejskiej. Co więcej kraje takie jak	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania

			Stany Zjednoczone zaoferowały fundusz refundacyjny dla operatorów regionalnych, którego nie sposób znaleźć w ustawie. Zwracamy na okres 2028 wskazany w Wielkiej Brytanii i mając na uwadze okres amortyzacji sprzętu telekomunikacyjnego w Polsce, **wnosimy o zmianę na 2030** tzn. 10 lat.	poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący

				w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.
412.	Home.pl	Art. 66a-c	Nowelizacja przyzna Kolegium do spraw cyberbezpieczeństwa (organ opiniodawczo-doradczy przy Radzie Ministrów) nową kompetencję, jaką będzie możliwość oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Przy sporządzeniu oceny przeprowadza się analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym, oraz prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego. Wniosek o sporządzenie oceny składa członek Kolegium. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania przekazywana jest Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". Skutkiem oceny określającej wysokie ryzyko korzystania ze sprzętu lub oprogramowania będzie zakaz wprowadzenia do użytkowania takiego sprzętu lub oprogramowania. Z kolei dotychczas używany sprzęt i oprogramowanie ocenione jako wysoce ryzykowne - będą musiały zostać wycofane z użycia przez podmioty z nich korzystające w ciągu 5 lat od ogłoszenia komunikatu o ocenie. W przypadku operatorów usług kluczowych nie stosujących się do powyższych obowiązków kara wynosi do 3% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			Uwagi w ramach konsultacji: - do art. 66a ust. 1: nowelizacja nie zawiera definicji „sprzętu lub oprogramowania”, co powoduje brak pewności co do grona adresatów przepisu, należy zasugerować sprecyzowanie tego pojęcia w nowelizacji; - do art. 66a: nowelizacja nie zakłada udziału dostawcy w toku postępowania poprzedzającego wydanie oceny, nie wskazuje również czy w postępowaniu znajdują zastosowanie przepisy kodeksu postępowania administracyjnego; należy zasugerować uzupełnienie nowelizacji w tym zakresie; - do art. 66a ust. 8: dostawca sprzętu lub oprogramowania którego dotyczy ocena może odwołać się od oceny do Kolegium - w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymuje działań związanych z ograniczeniami prowadzenia działalności dostawcy w zakresie dot. sprzętu lub oprogramowanie podlegającego ocenie; nie ma również możliwości dalszego zaskarżenia decyzji do sądu administracyjnego; należy zasugerować odstąpienie od natychmiastowej wykonalności oceny ewent. wprowadzenie rekompensat dla dostawców z powodu ograniczenia w obrocie sprzętem/oprogramowaniem, jeśli na skutek odwołania od oceny, Kolegium przywróci możliwość ich swobodnej sprzedaży; należy zasugerować wprowadzenie trybu odwoławczego od orzeczenia Kolegium dot. oceny;	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą

				musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
413.	IAB Polska	Art. 66a 66b 66c	Projektowane artykuły 66a, 66b i 66c ustawy o KSC (art. 1 ust. 29 i n. Projektu) przewidują, że Kolegium do spraw cyberbezpieczeństwa nabędzie nową kompetencję dotyczącą oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Wynik powyższego postępowania będzie ogłaszany w Monitorze Polskim. Tylko dostawcy z oceną wysokiego ryzyka będą mieli legitymację do złożenia odwołania, które będzie rozpatrywane ponownie przez Kolegium (projektowany art. 66a ust 8 ustawy o KSC). W przypadku uzyskania oceny ryzyka określającej wysokie lub umiarkowane ryzyko dostawca sprzętu lub oprogramowania, będzie podlegał sankcjom przewidzianym w projektowanym art. 66b ustawy o KSC. Należy również podkreślić, że sankcja za uzyskanie wysokiej oceny ryzyka jest równoznaczna z zakazem wprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania oraz koniecznością ich wycofania z rynku w ciągu 5 lat. Powyższa sankcja w ocenie konstytucjonalistów wydaje się być sprzeczna z zasadą niedziałania prawa wstecz.	**Uwaga częściowo uwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za

			Dodatkowo, zgodnie z art. 66c projektu ustawy o KSC, Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Z projektowanych art. 66b i 66c wynika, że de facto przedsiębiorcy (w tym dostawy i operatorzy) w wyniku oceny Kolegium będą na przykład musieli wycofać się z już prowadzonych inwestycji, które planowane są często w trybie długofalowym. W praktyce może to po prostu oznaczać zakaz prowadzenia działalności gospodarczej dla konkretnego przedsiębiorcy, co w sposób oczywisty zaburza cały system konkurencyjności na rynku podobnych usług czy towarów. W tym miejscu należy również wskazać, że decyzje Kolegium dotyczące dostawców sprzętu i oprogramowania dotykają wszystkie podmioty krajowego systemu cyberbezpieczeństwa. Decyzje dla konkretnych dostawców są wydawane dla poszczególnych obszarów, a co za tym idzie - takie decyzje mogą być wydane nie tylko dla usług telekomunikacyjnych, ale również dla usług komunikacji elektronicznej – co wynika z przyjęcia przez ustawodawcę w nowelizacji wspólnego pojęcia stanowiącego, że usługi o różnym charakterze i przeznaczeniu są traktowane jak usługi „jednego rodzaju”, Niesie to za sobą zagrożenie, że dostawcy usług komunikacji elektronicznej świadczący usługi w zakresie np. czatów albo poczty elektronicznej będą tak samo traktowani jak dostawcy usług telekomunikacyjnych. W konsekwencji może to oznaczać, że serwery danego producenta używane również do świadczenia usługi komunikacji interpersonalnej muszą zostać na mocy decyzji Kolegium wymienione w ciągu 5 lat, co pociągnie za	wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę

			sobą istotne nakłady pieniężne dla każdego podmiotu zaangażowanego lub pośredniczącego w dostawie takiej usługi, a w konsekwencji wpłynie również na konsumenta. Wzrost ceny takiej usługi wobec użytkownika końcowego może oznaczać, że korzystanie z niej przestanie być dla niego opłacalne i doprowadzi tym samym do wyeliminowania usługi z rynku. Dla średnich i małych przedsiębiorców może to oznaczać koniec prowadzonej działalności, a dla społeczeństwa obniżenie dostępności nowoczesnych usług czy nawet wzrost wykluczenia cyfrowego. Kolejną konsekwencją przyjęcia regulacji pozwalającej na wydawanie dyskrecjonalnych decyzji przez Kolegium może być również wycofanie się lub ograniczenie zaangażowania inwestorów zagranicznych z ryku krajowego przez wzgląd na brak pewności co do otoczenia inwestycyjnego Polski. Ponadto konsekwencje przewidziane przez projekt nie kończą się jednak tylko na powyższym zakresie, ponieważ projekt przewiduje również zmiany w ramach Prawa zamówień publicznych. Jak **wskazują konstytucjonaliści powyższe regulacje budzą uzasadnione wątpliwości z perspektywy podstawowych zasad konstytucyjnych**, takich jak niedziałanie prawa wstecz (art. 2 Konstytucji), zasady wolności działalności gospodarczej (art. 20 i 22 Konstytucji) oraz zasady równości wobec prawa i zakazu dyskryminacji (art. 32 Konstytucji). Szczególne zastrzeżenia budzą poniższe kwestie: • Opisana procedura dokonywania oceny przez Kolegium cechuje się jednostronnością, uznaniowością i subiektywnością;	wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. Zrezygnowano z planów wycofania sprzętu lub oprogramowania.

			• Kryteria oceny w zakresie omawianego postępowania są nieprecyzyjne, co rodzi niebezpodstawne obawy o zachowanie w ramach postępowania zasady niedyskryminacji; • Kolegium prowadzi postępowanie bez udziału stron, a o jego rezultacie podmiot dowiaduje się z Monitora Polskiego; • Zasadność odwołania budzi również organ je rozpatrujący tj. to samo Kolegium, które dokonało oceny; • Ponadto uprawnienie do odwołania się od oceny dokonanej przez Kolegium przysługuje tylko i wyłącznie przedsiębiorcy, który uzyskał wysoką ocenę, co stanowi istotne pokrzywdzenie interesów pozostałych podmiotów z ocenami niższymi. Na marginesie warto również zwrócić uwagę, że w przypadku wystąpienia nowych okoliczności, mogących mieć wpływ na ocenę ryzyka dostawcy sprzętu lub oprogramowania, tylko członek Kolegium może złożyć wniosek o zmianę oceny przez Kolegium. Zatem, również na tym etapie zostały wykluczone jakiekolwiek działania ze strony dostawcy sprzętu lub oprogramowania, będącego przedmiotem uprzedniej oceny ze strony Kolegium. W ocenie IAB Polska konieczne jest dokonanie następujących zmian w ramach przedmiotowej procedury. W pierwszej kolejności, kryteria które są brane pod uwagę w czasie postępowania powinny zostać zrewidowane i skonkretyzowane. Obecne ich brzmienie pozostawia zbyt wiele miejsca na subiektywne podejście Kolegium. W dalszym zakresie niezbędne jest zapewnienie dostawcom sprzętu lub oprogramowania czynnego udziału w zakresie całego postępowania oraz na etapie	

			po jego zakończeniu (wspomniana powyżej zmiana okoliczności). Kolejnym postulatem jest zmiana charakteru wydawanej decyzji, która powinna podlegać kontroli instancyjnej i weryfikacji sądowej. IAB Polska postuluje również modyfikację zasad publikacji oceny w Monitorze Polskim, która powinna być uzależniona od uprawomocnienia się decyzji Kolegium. Na zakończenie tej części, należy również podkreślić, że jedynie ostateczna decyzja administracyjna w zakresie oceny Kolegium, powinna być kwalifikowana jako przesłanka wykluczenia z postępowania toczącego się w trybie Prawa zamówień publicznych	
414.	PIIT	67 ust 4 pkt 5	**4. <u>Art. 2 pkt 30 – art. 67a ust. 4 pkt 5</u>** W obecnym brzmieniu projektu ustawy ostrzeżenia i polecenia zabezpieczające mogą dotyczyć kwalifikowanych dostawców usług zaufania, o którym mowa w art. 3 pkt 20 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.), zwanego dalej „eIDAS". W pierwszej kolejności należy wyjść od definicja pojęcia „usługa zaufania", za którą zgodnie z art. 3 pkt 16 eIDAS uważa się: „usługa zaufania" oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą: a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub	**Uwaga częściowo uwzględniona** Do katalogu podmiotów, wobec których może być skierowane ostrzeżenie lub polecenie zabezpieczające zostaną dodani niekwalifikowani dostawcy usług zaufania.

			b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami. Z kolei za kwalifikowanego dostawcę usług zaufania zgodnie z art. 3 pkt 20 eIDAS należy uznać dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru. Natomiast dostawca usług zaufania (art. 3 pkt 19 eIDAS) to osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania. W praktyce obrotu gospodarczego różnica pomiędzy dostawcą usług zaufania, a kwalifikowanym dostawcą usług zaufania sprowadza się w do wpisu na listę kwalifikowanych dostawców usług zaufania, bowiem po względem skutków prawnych przykładowo w kontekście podpisu elektronicznego, który może być już wydawany przez każdego dostawcę usług zaufania, zgodnie z art. 25 ust. 1 eIDAS nie można odmówić podpisowi elektronicznemu skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych. Tym samym, to już na poziomie Unii Europejskiej wprowadzono przepisy, które w praktyce pod względem skutków prawnych zrównują podpis elektroniczny lub zaawansowany podpis elektroniczny na równi z kwalifikowanym podpisem elektronicznym. Od strony technicznej należy zwrócić uwagę na to, że zarówno podpis elektroniczny, zawansowany podpis elektroniczny i kwalifikowany podpis elektroniczny zapewniają integralność danych i	

			umożliwiają identyfikację osoby, która złożyła dane oświadczenie woli. W naszej ocenie do ujętego w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych nowego art. 67a ust. 4 pkt 5, który miałby pojawić się w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, do katalogu podmiotów, które miałyby się stosować do ostrzeżeń i poleceń zabezpieczających, należy włączyć wszelkie osoby lub podmioty wydające środki identyfikacji elektronicznej. Zgodnie art. 3 pkt 2 eIDAS środek identyfikacji elektronicznej oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online. Usługi identyfikacji elektronicznej umożliwiają identyfikację danej osoby fizycznej, oraz co do zasady umożliwia udostępnienie danych osobowych danej osoby fizycznej odbiorcy (tzw. klientowi) tych danych, na których przekazanie osoba fizyczna wyraziła zgodę. Jak wynika z przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) dane osobowe są na poziomie unijnym objęte szczególną ochroną prawną, a podmioty, które są administratorami danych osobowych lub przetwarzają takiej dane na polecenie administratora, z mocy powszechnie obowiązującego prawa muszą stosować środki techniczne na określonymi przepisami poziomie, które w głównej mierze mają zabezpieczyć dane osobowe przed ich ujawnieniem osobom lub podmiotom do tego nieuprawnionym, jak również administrator lub podmiot	

			przetwarzający musi rejestrować wszystkie osoby dopuszczone do przetwarzania danych w jego imieniu. Z tej przyczyny widzimy konieczność objęcia podmiotów świadczących usługi wydawania środków identyfikacji elektronicznej obowiązkiem stosowania się do ostrzeżeń i poleceń zabezpieczających. **<u>Propozycja zmiany przepisu</u>** Art. 2 pkt 30 – art. 67a ust. 4 pkt 5: „4. Ostrzeżenie i polecenie zabezpieczające może dotyczyć: (..) 5) dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.) oraz osoby lub podmioty wydające środki identyfikacji elektronicznej w rozumieniu art. 3 pkt 2 wymienionego rozporządzenia.”	
415.	KIGEIT	art. 67a	*„Art. 67a. 1. Pełnomocnik może wydać:* *1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego,* *2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego* *– po ~~zatwierdzeniu~~ wyrażeniu opinii przez Kolegium.* *~~2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium.~~*	**Wyjaśnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73

			~~*Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu.*~~ *8. W przypadku ~~odmowy zatwierdzenia przez~~ negatywnej opinii Kolegium Pełnomocnik ~~odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje~~ wydaje inne ostrzeżenie lub polecenie zabezpieczające.* **Uzasadnienie:** Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. Zastosowanie znajdzie więc przepis art. 106 k.p.a., który reguluje współdziałanie organów	zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest

				np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
416.	Polska Izba Handlu	Art. 67a	**Ostrzeżenia i polecenia zabezpieczające -** brak odniesienia do postępowania administracyjnego w stosunku do czynności podejmowanych przez Pełnomocnika **Propozycja:** Po ustępie 8 dodać ustęp 9*:* *"Postępowanie przed pełnomocnikiem toczy się w oparciu o przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ostrzeżenie ma formę decyzji administracyjnej."* **Uzasadnienie**	**Wyjasnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w

			Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające. Powinno być wskazane w oparciu o jakie przepisy toczy się postępowanie przed Pełnomocnikiem. W szczególności, że zgodnie z art. 67a ust. 2 Projektu „*ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu*". Konsekwencją stosowania przepisów k.p.a. będzie zastosowanie art. 106 k.p.a., który reguluje współdziałanie organów. Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. *Ostrzeżenie wydaje się w formie decyzji administracyjnej.* Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie", jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania" do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia.	formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia

				incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
417.	PIIT	Art. 67a-67c	**3. <u>Art. 67a – ostrzeżenie i polecenie zabezpieczające</u>** Drugą, jeszcze bardziej interwencyjną metodą działania mogącą skutkować wykluczeniem określonych dostawców są przewidziane w projekcie ustawy ostrzeżenia oraz polecenia zabezpieczające. Takie instrumenty Pełnomocnik może wydawać po analizie i współpracując z Zespołem (*CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach*	**Uwaga częściowo przyjęta** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie

			CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa.). Konsultacje z podmiotami, których ostrzeżenie lub polecenie może dotyczyć, są fakultatywne. Środki te podlegają zatwierdzeniu Kolegium. Stosowanie rozwiązań wynikających z ostrzeżeń i poleceń zabezpieczających może wiązać się ze skutkami na poziomie umów cywilnoprawnych oraz potencjalnej odpowiedzialności odszkodowawczej. W związku z tym należy wprowadzić wyraźne przepisy zwalniające podmioty zobowiązane z jakiejkolwiek odpowiedzialności cywilnoprawnej wobec stron trzecich, które mogą wysuwać roszczenia związane ze skutkami zastosowania ostrzeżeń lub poleceń zabezpieczejących. **I.** **1.1. Art. 67b ust. 1 pkt 3 oraz ust. 3 - ostrzeżenie** Instytucja wydawania ostrzeżeń, jako taka może być uznana za zasadną. Może ona stanowić istotną wytyczną dla podmiotów związanych z cyberprzestrzenią do podejmowania określonych działań. W zakresie podmiotów publicznych rozwiązanie takie może być nawet obligatoryjne. W przypadku jednak podmiotów prywatnych zaproponowany zakres oczekiwanych zachowań, jakie takie podmioty miałyby podejmować jest dalece nieproporcjonalne i stanowi de facto mechanizm zewnętrznego sterowania działalnością przedsiębiorstw przez Pełnomocnika. Potencjalnie zbyt lekkie, ostrożnościowe jedynie korzystanie z tego środka może prowadzić do bardzo wysokich obciążeń przedsiębiorców oraz konieczności podejmowania ogromnego wysiłku organizacyjnego i finansowego. W skrajnych przypadkach może prowadzić do faktycznego zamknięcia działalności, np. w	podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk

			przypadku zakazu stosowania określonego sprzętu (podczas gdy tego mają co do zasady przecież dotyczyć oceny Kolegium) bez jakichkolwiek okresów przejściowych. Wydaje się również, że Pełnomocnik nie będzie też posiadał odpowiedniej wiedzy, aby nakazywać (a nie podpowiadać lub rekomendować) jakie poprawki czy konfigurację sprzętu należy zastosować w danym przypadku. Ponadto rozwiązania takie jak szacowanie ryzyka, czy przegląd planów są działaniami bardzo czasochłonnymi i kosztownymi, które w przypadku nawet realnego i bliskiego ryzyka nie stanowią bezpośredniej odpowiedzi i reakcji na zagrożenie. Dodatkowo zwracamy uwagę, iż nakaz wprowadzenia reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL jest technicznie niemożliwy do realizacji przez przedsiębiorców telekomunikacyjnych. Działanie takie jest możliwe do realizacji przez administratorów sieci niepublicznych/prywatnych, zarządzających dostępem użytkowników tych sieci do sieci Internet. Przepisy dot. ostrzeżeń oraz poleceń zabezpieczających należy również zmodyfikować w sposób wskazujący, że mogą one dotyczyć wyłączenie sprzętu, oprogramowania lub usług podmiotów, których może dotyczyć lub których dotyczy incydent krytyczny. **Postulaty:** o Art. 67b ust. 1 pkt 3 należy usunąć lub zmodyfikować tak, aby w zakresie, w jakim ma dotyczyć przedsiębiorców był traktowany, jako faktyczne ostrzeżenie i wskazanie	związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

			możliwości wyboru ścieżek działania, a nie „polecenie”, „nakaz”, „zakaz”. o W przypadku utrzymania formy nakazowej, w której rozstrzygnięcie stanowi o prawach i obowiązkach konkretnego podmiotu ostrzeżenie powinno być wydawane w drodze decyzji administracyjnej, która jest zaskarżalna w normalnym trybie administracyjnym i sądowym. Wydanie go w formie „Komunikatu” zamyka jego adresatom możliwość ścieżki odwoławczej. Rolą wydającego tak ważne rozstrzygnięcia musi być ustalenie adresatów i ocena skutków. o Okres, na jaki może być wydane ostrzeżenie musi być ściśle skorelowany z zagrożeniem. Proponowany termin 2 lat jest zupełnie abstrakcyjny i wskazuje na zamiar stosowania ostrzeżeń, w sposób oderwany od faktycznych zagrożeń. Okres, jaki ostrzeżenie powinno obowiązywać to maksymalnie 10 dni, z możliwością przedłużenia o ile zagrożenie nie minęło. o Ostrzeżenia nie mogą być również stosowane do rozwiązywania kwestii oceny dostawców, które powinny być procedowane ścieżką oceny ryzyka właściwą dla Kolegium. o Konsultacje z podmiotem objętym decyzją powinny być obligatoryjne. o Z uwagi na postulowaną zmianę charakteru „ostrzeżeń” należy rozważyć przeniesienie tego obowiązku na właściwe CSiRT, które zresztą już dzisiaj powinny podobne działania realizować. o W przypadku utrzymania charakteru ostrzeżeń należy je wprowadzać w drodze decyzji administracyjnej.	

			○ W przypadku utrzymania tego narzędzia, Pełnomocnik powinien być każdorazowo zobowiązany do zwrotu kosztów i ewentualnych strat związanych z wydaniem ostrzeżenia. ○ W art. 67a ust. 3 należy dodać pkt. 6 o następującej treści „6) ocenę możliwości technicznych wdrożenia ostrzeżenia oraz polecenia zabezpieczającego;" ○ W art. 67b ust. 3 po punktach 1 – 7 dodać „- o ile jest to techniczne możliwe." **1.2. Art. 67c – polecenie zabezpieczające** Polecenie zabezpieczające może być stosowane w przypadku wystąpienia incydentu krytycznego i przewiduje jeszcze dalej idące środki niż w przypadku ostrzeżenia. **Postulaty:** ○ Art. 67c ust. 4 należy usunąć lub zmodyfikować tak, aby w zakresie, w jakim ma dotyczyć przedsiębiorców był traktowany, jako określenie możliwych ścieżek działania, a nie „polecenie", „nakaz", „zakaz". ○ W przypadku utrzymania tego narzędzia, Pełnomocnik powinien być każdorazowo zobowiązany do zwrotu kosztów i ewentualnych strat związanych z wydaniem ostrzeżenia. ○ Okres, na jaki może być wydane polecenie musi być ściśle skorelowany z zagrożeniem. Proponowany termin 2 lat jest zdecydowanie zbyt długi. Polecenie może być	

			wydawane wyłącznie na okres obsługi incydentu krytycznego. o Ostrzeżenia nie mogą być również stosowane do rozwiązywania kwestii oceny dostawców, które powinny być procedowane ścieżką oceny ryzyka właściwą dla Kolegium. o Konsultacje z podmiotem objętym decyzją powinny być obligatoryjne.	
418.	SmartWeb Media	Art. 67a ust.1	Z punktu widzenia poprawności legislacyjnej, należałoby również doprecyzować, że uprawnienia Pełnomocnika, o których mowa w projektowanym art. 67a ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, tj. wydawanie ostrzeżeń i poleceń zabezpieczających, winny być wydawane w formie decyzji administracyjnej, oraz podlegać pod reżim odwoławczy wyznaczony przepisami k.p.a.	**Wyjaśnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również

				zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na

				Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
419.	Narodowy Bank Polski	art. 67a ust. 4 pkt 1	Zmianę brzmienia projektowanego art. 67a ust. 4 pkt 1 na następujące: „1) podmiotów, o których mowa w art. 4 pkt 1-8 oraz pkt 10-16;”.	**Uwaga nieuwzględniona** Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych.
420.	Narodowy Bank Polski	art. 67a ust. 4 pkt 6	Narodowego Banku Polskiego jedynie w zakresie w jakim nie wywiera wpływu na realizację zadań NBP. Po ogłoszeniu komunikatu, o którym mowa w ust. 6, NBP przekazuje Pełnomocnikowi informację o ewentualnym ograniczeniu stosowania wydanych ostrzeżeń i poleceń zabezpieczających.”.	**Uwaga nieuwzględniona** Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych.
421.	Fundacja Bezpieczna Cyberprzestrzeń	art. 67a ust. 8	po ust. 8 należy dodać ust. 9 lub inny przepis, w którym podmiot, któremu zostało wydane polecenie zabezpieczające może wystąpić o zwrot poniesionych kosztów, w przypadku odmowy zatwierdzenia tego polecenia przez Kolegium i odwołania polecenia zabezpieczającego w części lub w całości, o czym mowa w art. 67a ust. 8.	**Wyjaśnienie** Uwaga jest bezprzedmiotowa, ponieważ według nowej wersji projektu Kolegium nie będzie zatwierdzać polecenia zabezpieczającego.
422.	SayF	Art. 67 a i b	Nowo wprowadzone artykuły nie określają na podstawie jakich kryteriów pełnomocnik wydaje ostrzeżenia i polecenia zabezpieczające.	**Wyjaśnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane

				w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy,

				czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
423.	Nanocoder	Art. 67 a i c	Art. 67a i 67c również powinny zostać objęte poprawkami, z uwagi na fakt, że zarówno ostrzeżenie jak i polecenie zabezpieczenia powinny mieć formę decyzji administracyjnej, a	**Wyjaśnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik.

			polecenie zabezpieczające nie powinno być wydane z rygorem natychmiastowej wykonalności. Wynika to z faktu, iż działania Pełnomocnika powinny podlegać Kodeksowi Postępowania Administracyjnego, tym samym ostrzeżenie i polecenie zabezpieczenia powinno być przyjęte w formie decyzji administracyjnej. W niniejszym projekcie występuje kilka wyjątków, tj. sytuacji, w których polecenie zabezpieczające wdrożone ma zostać natychmiast. Będzie to miało nieodwracalne skutki, tego rodzaju zabezpieczenia powinny być pozbawione rygoru natychmiastowej wykonalności.	Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w

				ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
424.	Home.pl	Art. 67 a-c	W celu zapobiegania i zwiększenia skuteczności reagowania na incydenty krytyczne nowelizacja zakłada przyznanie	**Uwaga częściowo uwzględniona**

			Pełnomocnikowi Rządu do Spraw Cyberbezpieczeństwa nowej kompetencji: - możliwość wydawania ostrzeżeń i poleceń zabezpieczających (m. in. wobec operatora usług kluczowych). Ostrzeżenie stosuje się w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, które może skutkować wystąpieniem incydentu krytycznego i nie jest decyzją administracyjną. W jego ramach wskazuje się rodzaje podmiotów, których dotyczy, określone zachowanie, które zmniejszy ryzyko, datę wejścia w życie i okres obowiązywania, a także uzasadnienie. Wydaje się je na okres nie dłuższy niż 2 lata, choć Pełnomocnik będzie mógł jednokrotnie przedłużyć jego okres obowiązywania nie dłużej niż o kolejne dwa lata. Jeżeli przemawia za tym interes publiczny, informacja o zastosowanym ostrzeżeniu może być udostępniona za pomocą środków masowego przekazu. W ramach ostrzeżenia można podmiotowi ~~nakazać zakaz~~ zakazać korzystania z określonego sprzętu lub oprogramowania oraz nakazać wprowadzenie reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL. Polecenie zabezpieczające jest decyzją administracyjną, która ma rygor natychmiastowej wykonalności. Stosuje je Pełnomocnik w razie wystąpienia incydentu krytycznego. Zawiera wskazanie podmiotów, których dotyczy, wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu, datę wejścia w życie i uzasadnienie. W razie nie zastosowania się do polecenia zabezpieczającego operator usługi kluczowej podlega administracyjnej karze pieniężnej. Pełnomocnik ogłasza w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” komunikaty o	Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc.

			wydanych i odwołanych ostrzeżeniach i poleceniach zabezpieczających. **Uwagi w ramach konsultacji:** **-** do art. 67a ust. 1 pkt 1 (Ostrzeżenie): Procedura wydania ostrzeżenia jest odformalizowana i nie zapewnia dostawcom udziału w postępowaniu dot. wydania ostrzeżenia (nowelizacja nie zakłada obligatoryjnego udziału dostawcy w ramach postępowania przed wydaniem ostrzeżenia – a jedynie fakultatywny decyduje o tym organ prowadzący postępowanie Pełnomocnik – nowy art. 67a ust. w przypadku ostrzeżenia nowelizacja nie przewiduje trybu odwoławczego; jednocześnie przy orzekaniu o wydaniu ostrzeżenia organ posiada duży zakres uznaniowości; w konsekwencji – może dojść do istotnych ograniczeń działalności dostawcy na znaczny okres czasu bez możliwości kontrolowania prawidłowości działań organu lub sprzeciwienia się tym działaniom; należy w związku z tym zasugerować: dodanie do nowelizacji zapisów precyzujących przesłanki wydana ostrzeżenia, aby ograniczyć uznaniowość organu, gwarantujących dostawcom udział w postępowaniu o wydanie ostrzeżenia, zapewnienie możliwości odwołania od ostrzeżenia, zapewnienie rekompensat za szkody spowodowane wydaniem ostrzeżenia. - do art. 67a ust. 1 pkt 2 (Polecenia): ograniczenia związane poleceniem mogą zostać wprowadzone niezwłocznie, a ich skutki mogą znacznie ingerować w prowadzenie działalności gospodarczej dostawcy; rozstrzygniecie organu – choć wydawane w formie decyzji adm. i podlegające zaskarżeniu, cechuje się znaczną uznaniowością; decyzja w przedmiocie wydania polecenia jest natychmiast wykonalna; należy w związku z tym zasugerować: dodanie do nowelizacji zapisów precyzujących przesłanki wydana polecenia, aby	Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

			ograniczyć uznaniowość organu, zapewnienie rekompensat za szkody spowodowane wydaniem polecenia.	
425.	Unia Metropolii Polskich	Art. 67c 1	Pelnomocnik ds. cyberbezpieczeństwa z mocy ustawy będzie mógł wydawać bezpośrednie nakazy zabezpieczające. W drodze tego nakazu będzie można odciąć konkretne zasoby, IP albo konkretne serwery od polskiego internetu. Intencją jest zapewnienie nam bezpieczeństwa. Jednak kryteria, które są zawarte w tym projekcie ustawy, są poza jakąkolwiek kontrolą sądową i tak szerokie, że właściwie mogą służyć do dowolnego celu. W projekcie wskazuje się, że „polecenia zabezpieczające" będą wydawane tylko w przypadku wystąpienia „incydentów krytycznych". Tylko, że instytucja państwa sama będzie decydowała o tym, co stanowi taki incydent, oznacza to możliwość niemal nieograniczonego cenzurowania pojawiających się w Internecie treści, które zostaną uznane za niewygodne. **Propozycja:** wykreślenie z projektu ustawy możliwości wydawania tzw. poleceń zabezpieczających Omawiany przepis może stanowi zagrożenie dla wolności słowa.	**Uwaga nieuwzględniona** Projektowane przepisy dot. ostrzeżenia i polecenia zabezpieczającego nie mają na celu ograniczenie wolności słowa i dostępu do internetu. . Ich stosowanie jest ograniczone tylko do niektórych grup podmiotów z sektorów gospodarki kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa m.in. do operatorów usług kluczowych, administracji publicznej, czy przedsiębiorców telekomunikacyjnych. Co więcej, środki te mogą być aktywowane w sytuacji zagrażającej wystąpieniu incydentu krytycznego7 (ostrzeżenie) lub w trakcie jego trwania, w związku z potrzebą zapewnienia koordynacji i odpowiednio szybkiej reakcji na zażeganie sytuacji kryzysowej wywołanej cyberatakiem (polecenie zabezpieczające).
426.	Mobile Logic	Art. 67c	Ponadto nakładany w art. 67c rygor natychmiastowej wykonalności dla zabezpieczenia powinien zostać usunięty. Tego typu działanie będzie miało nieodwracalne skutki i w związku z tym jest nie do przyjęcia.	**Uwaga nieuwzględniona** Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. Polecenie zabezpieczające ma na celu ograniczyć skutki incydentu krytycznego, który może zagrażać obywatelom, państwu, gospodarce. Dlatego rygor natychmiastowej wykonalności polecenia zabezpieczającego jest niezbędny.

427.	Polska Izba Handlu	Art. 67c	**Projekt przepisu:** brak odniesienia do postępowania administracyjnego w odniesieniu do „ostrzeżenia” **Propozycja:** słowo „ostrzeżenie” dodane do Art. 67c punkt 1. *"Pełnomocnik wydaje ostrzeżenie i polecenia zabezpieczające w formie decyzji administracyjnej".* **Uzasadnienie** Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. *Ostrzeżenie wydaje się w formie decyzji administracyjnej.* Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie”, jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania” do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia	**Wyjaśnienie** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc.

				Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.

428.	Polska Izba Handlu	Art. 67c ust. 1	**Propozycja**: wykreślić rygor natychmiastowej wykonalności decyzji **Uzasadnienie** Z uwagi na nieodwracalne skutki wykonania polecenie zabezpieczającego z rygorem natychmiastowej wykonalności, powinien być ten rygor usunięty. Przykładowo w Prawie telekomunikacyjnym, zgodnie z art. 206 ust. 2aa, decyzje regulacyjne podlegają natychmiastowemu wykonaniu, ale z wyjątkiem decyzji w sprawie nałożenia kar, właśnie z uwagi na ich nieodwracalne skutki	**Uwaga nieuwzględniona** Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu. Polecenie zabezpieczające ma na celu ograniczyć skutki incydentu krytycznego, który może zagrażać obywatelom, państwu, gospodarce. Dlatego rygor natychmiastowej wykonalności polecenia zabezpieczającego jest niezbędny.
429.	KIGEIT	Art. 67c ust. 1	**Proponowana zmiana:** *"Art. 67c. 1. Pełnomocnik wydaje ostrzeżenie i polecenie zabezpieczające w ~~drodze~~ formie decyzji administracyjnej, od której przysługuje odwołanie albo wniosek o ponowne rozpatrzenie sprawy do ministra właściwego do spraw informatyzacji. ~~Decyzja podlega natychmiastowemu wykonaniu.~~ "* **Uzasadnienie** Zgodnie z art. 67c ust. 1 Projektu: *Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej.* Wprowadza to niejasność w odniesieniu do charakteru ostrzeżenia, które również stanowi decyzję administracyjną. Kluczowy element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie", jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania" do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia. Mając na uwadze, że Pełnomocnikiem może zostać sekretarz stanu lub podsekretarz stanu z każdego ministerstwa, zasadne jest zmodyfikowanie zasady ogólnej odwołania do organu	**Wyjaśnienie** Ostrzeżenie będzie miękkim środkiem, zalecającym działania. Za niedostosowanie się do ostrzeżenia nie będą grozić kary.

			wyższego stopnia. W każdym przypadku organem rozpoznającym sprawę w drugiej instancji winien być minister właściwy do spraw informatyzacji, nawet jeśli Pełnomocnika powołano w innym ministerstwie. Z uwagi na nieodwracalne skutki wykonania polecenia zabezpieczającego z rygorem natychmiastowej wykonalności, powinien być ten rygor usunięty	
430.	Fundacja Bezpieczna Cyberprzestrzeń	art. 67c ust. 2	należy doprecyzować, kiedy kończy się czas koordynacji obsługi incydentu krytycznego, gdyż w przepisach ustawy zmieniającej i zmienianej nie ma obowiązku ogłaszania tego faktu. Należy połączyć ten przepis z przepisem wskazującym w obowiązkach CSIRT poziomu krajowego informowania o zakończeniu koordynacji obsługi incydentu krytycznego	**Uwaga nieuwzględniona** Nie jest możliwe określenie czasu koordynacji incydentu krytycznego. Polecenie zabezpieczające będzie obowiązywać maksymalnie dwa lata.
431.	T-Mobile Polska	Art. 73 pkt 14	***14) ust. 2a wynosi:*** *a) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 1 w wysokości do 3% jego całkowitego rocznego ~~światowego~~ obrotu z poprzedniego roku obrotowego, osiągniętego na obszarze Rzeczypospolitej Polskiej,* *b) w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 2 w wysokości do 1% jego całkowitego rocznego ~~światowego~~ obrotu z poprzedniego roku obrotowego, osiągniętego na obszarze Rzeczypospolitej Polskiej,* **Uzasadnienie:** Dla uniknięcia ewentualnych wątpliwości interpretacyjnych, proponujemy zmianę mającą na celu doprecyzowanie, iż w przypadku międzynarodowych grup telekomunikacyjnych, ewentualna sankcja dotyczy wyłącznie przedsiębiorcę telekomunikacyjnego (operatora) funkcjonującego na obszarze RP, a nie całej międzynarodowej grupy kapitałowej, do której należy przedsiębiorca prowadzący działalność w Polsce.	**Uwaga nieuwzględniona** Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego.

432.	PIIT	Art. 73 ust. 2a	**4. Art. 73 ust. 2a – kary pieniężne** **Postulat:** ○ Zwracamy uwagę na bardzo wysokie potencjalne kary pieniężne związane z naruszeniem określonych przepisów. W naszej ocenie powinny one zostać określone na poziomie zbliżonym do pozostałych kar określonych w ustawie KSC, a w wypadku pozostawienia wartości procentowej nie powinny odnosić się do obrotu na poziomie globalnym, co rodzi zbędne wątpliwości dot. określania podstawy kary dla podmiotów działających i zarejestrowanych w Polsce, ale posiadających międzynarodową strukturę właścicielską.	**Uwaga nieuwzględniona** Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego.
433.	Narodowy Bank Polski	Art. 73 ust. 2a	Z punktu widzenia NBP wątpliwości budzi projektowany art. 73 ust. 2a, który przewiduje nałożenie administracyjnej kary pieniężnej na podmiot krajowego systemu cyberbezpieczeństwa, który nie dostosował się do obowiązków określonych w art. 66b ustawy o KSC. Do kręgu podmiotów objętych sankcjami, zalicza się także Narodowy Bank Polski, na który – w myśl aktualnie projektowanego art. 74 ust. 1a pkt 1 – może zostać nałożona kara pieniężna przez organ nadzorujący. Ze względu na konstytucyjny status Narodowego Banku Polskiego, a także obowiązujące rozwiązania w ustawie o KSC, brak jest organu sprawującego nadzór nad NBP, co oznacza, że przytoczone powyżej przepisy odnoszące się do możliwości nakładania administracyjnej kary pieniężnej na NBP nie będą miały zastosowania. Zasadnym jest zatem wyłączenie NBP	**Uwaga nieuwzględniona** Obowiązek dostosowania się do polecenia zabezpieczającego nie wpływa na konstytucyjną niezależność Narodowego Banku Polskiego. Nie dotyczy jego zadań konstytucyjnych i ustawowych.

			z zakresu podmiotowego omawianych przepisów, tj. projektowanego art. 73 ust. 2a oraz art. 74 ust. 1a pkt 1.	
434.	Związek Banków Polskich	Art. 73 pkt 14	4) ust. 2a wynosi: a)w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 1 w wysokości do 300 000 zł, b)w przypadku podmiotów określonych w art. 4 pkt 1-2a nie stosujących się do art. 66b ust. 2 w wysokości do 100 000 zł, c)w przypadku podmiotów publicznych do 300 000zł". Wysokość kar w tym zakresie jest niewspółmiernie wyższa niż w przypadku innych uchybień. Proponujemy zmianę z % odnoszących się do obrotu firm z sektora prywatnego na konkretne kwoty. Kara wprowadza dotkliwość jednak nie ma aż tak dużej niewspółmierności kary sektora prywatnego w porównaniu z sektorem publicznym.	**Uwaga nieuwzględniona** Kary, których wymiar odnosi się do światowego obrotu, są niezbędne w celu zapewnienia skuteczności przepisów, które mają na celu ochronę bezpieczeństwa narodowego.
435.	Narodowy Bank Polski	Art. 74 ust. 1a pkt 1	Zmianę brzmienia projektowanego art. 74 ust. 1a pkt 1 na następujące: „1) w przypadku podmiotów określonych w art. 4 pkt 7-8 oraz pkt 10-15 – organ nadzorujący"	**Wyjaśnienie** **Przepis został zmieniony**
436.	SayF	Rozdział 14	Brak wskazania kar dla przedsiębiorców komunikacji elektronicznej.	**Uwaga uwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
437.	Związek Przedsiębiorców i	Rozdział 4a	Przedstawiony projekt zakłada wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa zupełnie nowego rozdziału 4a dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej. Pragniemy podkreślić, że analogiczne	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz

	Pracodawców		regulacje znajdują się już w projekcie prawa komunikacji elektronicznej. Istnieje zatem potrzeba przyjęcia jednolitego podejścia i uregulowania obowiązków przedsiębiorców komunikacji elektronicznej w jednym akcie. Część z opisywanych obowiązków podmiotów ma charakter dosyć ogólny (jak choćby „podejmowanie środków technicznych i organizacyjnych zapewniających poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka"). Faktyczna „głębokość" tychże obowiązków zależeć będzie w dużej mierze od wydanych na podstawie nowych przepisów aktów wykonawczych. Szczegółowe parametry tychże obowiązków, takie jak minimalny zakres ww. środków technicznych i organizacyjnych, czy sposób dokumentowania ich, mają być zgodnie z analizowanym projektem opisane w rozporządzeniu ministra właściwego ds. informatyzacji. Minister ten będzie również określał próg incydentu telekomunikacyjnego, którego przekroczenie spowoduje obowiązek zgłoszenia incydentu przez przedsiębiorcę. Należy w tym miejscu podkreślić, że proponowane regulacje wykraczają nieco ponad minimalny poziom obowiązków przewidziany w EKŁE, choćby w zakresie dostawców interpersonalnej komunikacji elektronicznej niewykorzystujących numerów.	przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
438.	KIGEIT	Rozdział 4a	**Propozycja zmiany:** Przeniesienie Rozdziału 4a art. 20a-20f „obowiązki przedsiębiorców komunikacji elektronicznej" do Rozdziału 5 PKE i dokonanie ich ujednolicenia **Uzasadnienie:** Zakres rozdziału 4 a pokrywa się z treścią rozdziału 5 PKE. Istnieje ryzyko powstania wątpliwości interpretacyjnych i trudności w stosowaniu przepisów w praktyce. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych.

				EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
439.	SayF	Rozdział 4a	Pełny obraz obowiązków przedsiębiorcy komunikacji elektronicznej będzie znany po analizie przepisów z zakresu bezpieczeństwa zawartych w KSC oraz w PKE. Proponuje się przeredagować Rozdział 4 w taki sposób, aby obowiązki tam określone związane były wyłącznie z cyberbezpieczeństwem w komunikacji elektronicznej. Regulując sprawy związane z „sytuacjami szczególnego zagrożenie” rozszerza się zakres regulacji o przedmioty nie mające wiele (albo nic) wspólnego z cyberbezpieczeństwem. Na przykład: co wspólnego z cyberbezpieczeństwem ma działanie przedsiębiorcy telekomunikacyjnego po wprowadzeniu stanu nadzwyczajnego?	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne.

				Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
440.	Polska Izba Handlu	Art. 2 pkt 12 projektu Rozdział 4a	**Propozycja zmiany:** Przeniesienie Rozdziału 4a art. 20a-20f „obowiązki przedsiębiorców komunikacji elektronicznej" do Rozdziału 5 PKE i dokonanie ich ujednolicenia. **Uzasadnienie:** Zakres rozdziału 4 a pokrywa się z treścią rozdziału 5 PKE. W przeciwnym wypadku istnieje ryzyko powstania wątpliwości interpretacyjnych i trudności w ich stosowaniu w praktyce. Obowiązki związane z kwestiami cyberbezpieczeństwa podlegają wymogom Art. 13a i 13b dyrektywy 2002/21/WE.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też

				administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
441.	Fundacja Bezpieczna Cyberprzestrzeń	[ustawa zmieniana] art. 8 pkt 2 lit c	proponuje się usunąć ten przepis. Rozciąga on w sposób nieuzasadniony zakres systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej na usługi, które mogą nie być świadczone w sposób elektroniczny oraz które są świadczone przez podmioty zewnętrze, tym samym to w zakresie ich odpowiedzialności powinno być utrzymanie ciągłości ich działania	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.
442.	Fundacja Bezpieczna Cyberprzestrzeń	[ustawa zmieniana] art. 8 pkt 5 lit. c	Proponuje się usunąć ten przepis. Przedmiotowy przepis zawiera się w przepisie w lit. a .	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.
443.	Fundacja Bezpieczna Cyberprzestrzeń	[ustawa zmieniana] art. 11 ust. pkt 1	Proponuje się usunąć ten przepis. Obsługa incydentu zawiera się w szerszym znaczeniowo zarządzaniu incydentem, który jest obowiązkiem z art. 8 pkt 4. Wydaje się, że nie można zarządzać incydentem, nie podejmując jego obsługi lub co najmniej są to pojęcia tożsame (np. FIRST CSIRT Services Framework nie wymienia oddzielnej usługi ani funkcji związanej z obsługą w obszarze zarządzania incydentami wskazując szereg usług, które mogą być utożsamiane z obsługą incydentu np. triage, analizy czy reagowanie).	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.

444.	KIGEIT	Art. 1 pkt 30 Projektu	**Propozycja dodania art. 67d:** *„**Art. 67d.** 1. Postępowanie przed Pełnomocnikiem lub Kolegium toczy się na podstawie przepisów ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego ze zmianami wynikającymi z niniejszej ustawy.”* **Uzasadnienie:** W projektowanych przepisach zostały przewidziane modyfikacje wobec regulacji przewidzianych w KPA, wobec czego zasadne jest potwierdzenie zakresu stosowania przepisów KPA w odniesieniu do postępowań toczących się przed Pełnomocnikiem lub Kolegium	**Wyjaśnienie** Stosowny przepis został dodany w nowelizacji
445.	PKN Orlen	Art. 1 ust. 3 Projektu	Propozycja nadania art. 1 punkt 3) Projektu następującego brzmienia: *„ użyte w art. 4 w pkt 6, w art. 7 w ust. 7 oraz w art. 9 w ust. 2, w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa ”, zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „ CSIRT sektorowy ”. ”* *„użyte w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 15 w ust. 2 w pkt* *3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5, w art. 44, w art. 48 w pkt 1, w art. 49 w ust. 3, w art. 64, w art. 65 w ust. 1 w pkt 2 i* *4, w art. 66 w ust. 7* *oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „ sektorowy* *zespół cyberbezpieczeństwa ”, zastępuje się użytymi w odpowiedniej liczbie i odpowiednim* przypadku wyrazami „ CSIRT sektorowy ” **oraz „CSIRT grupy kapitałowej”. ”**	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.

			1. Wprowadzenie pojęcia *„CSIRT grupy kapitałowej”* ma **zapewnić możliwość ustanowienia CSIRT grupy kapitałowej w ramach krajowego systemu cyberbezpieczeńs twa.** 2. Podział na dwie grupy przepisów wynika z tego, iż zdaniem PKN Orlen obowiązki i prawa wymienione w *art. art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2 oraz w art. 11 w ust. 3 aktualnej Ustawy o KSC* **nie powinny dotyczyć** CSIRT grupy kapitałowej. 3. Jednocześnie uprzejmie zauważamy, że art. 11 ust. 3 Ustawy o KSC już jest zmieniany w treści Projektu w wyniku czego zawarcie odwołania w punkcie Projektu wprowadzającym omawianą zmianę nie ma uzasadnienia.	
446.	PKN Orlen	Art. 4 pkt 16 Projektu	Propozycja zmiany aktualnego art. 4 punkt 16) Ustawy o KSC jak poniżej: *„Podmiot prowadzący SOC. ”* W przypadku przyjęcia zawartego w Projekcie art. 4 punkt 16) Projektu doszłoby do sytuacji, w ramach której SOC stanowiłyby odrębne podmioty krajowego systemu cyberbezpieczeństwa.	**Uwaga nieuwzględniona,** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością

				zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej.
447.	Transition Software	Art. 4 ust. 5 PZP	*Art. 4. Ustawy nie stosuje się do:* *(…)* *5) zamówień lub konkursów:* *a) którym nadano klauzulę zgodnie z przepisami o ochronie informacji niejawnych, lub* *b) jeżeli wymaga tego istotny interes bezpieczeństwa państwa, lub* *c) jeżeli wymaga tego ochrona bezpieczeństwa publicznego, lub* *d) którym muszą towarzyszyć, na podstawie odrębnych przepisów, szczególne środki bezpieczeństwa* *– w zakresie, w jakim ochrona istotnych interesów dotyczących -bezpieczeństwa państwa określonych w lit. a–d nie może zostać zagwarantowana w inny sposób niż udzielenie zamówienia bez zastosowania ustawy;*	**Wyjaśnienie** W ramach projektu zrezygnowano ze zmian w Prawie Zamówień Publicznych.
448.	Transition Software	Art., 131a PZP	*1. (…);* *1a. Przepisy niniejszego rozdziału stosuje się do zamówień dotyczących infrastruktury krytycznej, o której mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.* *2. Przepisy niniejszego rozdziału stosuje się również do zamówień obejmujących równocześnie zamówienia w dziedzinach*	**Wyjaśnienie** W ramach projektu zrezygnowano ze zmian w Prawie Zamówień Publicznych.

			obronności i bezpieczeństwa oraz inne zamówienia, do których zastosowanie mają przepisy ustawy, jeżeli udzielenie jednego zamówienia jest uzasadnione z przyczyn obiektywnych. *3. Ustawy nie stosuje się do zamówień obejmujących równocześnie zamówienia w dziedzinach obronności i bezpieczeństwa oraz zamówienia, co do których wyłączono stosowanie ustawy, jeżeli udzielenie jednego zamówienia jest uzasadnione z przyczyn obiektywnych*	
449.	PKN Orlen	Art. 2 pkt 4a KSC	Propozycja dodania do Ustawy o KSC art. 2 punkt 4a), w myśl którego: *„grupa kapitałowa - rozumie się przez to wszystkich przedsiębiorców, którzy są kontrolowani w sposób bezpośredni lub pośredni przez jednego przedsiębiorcę (w tym również tego przedsiębiorcę), do* którego należy więcej niż jeden operator usługi kluczowej z określonego sektora. ” Wprowadzenie definicji pojęcia ‚grupy kapitałowej” ma zapewnić możliwość wprowadzenia do Ustawy o KSC pojęcia „CSIRT grupy kapitałowej”'	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT (i dodawania definicji grupy kapitałowej). Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.
450.	PKN Orlen	Art. 3 pkt 6a KSC	Propozycja dodania do Ustawy o KSC art. 3 punkt 6a), w myśl którego *„ CSIRT grupy kapitałowej - Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający w **ramach oraz na poziomie grupy kapitałowej** ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa. ”* Wprowadzenie definicji pojęcia *„CSIRT grupy kapitałowej”* ma zapewnić możliwość ustanowienia *„CSIRT grupy kapitałowej”* w ramach krajowego systemu cyberbezpieczeństwa.	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.

451.	PKN Orlen	Art. 4 pkt 6a KSC	Propozycja dodania do Ustawy o KSC art. 4 punkt 6a) jak poniżej:*„ CSIRT grupy kapitałowej”* W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa *„CSIRT grupy kapitałowej”* niezbędne jest uwzględnienie w/w podmiotu w kolejnych przepisach Ustawy o KSC.	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.
452.	PKN Orlen	Obecne przepisy Ustawy o KSC czyli: art. 26 ust. 4., art. 32 ust. 4., art. 34 ust. 1, art. 39 ust. 1 - ust. 3 oraz ust 5 - ust. 9 art. 40 oraz art. 46, **które zawierają pojęcie: „sektorowy zespół cyberbezpieczeństwa”.**	Przepisy projektu zastępują w treści przepisów wymienionych obok pojęcie *„ sektorowy zespół cyberbezpieczeństwa ”* użytymi w odpowiedniej liczbie odpowiednim przypadku pojęciami: *„ CSIRT sektorowy i CSIRT Telco. ”.* 1. Propozycja zastąpienia pojęcia *„ sektorowy zespół cyberbezpieczeństwa ”* użytymi w odpowiedniej liczbie i odpowiednim przypadku pojęciami: *„ CSIRT sektorowy, CSIRT Telco oraz **CSIRT grupy kapitałowej.”*** 2. Ponadto w projektowanych przepisach Projektu (np. art. 46 ust. 2a)) pojęcia „CSIRT sektorowy oraz CSIRT Telco” należy zastąpić użytymi w odpowiedniej liczbie i odpowiednim przypadku: *„ CSIRT sektorowy, CSIRT TELCO oraz CSIRT grupy kapitałowej ”.* W przypadku zawarcia w krajowym systemie cyberbezpieczeństwa *„ CSIRT grupy kapitałowej ”* **niezbędne jest uwzględnienie w/w podmiotu w kolejnych przepisach Ustawy o KSC.**	**Uwaga nieuwzględniona.** Nie jest konieczna tworzenie nowego rodzaju CSIRT. Zadania doskonale wypełni podmiot w ramach grupy kapitałowej świadczący usługę SOC dla operatorów usługi kluczowej w ramach grupy kapitałowej.

453.	Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o.	OSR - Katalog Opisu usług	**Szacowane terminy dla poszczególnych usług** Prosimy o rozważenie podziału szacowanych terminów realizacji poszczególnych usług z Katalogu Usług cyberbezpieczeństwa wg np. kryterium wielkości firmy/ilości zatrudnionych pracowników. Z naszych doświadczeń wynika, że usługa np. analizy podatności - może być znacznie dłuższa niż proponowane 4-8 dni czy też usługa podnoszenia świadomości o zagrożeniach, przy ponad 10 tys. Pracownikach, nie jest w stanie być zrealizowana w zaproponowanym terminie 8-15 roboczodni, chyba że założenia terminowe dotyczyłyby tylko konkretnych działań w ramach tych usług.	**Uwaga nieuwzględniona,** terminy podane w OSR są prawidłowe.
454.	KIGEIT	OSR	**Brak przeprowadzenia oceny skutków regulacji** Zmiany zawarte w projekcie nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa mogą wiązać się z daleko idącymi negatywnymi skutkami społecznymi (likwidacja miejsc pracy, obniżenie dostępności nowoczesnych usług, wzrost wykluczenia cyfrowego), gospodarczymi (obniżenie konkurencyjności polskiej gospodarki, spadek zaufania inwestorów oraz wzmocnienie oligopoli) i politycznymi (uderza w harmonizację europejską oraz relacje międzynarodowe z krajami dotkniętymi sankcjami). Wynika to z konieczności wymiany sprzętu oraz aplikacji, które są obecnie w użyciu, na alternatywne, pochodzące od innych dostawców. Tymczasem w uzasadnieniu Projektu na s. 33 poświęconym skutkom gospodarczym i finansowym w ogóle nie ma o tym mowy. Wspomina się tylko o kosztach związanych z powoływaniem nowych struktur administracyjnych z zakresu cyberbezpieczeństwa (s. 49-52 uzasadnienia Projektu). Jest to istotne naruszenie procesu legislacyjnego (§ 28 Regulamin Pracy Rady Ministrów, t.j. M.P. z 2016 r. poz. 1006) świadczące o wadliwym charakterze Projektu.	**Uwaga częściowo uwzględniona, OSR zostanie uzupełniony.**

455.	KIGEIT	OSR	**Brak ocen skutków dotyczących projektu ustawy i powiązanych rodzajów ryzyka** 1) Projektodawca nie przeprowadził kompleksowej, wystarczającej i szczegółowej oceny skutków przed konsultacjami publicznymi w sprawie projektu prawa. 2) Projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa). 3) Operatorzy, dostawcy, stowarzyszenia branżowe ICT oraz odpowiednie zainteresowane strony nie są w stanie ocenić wpływu projektu ustawy w wyznaczonym terminie. 4) Termin wyznaczony na konsultacje publiczne nie jest zgodny z rygorem przejrzystości procesu decyzyjnego w administracji publicznej ze względu na znaczące skutki projektu ustawy, a także bez wstępnych konsultacji z zainteresowanymi stronami. **Potencjalny wpływ projektu ustawy na dostawców** 1) Kryteria oceny są niejasne, nieprzejrzyste, a zakres oceny jest zbyt szeroki. 2) Kryteria oceny są zbyt polityczne i nie obejmują mechanizmu norm technicznych i certyfikacji, takich jak NESAS i ENISA. 3) Spowoduje to dyskryminację między producentami i naruszenie konstytucyjnego prawa do dostaw towarów w Polsce i zakłócenie konkurencji. **Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych** 1) Obecnie nie ma zbyt wielu dostawców technologii 5G, więc wymagane ogromne zmiany w ramach sieci komórkowych, mogą opóźnić się o 3-5 lat.	**Uwaga częściowo uwzględniona, OSR zostanie uzupełniony.**

			2) Prawo operatorów do wyboru producenta będzie ograniczone. Ministerstwo Obrony Narodowej i Kolegium powinni ustanowić jasne kryteria techniczne i wymogi, do których operatorzy powinni się stosować. W przeciwnym razie naruszy to prawo konkurencji na szczeblu krajowym. Ostateczny wybór dostawcy przez operatorów powinien opierać się na normach techniki i technologii, innowacji, kosztów oraz bezpieczeństwa cybernetycznego. 3) Może dojść do określonych strat aktywów i dodatkowych nieprzewidzianych przez operatorów kosztów (migracji, integracji systemów), które mogą wpłynąć na koszt usług co znajdzie przełożenie w cenach taryf i innych usług. 4) Dla operatorów w Polsce projekt ustawy będzie miał poważne negatywne implikacje i będzie wyrządzał wielką szkodę ich poprzednim inwestycjom i prawom własności. Projekt tego prawa nie daje pewności prawa i zwiększa koszty operacyjne, co jest sprzeczne z warunkami określonymi w decyzjach administracyjnych dotyczących prowadzenia działalności. **Potencjalny wpływ projektu ustawy na konkurencję** 1) W Polsce nie ma aż tak wielu dostawców sprzętu do sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to bardzo szkodzić innowacjom w technologii i odroczy digitalizację Polski. Może to też oznaczać wzrost kosztów operatorów. 2) Przesłanki bezpieczeństwa narodowego nie powinno się nadużywać, a wyjątek dotyczący bezpieczeństwa narodowego powinien być stosowany z zachowaniem zasad proporcjonalności, obiektywności, przejrzystości i minimalnej ingerencji.	

			Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową 1) Mogą wystąpić straty w sektorze ICT (potencjalny wzrost cen z powodu braku konkurencji). Straty mogą powstać także w całej gospodarce (lokalne zatrudnienie, zamówienia publiczne, negatywny wpływ na PKB). 2) Projekt ustawy może mieć negatywny wpływ na gotowość podmiotów do składania ofert na spektrum 5G. 3) Ograniczenie operatorów do wyboru dostawcy może odroczyć również uruchomienie sieci 5G, a tym samy opóźni to rozwój Przemysłu 4.0. Może to przełożyć się na brak wykorzystania nowego „skoku technologicznego" (jakim jest Przemysł 4.0) do zbudowania kompetencji w tym obszarze. Szansę taką (jako Polska) już raz udało się wykorzystać budując kompetencje przemysłu elektronicznego w zakresie montażu elektronicznego (przejście z technologii telewizorów CRT na LCD). **Potencjalny wpływ projektu ustawy na postęp technologiczny** 1) Wyłączenie jakiegokolwiek producenta, spowoduje opóźnienie postępu w całym ekosystemie. Polska utraci możliwość skorzystania z dojrzałego ekosystemu 5G innych krajów. 2) Negatywny wpływ na życie i pracę podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, może to ograniczyć wzrost miejsc pracy, który wiązany jest z nową technologią. 3) Projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0 i może opóźnić szansę na stworzenie kompetencji w obszarze „usieciowienia gospodarki" w tym m.in.: urządzeń sieciowych nowej generacji, jak np.: samochodów podłączonych do sieci 5G, maszyn	

			produkcyjnych 5G, różnych urządzeń high-tech w automatyce i sterowaniu, maszyn rolniczych i systemów dla produkcji rolniczej, usług portowych, zdalnej edukacji, sprzętu medycznego, itp. 4) Projekt ustawy nie generuje zachęty dla odbudowy i rozwoju krajowego potencjału technologicznego w obszarze wytwarzania podzespołów elektronicznych (rewitalizacja przemysłu mikroelektronicznego).	
456.	Polska Izba Handlu	OSR	**Brak ocen skutków dotyczących projektu ustawy i powiązanych rodzajów ryzyka ;** 5) Projektodawca nie przeprowadził kompleksowej, wystarczającej i szczegółowej oceny skutków przed konsultacjami publicznymi w sprawie projektu prawa; 6) projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa); 7) Operatorzy, dostawcy, stowarzyszenia branżowe ICT oraz odpowiednie zainteresowane strony nie są w stanie ocenić wpływu projektu ustawy w ciągu zaledwie 10 dni roboczych; 8) Termin wyznaczony na konsultacje publiczne 22.09.2020 nie jest zgodny z rygorem przejrzystości procesu decyzyjnego w administracji publicznej ze względu na znaczące skutki projektu ustawy, a także bez wstępnych konsultacji z zainteresowanymi stronami. **Potencjalny wpływ projektu ustawy na dostawców ;** 4) kryteria oceny są niejasne, nieprzejrzyste, a zakres oceny jest zbyt szeroki 5) Kryteria oceny są zbyt polityczne i nie obejmują mechanizmu norm technicznych i certyfikacji,	**Uwaga częściowo uwzględniona, OSR zostanie uzupełniony.**

			6) Spowoduje to dyskryminację między producentami i naruszenie konstytucyjnego prawa do dostaw towarów w Polsce i zakłócenie konkurencji; projekt jest sprzeczny z zasadą niedyskryminacji i równego traktowania UE. **Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych ;** 5) Ze względu na brak wiodących dostawców technologii 5G, jak również wymagane ogromne zmiany w ramach sieci komórkowych, Polska 5G i Agenda Cyfrowa mogą opóźnić 3-5 lat; 6) Operatorzy mogą stracić zaufanie do otoczenia inwestycyjnego naszego kraju Mogą oni również stracić siłę napędową w celu przyspieszenia uruchomienia 5G z powodu ograniczenia inwestycji i opóźnień technicznych. 7) Prawo operatorów do wyboru producenta będzie ograniczone. Ustawodawca i rząd powinni ustanowić jasne kryteria techniczne i wymogi, do których operatorzy powinni się stosować. W przeciwnym razie naruszy to prawo konkurencji zarówno na szczeblu krajowym, jak i unijnym. Ostateczny wybór dostawcy przez operatorów powinien opierać się na normach technologii, innowacji, kosztów i bezpieczeństwa cybernetycznego; 8) Dla operatorów w Polsce, projekt ustawy będzie miał poważne negatywne implikacje i będzie wyrządzał wielką szkodę ich poprzednim inwestycjom i prawom własności. Projekt tego prawa nie daje pewności prawa i zwiększa koszty operacyjne, co jest sprzeczne z warunkami określonymi w decyzjach administracyjnych dotyczących prowadzenia działalności. **Potencjalny wpływ projektu ustawy na konkurencję ;**	

			3) Polska ma ograniczoną liczbę dostawców sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to bardzo szkodzić innowacjom w technologii i odroczy digitalizację Polski. Koszty operatorów wzrosną , a ceny usług dla konsumentów wzrosną ; 4) Artykuł 3 pkt 1 ustawy o zwalczaniu nieuczciwej konkurencji i nie pozwala na utrudnienie dostępu do rynku 5) Przyczyny bezpieczeństwa narodowego nie powinno się nadużywać, a wyjątek dotyczący bezpieczeństwa narodowego powinien być stosowany z zachowaniem zasada proporcjonalności , obiektywności, przejrzystości i minimalnej ingerencji. **Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową ;** 4) Ponad 8 mld euro straty w sektorze telekomunikacyjnym (wzrost cen z powodu braku konkurencji) ponad 10 mld euro straty w całej gospodarce (lokalne zatrudnienie, zamówienia publiczne, negatywny wpyw na PKB) 5) Projekt ustawy będzie miał negatywny wpływ na gotowość podmiotów do składania ofert na infrastrukturę i usługi 5G; 6) Ograniczenie operatorów do wyboru dostawcy odroczy również uruchomienie sieci 5G, Rozwój Przemysłu 4.0 zostanie zablokowany. Polska ucierpi na brakach związanych z niskimi kompetencjami w dziedzinie kompetencji międzynarodowych 7) Roszczenia o odszkodowanie wobec rządu polskiego podniesione przez operatorów i dostawców zostaną ostatecznie wypłacone przez podatników i konsumentów. Budżet będzie zasilał operatorów i	

			producentów zamiast ułatwić życie obywatelom, , szczególnie po pandemii **Potencjalny wpływ projektu ustawy na postęp technologiczny ;** 5) Wyłączenie producenta, zwłaszcza wiodącego w branży ICT, spowoduje opóźnienie postępu w całym ekosystemie. Polska utraci możliwość skorzystania z rozwiniętej infrastruktury 5G innych krajów. 6) Operatorzy mogą stracić zaufanie do otoczenia inwestycyjnego w Polsce,. Mogą oni również stracić siłę napędową przyspieszenia uruchomienia 5G z powodu ograniczenia inwestycji i opóźnień technicznych. 7) Negatywny wpływ na życie i pracę podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, straci możliwość stworzenia nowych miejsc pracy dla ponad 250 000 osób 8) Projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0, Polska straci kompetencje w obszarze samochodów podłączonych do sieci 5G, produkcji 5G, high-tech, rolnictwo 5G, usługi portowe, zdalna edukacja, sprzęt medyczny 5G. itp	
457.	Stowarzyszenie Inżynierów Telekomunikacji	OSR Art. 66b	W uzasadnieniu zmian, oceniając skutki regulacji wskazano wyłącznie, że nowoprojektowane przepisy będą mieć wpływ na przedsiębiorców telekomunikacyjnych i to tylko w takim zakresie, że zamiast do Prezesa UKE będą oni zobligowani zgłaszać incydenty do zespołów CSIRT, uznając jednocześnie brak skutków dla tego sektora w ujęciu pieniężnym. Należy jednak podkreślić, że w opisie celu i skutkach wprowadzenia art. 66b do ustawy o cyberbezpieczeństwie pominięte zostały koszty wymiany sprzętu lub oprogramowania, który był dostępny na rynku i z którego branża telekomunikacyjna korzystała przy budowie sieci i	**Uwaga częściowo uwzględniona, OSR zostanie uzupełniony.**

			świadczeniu usług. Nie można uznać, że takie działanie jest bez kosztowe. Wymiana sprzętu lub oprogramowania (często niezamortyzowanego księgowo) na nowy, wygeneruje dodatkowe koszty dla przedsiębiorcy telekomunikacyjnego, koszty, których poniesienia nie mógł przewidzieć, decydując się na zakup sprzętu lub oprogramowania, które następnie musi wycofać. Biorąc powyższe pod uwagę, wnosimy o uwzględnienie przedstawionych argumentów i wprowadzenie odpowiednich zmian w art. 66b ustawy o cyberbezpieczeństwie.	
458.	EXATEL	OSR	Niezależnie od wyżej wymienionych zagrożeń wskazać należy, że w kosztach OSR budowy i funkcjonowanie CSIRT nie uwzględniono części kosztów, które niewątpliwie powstaną przy budowie CSIRT: **1. Kosztów dotyczących etatyzacji:** – kosztów utrzymania kadry zarządczej dla CSIRT (poza administratorem ktoś musi zarządzać całą strukturą), – kosztów rekrutacji z rynku potrzebnych pracowników (koszt zewnętrznej rekrutacji na jeden etat to minimum 20 000 zł miesięcznie brutto), – kosztów szkolenia pozyskanych pracowników (koszty od 10 000 zł rocznie na pracownika), **2. Kosztów pośrednich dotyczących budowy CSIRT** – kosztów technicznego przystosowania pomieszczeń do budowy CSIRT; – kosztów przygotowania koncepcji dla samego sposobu funkcjonowania CSIRT, wyboru platformy sprzętowej; – kosztów narzędzi niezbędnych do obsługi incydentów (np. serwery, systemy trackingowe do obsługi zgłoszeń etc.)	**Uwaga nieuwzględniona.** CSIRT sektorowe mają być wyznaczone w pierwszej kolejności spośród jednostek podległych lub nadzorowanych przez organ właściwy do spraw cyberbezpieczeństwa, który już funkcjonuje.

			Biorąc powyższe pod uwagę, istnieją zagrożenia, które mogą uniemożliwić budowę CSIRT przez organy właściwe. Z tego względu wskazujemy, że konieczne jest umożliwienie organom właściwym zlecanie funkcji CSIRT sektorowego jednostkom spoza art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), w szczególności spółkom kontrolowanym w 100% przez Skarb Państwa. Niezbędne i zasadne wydaje się być wykorzystanie w tym procesie podmiotów będących własnością Skarbu Państwa i dysponujących niezbędnym doświadczeniem w zakresie budowy i funkcjonowania SOC. Zlecanie części zadań na zewnątrz da dostęp do zasobów ludzkich i narzędzi, a poprzez to umożliwi szybkie osiągnięcie zdolności operacyjnej do świadczenia usług CSIRT w planowanym okresie 18 miesięcy od dnia wejścia w życie niniejszej ustawy. Dostęp do wiedzy bazującej na zdobytych już doświadczeniach z rynku przez podmioty świadczące podobne usługi zapewni transfer wiedzy niezbędny do wypracowania wewnętrznych procedur. Ponadto wykorzystanie istniejących już zasobów po stronie Skarbu Państwa przyczyni się do obniżenia kosztów funkcjonowania samego systemu CSIRT sektorowych. W przypadku powierzenie realizacji CSIRT działającemu już podmiotowi dojdzie do efektu synergii, a poprzez to obniżenia kosztów jednostkowych. Biorąc powyższe pod uwagę zasadnym i koniecznym jest dopisanie do katalogu podmiotów, którym może zostać powierzona realizacja zadań CSIRT sektorowego spółkom akcyjnym pozostającym pod całkowitą kontrolą Skarbu Państwa.	
459.	Związek Banków Polskich	Art. 2 pkt. 5	**Propozycja zmiany** Incydent - każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych; **Uzasadnienie:**	**Uwaga nieuwzględniona** Dyrektywy unijne mają być wdrożone do porządku prawnego państwa członkowskiego w sposób zgodny

			Konieczność dostosowania definicji do definicji w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.	z celem dyrektywy, niekoniecznie musi to oznaczać dosłowne skopiowanie treści dyrektywy. Obecna definicja incydentu dobrze spełnia swoją funkcję obejmując wszystkie zdarzenia zagrażające sieciom i systemom informatycznym.
460.	Związek Banków Polskich	Art. 2 pkt. 12	**Propozycja zmiany** 12) Ryzyko - każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych; **Uzasadnienie:** Konieczność dostosowania definicji do definicji w Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.	**Uwaga nieuwzględniona** Dyrektywy unijne mają być wdrożone do porządku prawnego państwa członkowskiego w sposób zgodny z celem dyrektywy, niekoniecznie musi to oznaczać dosłowne skopiowanie treści dyrektywy.
461.	Związek Banków Polskich	Art. 5 – Załącznik nr 1 Bankowość i infrastruktura rynków finansowych	**Propozycja zmiany:** **Proponuje się dodanie do załącznika nr 1 - Bankowość i infrastruktura rynków finansowych następujące podmioty:** **- dostawców usług płatniczych, o których mowa w art. 4 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych;** **- krajowa instytucja płatnicza, o której mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych;** **- izba rozliczeniowa, o której mowa w art. 67 ustawy z dnia 29 sierpnia 1997 r. - Prawo bankowe.** **Uzasadnienie:** Brak ww. podmiotów powoduje stworzenie luki w systemie płatniczym kraju, co oznacza faktyczną niemożliwość wykrywania, przeciwdziałania i zwalczania cybericydnetów w obszarze realizacji i rozliczeń transakcji płatniczych.	**Uwaga nieuwzględniona, nie dotyczy projektu nowelizacji. Na dzień dzisiejszy nie planuje się zmiany treści załącznika nr 1.**

462.	Związek Banków Polskich	Art. 8 pkt 7) (nowy)	**Propozycja zmiany:** Proponuje się dodanie w art. 8 pkt 7 w brzmieniu: **7) zasoby ludzkie adekwatne do zakresu świadczonych usług kluczowych oraz ryzyka związanego ze świadczeniem tych usług.** **Uzasadnienie:** Posiadanie odpowiednich i proporcjonalnych do ryzyka środków technicznych i organizacyjnych, bez zapewnienia odpowiedniego i kompetentnego zespołu pracowników, będzie niekompletnym systemem cyberbezpieczeństwa, gdyż system ten winieni opierać się na trzech równoważnych komponentach: sprzęcie, procesach i ludziach.	**Uwaga nieuwzględniona**
463.	Związek Banków Polskich	Art. 9 ust. 1 pkt. 1	**Propozycja zmiany:** Proponuje się aby w art. 9 ust. pkt 1 otrzymał brzmienie: Operator usługi kluczowej: 1) wyznacza osobę, **osoby lub komórkę organizacyjną** odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. **Uzasadnienie:** Nie możemy wyznaczyć fizycznie jednej osoby musi to być cała lista kontaktowa osób lub tzw. punktu kontaktowego	**Uwaga nieuzwględniona** Istotą jest, żeby była możliwość kontaktu z konkretną osobą podczas obsługi incydentu.
464.	Związek Banków Polskich	Art. 12. Ust. 3	**Propozycja zmiany:** Proponuje się aby w art. 12 ust. 3 otrzymał brzmienie: 3. Operator usługi kluczowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, **dane osobowe** i informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.	**Uwaga nieuwzględniona** Już jest to uregulowane w art. 11 ust 1 pkt 5 in fine.

			Uzasadnienie: Ustawa wyraźnie rozgranicza dane osobowe od tajemnic prawnie chronionych. W związku z potrzebą sprawnej obsługi incydentu, jego koordynacji i zarządzania często zdarza się konieczność przekazania nie tylko tajemnic prawnie chronionych ale także danych osobowych np. osób pokrzywdzonych w celu ich ochrony	
465.	Związek Banków Polskich	Art. 15 ust. 2 pkt 2	**Propozycja zmiany:** 2. Audyt może być przeprowadzony przez: 2) **zespół składający się z** co najmniej dwóch audytorów posiadających: a)certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub b)co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub c)co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych; **Uzasadnienie:** Proponujemy, aby ustawa wskazywała na możliwość przeprowadzania audytu przez **zespół** co najmniej dwóch audytorów.	**Uwaga nieuwzględniona** Uwaga nie niesie ze sobą dodatkowej wartości normatywnej.
466.	Związek Banków Polskich	Art. 26 ust. 3 pkt 12	**Propozycja zmiany:** Proponuje się aby w art. 26 ust. 3 pkt. 12 otrzymał brzmienie: 3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy: 12) przekazywanie, w terminie do dnia 30 maja każdego roku, do	**Uwaga nieuwzględniona** Dyrektywa NIS w art. 14 i 16 mówią wyłącznie o incydentach poważnych lub istotnych.

			Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych **mających lub mogących spowodować obniżenie jakości lub** mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej; **Uzasadnienie:** Definicja incydentu poważnego określa dwa czynniki a mianowicie: 1. powodujący lub mogący spowodować poważne obniżenie jakości lub 2. przerwanie ciągłości świadczenia usługi kluczowej. Natomiast w art. 26 ust. 3 pkt 12 powołano się chyba błędnie jedynie na kwestie związane z ciągłością świadczenia usługi kluczowej?	
467.	Związek Banków Polskich	Art. 26 ust. 3 pkt 14 ppkt a), i c)	**Propozycja zmiany:** Proponuje się aby art. 26 ust. 3 pkt. 14 ppkt a) i c) otrzymały brzmienie: 3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy: 14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności: a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności **i zagrożeń cyberbezpieczeństwa**,	**Uwaga nieuwzględniona** Art. 32 już umożliwia analizę zagrożeń cyberbezpieczeństwa.

			... c) rozwija narzędzia i metody do wykrywania podatności i zagrożeń cyberbezpieczeństwa **oraz skutecznej obsługi incydentów**, **Uzasadnienie:** W zakresie analiz oprócz podatności analizowane są także zagrożenia cyberbezpieczeństwa. Dodatkowo nie wolno pominąć przy rozwijaniu narzędzi i metod niezbędnych do zwalczania incydentów.	
468.	Związek Banków Polskich	Art. 26 ust. 5 pkt 3 (nowy)	**Propozycja zmiany:** Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez: podmioty, o których mowa w ust. 6, jeżeli incydent wymaga współpracy w zakresie zadań Służby Kontrwywiadu Wojskowego, o których mowa w art. 5 ust. 1 i ust. 2 ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego. **Uzasadnienie:** Doświadczenia sektora bankowego wskazują, że podział podmiotowy pomiędzy poszczególnymi CSIRTami jest niewystarczający. W uzasadnionych przypadkach konieczne jest również wprowadzenie podziału przedmiotowego.	**Uwaga nieuwzględniona.** CSIRT MON koordynuje obsługę incydentu o charakterze terrorystycznym o którym mowa w art. 5 ust. 1 pkt 2a ustawy o SKW co konsumuję niniejszą uwagę.
469.	Związek Banków Polskich	Art. 26 ust. 7 pkt 7 (nowy)	**Propozycja zmiany:** Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez: podmioty, o których mowa w ust. 6, jeżeli incydent wymaga współpracy w zakresie zadań Agencji Bezpieczeństwa Wewnętrznego, o których mowa w art. 5 ust. 1 ustawy z dnia 24	**Uwaga nieuwzględniona.** CSIRT GOV koordynuje obsługę incydentu o charakterze terrorystycznym co konsumuję niniejszą uwagę.

			maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. **Uzasadnienie:** Doświadczenia sektora bankowego wskazują, że podział podmiotowy pomiędzy poszczególnymi CSIRTami jest niewystarczający. W uzasadnionych przypadkach konieczne jest również wprowadzenie podziału przedmiotowego.	
470.	Związek Banków Polskich	Art. 30 ust. 3	**Propozycja zmiany:** Proponuje się usunięcie art. 30 ust. 3, a dotychczasowy ust. 4 oznaczony zostaje jako ust. 3 **Uzasadnienie:** Proponuje się usunięcie tego przepisu, gdyż CSIRT NASK miałby możliwość samodzielnie decydować o zarządzaniu danym incydentem. Z doświadczeń sektora bankowego wynika, że bardzo często pierwsze informacje o incydentach pochodzą od klientów i ich zbagatelizowanie mogłoby wpłynąć negatywnie na reputację banku.	**Uwaga nieuwzględniona** Obsługa incydentów które dotknęły osoby fizyczne i podmioty spoza krajowego systemu cyberbezpieczeństwa nie jest głównym zadaniem CSIRT NASK. Dlatego te zgłoszenia muszą być w miarę dysponowania zasobami przez CSIRT NASK.
471.	Związek Banków Polskich	Art. 32 ust. 1	**Propozycja zmiany:** Proponuje się aby w art. 32 ust. 1 otrzymał brzmienie: 1. CSIRT MON, CSIRT NASK i CSIRT GOV **oraz właściwy CSIRT sektorowy oraz właściwy ISAC dla danego sektora, sektorów lub podsektorów** mogą wykonywać niezbędne działania techniczne związane z analizą **podatności i** zagrożeń cyberbezpieczeństwa, zarządzaniem obsługi incydentu, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego. **Uzasadnienie:**	**Uwaga nieuwzględniona** ISAC nie są jednostką operacyjną. Zatem nie może dokonywać analizy podatności, lecz może przekazywać informacje uzyskane od zespołów CSIRT o wykrytych podatnościach.

			CSIRT sektorowe oraz ISAC mogąc przeprowadzać techniczne analizy zagrożeń mogą w istotny sposób wesprzeć CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie zarządzania incydentami poważnymi, istotnymi i krytycznymi.	
472.	Związek Banków Polskich	Art. 34 ust. 3 **- nowy**	**Propozycja zmiany:** Proponuje się dodanie w art. 34 ust. 3 w brzmieniu: 3. Do CSIRT sektorowych oraz ISAC koordynujących obsługę incydentu, który doprowadził do naruszenia danych osobowych przepis ust. 2 stosuje się odpowiednio. **Uzasadnienie:** CISIRT sektorowe i ISAC koordynując obsługę incydentu powinny współpracować z organem właściwym do spraw ochrony danych osobowych. Brak tej możliwości współpracy znacząco ogranicza skuteczność obsługi incydentu przez OUK.	**Uwaga nieuwzględniona.** ISAC nie są jednostką operacyjną, a więc nie zajmują się na reagowaniem na incydenty.
473.	Związek Banków Polskich	Art. 37 ust. 2 i 3	Proponuje się aby było jedno miejsce, w którym będą publikowane informacje o incydentach poważnych i istotnych. Użytkownicy mogą być zdezorientowani gdzie szukać informacji. Dlatego proponuje się ustalenie jednego centralnego miejsca publikacji na poziomie zarządzania ww. incydentami. Dodatkowo, takie publikacje na poziomie koordynacji mogą dokonywać CISRT sektorowe oraz na poziomie obsługi incydentu - operatorzy usług kluczowych oraz dostawcy usług internetowych.	**Uwaga nieuwzględniona.** Podłączenie się podmiotów krajowego systemu cyberbezpieczeństwa do systemu z art. 46 pozwoli na otrzymywanie tych informacji z tego systemu w ramach określonych w porozumieniu z ministrem do spraw informatyzacji.
474.	Związek Banków Polskich	Art. 39 ust. 1	**Propozycja zmiany:** Proponuje się aby w art. 39 ust. 1 otrzymał brzmienie: Art. 39. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowe oraz ISAC** przetwarzają **informacje stanowiące tajemnice prawnie chronione** oraz **informacje związane** z incydentami i	**Uwaga nieuwzględniona.** Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione.

			zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679", w zakresie i w celu niezbędnym do realizacji tych zadań. **Uzasadnienie:** W celu skutecznego działania CSIRT MON, CSIRT NASK, CSIRT GOV niezbędne jest wprowadzenie podstawy prawnej do przetwarzania informacji stanowiących tajemnice prawnie chronionych oraz dane osobowe. Konieczne jest również wprowadzenie do tego przepisu CSIRT sektorowych i ISAC.	
475.	Związek Banków Polskich	Art. 39 ust. 3	**Propozycja zmiany:** Proponuje się aby w art. 39 ust. 3 otrzymał brzmienie: 3. CSIRT MON, CSIRT NASK, CSIRT GOV, **CSIRT sektorowe i ISAC** przetwarzają **tajemnice prawnie chronione oraz informacje, w tym dane osobowe** związane z incydentami i zagrożeniami cyberbezpieczeństwa: 1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych; 2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 3) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług; 4) gromadzone przez podmioty publiczne w związku z realizacją	**Uwaga nieuwzględniona**. Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione.

			zadań publicznych dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1. **Uzasadnienie:** Obok danych osobowy należy dodać również tajemnice prawnie chronione, gdyż wówczas podmioty uprawnione mogą pozyskać kompletną - pełną informację. Zasadne jest również dodanie do wskazanego przepisu ISAC.	
476.	Związek Banków Polskich	Art. 39 ust. 7	**Propozycja zmiany:** Proponuje się aby w art. 39 ust. 7 otrzymał brzmienie: 7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, CISRT telco i **ISAC** mogą przekazywać sobie wzajemnie **informacje**, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych. **Uzasadnienie:** W ust. 3 jest mowa nie tylko o danych osobowych, więc wskazane jest aby użyć innego określenia np. informacje. Ponadto w celu skutecznej realizacji zdań ISAC, zasadne jest wskazanie go również w tym przepisie.	**Uwaga nieuwzględniona** ISAC nie jest jednostką operacyjną.
477.	Związek Banków Polskich	Art. 39 ust. 10 - nowy	**Propozycja zmiany:** Proponuje się dodanie w art. 39 ust. 10 w brzmieniu: 10**. Operatorzy usług kluczowych, dostawcy usług cyfrowych, przedsiębiorcy komunikacji elektronicznej, dostawcy usług internetowych oraz ISAC są uprawnieni do przetwarzania, w tym udostępniania sobie nawzajem informacji stanowiących tajemnice prawnie chronione, w szczególności danych osobowych obejmujących także dane określone w art. 9 ust. 1**	**Uwaga nieuwzględniona**. Taki przepis naruszałby zasady przetwarzania informacji niejawnych oraz inne tajemnice prawnie chronione.

			rozporządzenia 2016/679, w przypadkach przestępstw lub uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę operatorów usług kluczowych, dostawców usług cyfrowych, przedsiębiorców telekomunikacyjnych oraz dostawców usług internetowych oraz ich klientów w celu ich wykrywania, analizowania, zapobiegania i zwalczania. **Uzasadnienie:** Brak przepisów umożliwiających przetwarzanie informacji stanowiących tajemnice prawnie chronione, w tym dane osobowe pomiędzy OUK, DUC, telekomami, ISP oraz ISAC uniemożliwia sprawą wymianę informacji o incydentach w celu skutecznej ich obsługi i koordynacji oraz przeprowadzania analiz.	
478.	Związek Banków Polskich	Art. 39 ust. 11 - nowy	**Propozycja zmiany:** **Proponuje się dodanie w art. 39 ust. 11 w brzmieniu:** **11. W przypadkach, o których mowa w ust. 10 w zakresie przetwarzania danych osobowych przepisów art. 5 oraz art. 12-22 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych nie stosuje się.** **Uzasadnienie:** Jest to niezmiernie ważny przepis z punktu widzenia skutecznego wykrywania i ścigania przestępców popełniających przestępstwa na szkodę operatorów usług kluczowych oraz dostawców usług cyfrowych i ich klientów - absurdem byłby obowiązek informacyjne względem tych osób, że podmioty uprawnione przetwarzają ich dane osobowe i dodatkowo wystąpienie o ich zgodę na przetwarzanie ich danych. Na powyższe zezwala art. 23 ust. 1 lit. d) RODO - d)zapobieganiu przestępczości, prowadzeniu	**Uwaga nieuwzględniona,** nie dotyczy projektu nowelizacji.

			postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych lub wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom;	
479.	Związek Banków Polskich	Art. 39 ust. 12 - nowy	**Propozycja zmiany:** Proponuje się dodanie w art. 39 ust. 12 w brzmieniu: **12. Operator usług kluczowych, dostawca usług cyfrowych lub ISAC nie ponoszą odpowiedzialności cywilnej za szkodę, która może wynikać z wykonywania przez nich ustawowych obowiązków w zakresie przeciwdziałaniu przestępstwom, gdy działając z należytą starannością i w dobrej wierze zgłosili właściwym organom zawiadomienie o podejrzeniu popełniania przestępstwa, a te po weryfikacji uznały podejrzenie za nieuzasadnione. W takich przypadkach odpowiedzialność za szkodę wynikłą z podjętych działań przez operatora usług kluczowych lub dostawcy usług cyfrowych ponosi Skarb Państwa.** **Uzasadnienie:** Potrzeba prowadzenia prawnej ochrony OUK, DUC i ISAC w sytuacjach wypełniania przez nich obowiązków wynikających z niniejszej ustawy w dobrej wierze.	**Uwaga nieuwzględniona** Zasady odpowiedzialności Skarbu Państwa regulują przepisy Kodeksu cywilnego. Skarb Państwa nie może ponosić odpowiedzialności deliktowej za niepaństwowe osoby prawne.
480.	Związek Banków Polskich	Art. 46 ust. 4 - nowy	**Propozycja zmiany:** **Proponuje się dodanie w art. 46 ust. 4 w brzmieniu:** **4. O ile istnieją sektorowe lub podsektorowe systemy informacyjne, zapewniające, w szczególności, obsługę incydentów lub koordynację obsługi incydentów, Minister właściwych do spraw informatyzacji włącza te systemy do systemu, o którym mowa w ust. 1. Zasady korzystania z tych systemów określa porozumienie zawarte pomiędzy Ministrem a właścicielami tych systemów.**	**Uwaga nieuwzględniona** Uwaga nie dotyczy projektu nowelizacji.

			Uzasadnienie: Sektor bankowy własnym kosztem wytworzył wiele systemów wspierających bezpieczeństwo banków oraz ich klientów. Istotne jest aby wykorzystywać je w ramach krajowego systemu cyberbezpieczeństwa. Poza tym obowiązki informacyjne o incydentach np. względem CSIRT MON, CSIRT NASK i CSIRT GOV mogłyby być realizowane z ich użyciem. Pozwoli to uniknąć dublowania czynności związanych z notyfikacją incydentów do wielu instytucji państwowych np. KNF, PUODO, prokuratury, policji itp**.**	
481.	Związek Banków Polskich	Art. 51 - nowy	**Propozycja zmiany:** Proponuje się dodanie nowego art. 51 w brzmieniu (zmianie ulegnie numeracja kolejnych artykułów): Art. 51. Minister właściwy do spraw informatyzacji, na wniosek i w uzgodnieniu z organami właściwymi do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi lub ISAC może wydać w drodze rozporządzenia techniczne i proceduralne mechanizmy zwiększające bezpieczeństwa operatorów usług kluczowych i dostawców usług cyfrowych oraz ich klientów. **Uzasadnienie:** Proponuje się dodanie przepisu umożliwiającego ministrowi właściwemu do spraw informatyzacji, na wniosek w uzgodnieniu z wymienionymi podmiotami wydawanie w drodze rozporządzenia określającego techniczne i proceduralne mechanizmy zwiększające bezpieczeństwa operatorów usług kluczowych i dostawców usług cyfrowych oraz ich klientów. Przykładowym rozwiązaniem mogłoby być wprowadzenie przepisu o możliwości blokowania ruchu na serwery	**Uwaga nieuwzględniona** Uwaga nie dotyczy projektu nowelizacji.

			wykorzystywane przez przestępców do gromadzenia tajemnic prawnie chronionych i danych osobowych.	
482.	Związek Banków Polskich	Art. 54 ust. 1	**Propozycja zmiany:** Proponuje się aby w art. 54 ust. 1 otrzymał brzmienie: 1. **O ile odrębne przepisy nie stanowią inaczej** do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. **Uzasadnienie:** Zakres sprawowania kontroli i nadzoru w sektorze finansowych określony jest m. in. W ustawie - prawo bankowe oraz ustawie o KNF. Zawarte w tych ustawach uregulowania powinny być lex specialis względem przepisów dotyczących kontroli w ustawie o krajowym systemie cyberbezpieczeństwa.	**Uwaga nieuwzględniona** Uwaga nie dotyczy projektu nowelizacji.

Zbiorcza tabela uwag do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (poprzedni tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa (UD68).

Część II

Liczba organizacji, które otrzymały zaproszenia:
Organizacje, które zgłosiły swoje uwagi: Związek Banków Polskich, Santander, Narodowy Instytut Cyberbezpieczeństwa, Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM, Bank Handlowy, Q-PRO Jakub Stoparek, RFCell Technologies Sp. z.o.o., KGHM/Związek Pracodawców Polska Miedź, Stowarzyszenie Libertariańskie, SayF, Transition Software, Izba Gospodarcza Gazownictwa/Polska Spółka Gazownictwa Sp. z.o.o./PGNIG SA Oddział w Zielonej Górze, Izba Przemysłowo-Handlowa Polska-Azja, Huawei Polska, Business Centre Club, Digital Poland, Excogitate, Fundacja Bezpieczna Cyberprzestrzeń, Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji KIGEIT, Narodowy Bank Polski, Naczelna Organizacja Techniczna. Federacja Stowarzyszeń Naukowo-Technicznych, Polskie Centrum Badań i Certyfikacji, Polski Związek Pracodawców Przemysłu Farmaceutycznego, T-Mobile, Federacja Przedsiębiorców Polskich, 1Innosystems, Polska Izba Komunikacji Elektronicznej, Fabryka E-Biznesu, Unia Metropolii Polskich, Krajowa Izba Gospodarki Cyfrowej DigiCom, Home.pl, Install Tech, Polska Izba Handlu, ISACA Warsaw Chapter, Krajowy Sekretariat Łączności NSZZ Solidarność, MJC Sp. z.o.o., IAB Polska, Federacja Konsumentów, Stowarzyszenie „Miasta w Internecie", Stowarzyszenie Inżynierów Telekomunikacji, Uniwersytet Jagielloński Collegium Medicum, PKP Energetyka, Sektorowa Rada ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo, Polskie Towarzystwo Informatyczne, ISSA Polska, Związek Przedsiębiorców i Pracodawców, Krajowy Depozyt Papierów Wartościowych, Politechnika Wrocławska. Wrocławskie Centrum Sieciowo-Superkomputerowe, EXATEL, S4IT Michał Podgórski, Orange Polska, Polsko-Chińska Główna Izba Gospodarcza SinoCham, Aberit, Młodzieżowy Delegat RP przy NATO, ERSTAR, ETOB-RES, Fundacja Alatum, GBX Soft, Instytut Lema, Mobile Logic, Mobilne Miasto, Nanocoder, NeuroGames Lab, SmartWeb Media, TELDATA, TEP Doradztwo Biznesowe, TILT, Związek Cyfrowa Polska, Signum Edward Kuś Marcin Kuś, PKN Orlen, Skandynawsko-Polska Izba Gospodarcza, Liquid Systems, Instytut Staszica, Akademia Sztuki Wojennej, Krajowa Izba Komunikacji Ethernetowej, Qualitel Service, JARTEL, Izba Gospodarki Elektronicznej, Konfederacja Lewiatan
Podmioty, które odpowiedziały na zaproszenie, ale nie zgłosiły uwag do projektu: Porozumienie Zielonogórskie. Federacja Związków Pracodawców Ochrony Zdrowia
Podmioty, które zrezygnowały z udziału w konsultacjach:

1.	Qualitel Service	Uwaga ogólna	Na przestrzeni ostatnich tygodni jesteśmy świadkami dyskusji na temat nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Jako firma z branży telekomunikacyjnej my również jesteśmy zainteresowani tą sprawą. Wierzymy, że ta Ustawa będzie miała duży wpływ na rozwój branży	**Uwaga nieuwzględniona** Dostawca będzie oceniany pod kątem technicznym i

			telekomunikacyjnej, a także jest ściśle związana z przyszłym rozwojem naszej firmy. Doceniamy, że Ministerstwo Cyfryzacji dokłada wszelkich starań, aby poprawić poziom cyberbezpieczeństwa i chronić prywatność obywateli, jednakże martwimy się, że ocenianie dostawców na podstawie nietechnicznych czynników nie zapewni zwiększenia poziomu cyberbezpieczeństwa w Polsce, a co więcej, wpłynie negatywnie na zatrudnienie i rozwój branży ICT. W związku z powyższym, w celu zapewnienia obiektywnych standardów, sugerujemy wprowadzenie ściśle określonych wymogów technicznych dotyczących sprzętu w kluczowych sektorach, które powinny być spełnione przez wszystkich dostawców sprzętu niezależnie od kraju pochodzenia. Uważamy, że takie rozwiązanie wpłynęłoby pozytywnie i kompleksowo na poziom cyberbezpieczeństwa w Polsce. Sugerujemy przeprowadzić pełną analizę skutków płynących z Projektu nowelizacji ustawy oraz konsultacji społecznych, co pozwoliłoby obywatelom brać aktywny udział w debatach dotyczących ich rzeczywistych interesów, a także pozwoliłoby Ministerstwu na opracowanie projektu ustawy pozbawionego ryzyka negatywnego wpływu na branżę teleinformatyczną i bezpośrednio na społeczeństwo.	nietechnicznym, tak jak to ujmuje Toolbox 5G. Interesariusze mogli wypowiedzieć się w ramach konsultacji publicznych
2.	JARTEL	Uwaga ogólna	Jako firma P.R.T. JARTEL z branży ICT, świadczymy usługi dla wielu firm telekomunikacyjnych. Ostatnio dowiedzieliśmy się, że wprowadzono Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, który może mieć duży wpływ na branżę telekomunikacyjną, i w którym to wprowadzono kryterium oceny ryzyka dostawców oprogramowania i sprzętu w budowie sieci 5G. Zauważyliśmy jednak, że kryterium oceny koncentruje się głównie na czynnikach nietechnicznych. Jednocześnie wątpimy, czy takie kryterium oceny może dokładnie ocenić zdolność dostawcy do zapewnienia sprzętu i oprogramowania o wysokiej jakości. Ponadto operatorzy są również zobowiązani do wymiany całego sprzętu zakupionego od dostawców wysokiego ryzyka w ciągu 5 lat i poniesienia kosztów wymiany, co zwiększy koszty działalności dla operatorów, co z kolei może wpłynąć negatywnie na pracę ich dostawców jak również ceny usług. W związku z powyższym, sugerujemy, aby Projekt odnosił się do unijnych standardów ujednoliconej oceny dostawców, tym samym wdrażając bardziej rygorystyczne zarządzanie krytycznym sprzętem lub oprogramowaniem.	**Uwaga nieuwzględniona** Dostawca będzie oceniany pod kątem technicznym i nietechnicznym, tak jak to ujmuje Toolbox 5G. Interesariusze mogli wypowiedzieć się w ramach konsultacji publicznych

			Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa będzie miała głęboki wpływ na branżę ICT oraz przyszły rozwój cyfrowy Polski, dlatego też mamy nadzieję, że pojawi się okazja do publicznej dyskusji, która pozwoliłaby Państwu wysłuchać opinii wszystkich interesariuszy i przeprowadzić bardziej wszechstronną analizę wpływu Ustawy. Sądzimy, że takie podejście pozwoliłoby na poprawę poziomu cyberbezpieczeństwa w Polsce. Dziękujemy za poświęcenie nam uwagi.	
3.	Konfederacja Lewiatan	Uwaga ogólna	Konfederacja Lewiatan aktywnie i od samego początku uczestniczy w dyskusjach na temat tworzącego się krajowego systemu cyberbezpieczeństwa oraz regulacji dotyczących rynku komunikacji elektronicznej. Naszymi członkami są kluczowi gracze polskiego rynku cyfrowego, a także podmioty zaliczane do krajowego systemu cyberbezpieczeństwa w różnych sektorach. Dzięki tym doświadczeniom dobrze rozumiemy i w pełni popieramy ideę maksymalnego bezpieczeństwa w cyberprzestrzeni. Wszelkie ryzyka w tym obszarze są bowiem bezpośrednio ryzykiem dla nas samych, jak i reprezentowanych przez nas przedsiębiorstw. Ryzykiem o tyle kluczowym, że niewłaściwe zarządzanie nim może oznaczać ogromne skutki finansowe, a w skrajnych przypadkach przesądzać o dalszym losie danej organizacji. Stąd, co do zasady wspieramy działania rządu mające na celu podniesienie poziomu cyberbezpieczeństwa zarówno w sektorze publicznym, jak i prywatnym. Podobnie za zasadne uznajemy, o ile nie ingeruje to zbytnio w konkurencyjny rynek, wzmacnianie publicznych instytucji w zakresie ich finansowania, organizacji i kompetencji. Jednak, pod dogłębnej analizie stwierdzamy, że przedstawiony do konsultacji projekt ustawy stanowi bardzo poważne wyzwanie, a po części także zaskoczenie dla podmiotów, które miałyby zostać objęte nowymi regulacjami. W znakomitej bowiem części kształt proponowanych przepisów został ustalony bez udziału partnerów społecznych i adresatów nowych przepisów. Tymczasem jak zakładamy, to na wzajemnym dialogu, zrozumieniu potrzeb oraz współpracy powinien być budowany spójny i efektywny system cyberbezpieczeństwa. Z tych względów uważamy, że tak daleko idąca interwencja legislacyjna powinna zostać poprzedzona szeroką dyskusją merytoryczną z wszystkimi zainteresowanymi uczestnikami rynku, a kształt projektu winien odzwierciedlać gruntownie przemyślaną i	**Wyjaśnienie** Interesariusze mogli wypowiedzieć się w ramach konsultacji publicznych

			kompromisową koncepcję poprawy cyberbezpieczeństwa. Podobnie jak dzieje się to w ramach dyskusji nad kształtem przyszłych aktów prawnych na poziomie unijnym, czy jak udało się to przeprowadzić w toku dyskusji nad przyjętymi niedawno rozporządzeniami do art. 176a i 175d ustawy – Prawo telekomunikacyjne. Dlatego już na wstępie przedstawiamy nasze postulaty o charakterze podstawowym, które w dalszej części uszczegóławiamy i dodatkowo uzasadniamy. Liczymy na możliwość ich przedyskutowania, a przede wszystkim uwzględnienia w toku dalszych prac legislacyjnych. 1. W pierwszej kolejności za zasadne uważamy przeprowadzenie oraz przedstawienie w projekcie szerszego odniesienia do oceny skutków regulacji. To w naszej ocenie kluczowy element dla dalszej rzetelnej dyskusji na temat projektu ustawy. Obszary takiej analizy przedstawiamy w uwagach szczegółowych.	
4.	Konfederacja Lewiatan	Uwaga ogólna	2. Postulujemy, aby przyspieszyć prace na poziomie UE w celu przyjęcia wspólnego podejścia do oceny bezpieczeństwa sprzętu i oprogramowania. Zauważamy bowiem, że kwestie cyberbezpieczeństwa nie są ograniczone granicami państwowymi. Tym bardziej takich ograniczeń nie będą znały bazujące na sieciach 5G rozwiązania, jak chociażby korytarze transportowe umożliwiające autonomiczny ruch pojazdów. Niestety na poziomie UE przyjęto dotychczas dość ogólne wytyczne kierunkowe, które skutkują w praktyce tym, że kraje UE, w tym sąsiedzi Polski przyjmują zupełnie odmienne podejście do kwestii bezpieczeństwa sieci 5G oraz dostawców. Takie wyspowe podejście do cyberbezpieczeństwa nie służy w naszej ocenie tworzeniu równego i jednolitego rynku cyfrowego na poziomie UE.	**Wyjaśnienie** UE przyjęła wspólne podejście do oceny bezpieczeństwa – jest nim Toolbox 5G
5.	Konfederacja Lewiatan	Uwaga ogólna	Obok konsultowanych rozwiązań za istotne uważamy zaadresowanie zagrożeń cyberbezpieczeństwa po stronie użytkowników końcowych, w tym związanych z używanymi przez nich aplikacjami, które wielokrotnie stanowią istotne wektory ataków. Ten obszar pozostawiony jest dotychczas bez wyraźnego zaadresowania, podczas gdy z perspektywy większości użytkowników właśnie tutaj istnieje największe zagrożenie dla bezpieczeństwa.	**Wyjaśnienie** – Obywatele nie są bezpośrednio objęci ustawą, jednakże celem nadrzędnym ustawy jest zapewnianie cyberbezpieczeństwa na poziomie kraju, a w tym niezakłóconego świadczenia usług kluczowych i

				cyfrowych dla obywateli. Ustawa reguluje kwestie obowiązku informowania przez podmioty krajowego systemu cyberbezpieczeństwa o zagrożeniach cyberbezpieczeństwa oraz sposobach zabezpieczenia się przed tymi zagrożeniami (art. 9 ust 1 pkt 2). Natomiast kwestia podnoszenia świadomości społecznej o cyberbezpieczeństwie różnych grup użytkowników internetu jest przedmiotem szerokiej działalności informacyjno-edukacyjnej ministra właściwego ds. informatyzacji, która również jest umocowana ustawą (art. 45 ust. 1 pkt.4)
6.	Konfederacja Lewiatan	Uwaga ogólna	Rynek komunikacji elektronicznej powinien nadal pozostać kompleksowo regulowany sektorowo ze względu na jego szczególne cechy, aktualny kształt przepisów unijnych oraz bardzo ograniczony czas na wprowadzenie rewolucyjnych zmian w tym zakresie. Tym samym, na obecnym etapie należałoby zrezygnować w projekcie z przepisów dotyczących objęcia przedsiębiorców komunikacji elektronicznej nowymi obowiązkami w ramach ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie włączenia ich do krajowego systemu cyberbezpieczeństwa oraz wprowadzenia nowego reżimu raportowego w zakresie incydentów. Szczególnie, że istnieje już właściwy dla takich podmiotów kanał raportowania do Prezesa Urzędu	Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc

			Komunikacji Elektronicznej, a następnie do podmiotów krajowego systemu cyberbezpieczeństwa. Właściwy tryb w tym zakresie został już przedstawiony w projekcie PKE, a jego ewentualne rozszerzenie wymaga pogłębionej dyskusji i czasu.	poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa

				sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
7.	Konfederacja Lewiatan	Uwaga ogólna	5. Jeśli podmioty krajowego systemu cyberbezpieczeństwa potrzebują dodatkowych lub bardziej bezpośrednich informacji o incydentach w sieciach telekomunikacyjnych jesteśmy otwarci na dyskusję na temat możliwości poprawy aktualnego systemu raportowania, w którym to Prezes UKE powinien przekazywać CSIRT takie informacje. Rozwiązaniem mogłoby być zobowiązanie Prezesa UKE do przekazywania wszystkich informacji o incydentach w sieciach do CSIRT krajowych i pozostawienie im oceny wpływu na cyberbezpieczeństwa oraz ewentualnego powiadamiania objętych zagrożeniem podmiotów.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez

				operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
8.	Konfederacja Lewiatan	Uwaga ogólna	6. Przepisy dotyczące nowych uprawnień Pełnomocnika oraz Kolegium wymagają w naszej ocenie rewizji, w szczególności pod kątem skupienia na samych urządzeniach i oprogramowaniu, mocniejszym uwzględnieniu kwestii technicznych, a wreszcie zapewnienia większej elastyczności i czasów na dostosowanie dla użytkowników urządzeń i oprogramowania uznanych za stwarzające wysokie lub umiarkowane ryzyko. W szczególności powinny zostać poszanowane okresy amortyzacji użytkowanych już w sieciach urządzeń, a także możliwość pełnego (w tym okresie) użytkowania posiadanego sprzętu lub oprogramowania, w tym ewentualnych zakupów lub wdrożeń, które są niezbędne dla napraw awarii i utrzymania ciągłości świadczenia usług, w tym telekomunikacyjnych. W zakresie samej oceny proponujemy przede wszystkim wykorzystanie modeli certyfikacji na poziomie unijnego schematu certyfikacji bazującego na Akcie o cyberbezpieczeństwie, tj. wprowadzenie zasad	**Uwaga nieuwzględniona** Kryteria oceny opisane w Toolbox 5g są techniczne i nietechniczne. Planowane jest wdrożenie niniejszą nowelizacją również Aktu o cyberbezpieczeństwie

			wymagających od producentów dokonania odpowiedniej certyfikacji swoich urządzeń i oprogramowania	
9.	Konfederacja Lewiatan	Uwaga ogólna	7. Mechanizm oceny ryzyka powinien dotyczyć sprzętu i oprogramowania wchodzącego w skład infrastruktury krytycznej oraz opierać się przede wszystkim o wymagania techniczne, a nie geopolityczną charakterystykę dostawcy. Przepisy w tym zakresie powinny być wyjątkowo precyzyjne, a procedura oparta o obiektywne merytoryczne kryteria z uwzględnieniem skutków dla konkurencyjności rynku, kosztów wdrożenia etc., w celu uniknięcia zarzutu dyskryminacji.	**Uwaga nieuwzględniona** Kryteria oceny opisane w Toolbox 5g są techniczne i nietechniczne.
10.	Konfederacja Lewiatan	Uwaga ogólna	8. Ocenę sprzętu i oprogramowania należy przeprowadzać według obowiązujących przepisów ustawy Kodeksu postępowania administracyjnego oraz ustawy Prawo przedsiębiorców. Koniecznym jest stosowanie przejrzystych zasad, umożliwiających aktywny udział dostawcy w postępowaniu oraz zapewnienie procedury odwoławczej, w tym prawo weryfikacji decyzji przez sądy administracyjne	**Uwaga uwzględniona** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.

11.	Konfederacja Lewiatan	Uwaga ogólna	9. Przeprowadzenie ewentualnej oceny powinno zostać powierzone wyspecjalizowanemu organowi regulacyjnemu, który dysponuje odpowiednimi kompetencjami i zasobami tj. np. Prezes Urzędu Komunikacji Elektronicznej.	
12.	Konfederacja Lewiatan	Uwaga ogólna	10. Z uwagi na dotychczasowe doświadczenia operatorów usług kluczowych (OUK) przedstawiamy propozycje modyfikacji proponowanych zasad realizacji obowiązków OUK, w szczególności poprzez dopuszczenie innych form organizacyjnych niż wyodrębniony SOC. W naszej ocenie taka elastyczność, w tym w zakresie możliwości realizacji zadań w strukturze rozproszonej, gdzie SOC jest jedynie jej częścią jest kluczowa dla OUK realizujących zadania własnymi siłami. Natomiast OUK, którzy korzystają z usług zewnętrznych powinni mieć możliwość ich realizacji w modelu mieszanym, tj. wykorzystania struktury wewnętrznej oraz zamawiania na zewnątrz jedynie części usług niezbędnych dla kompleksowej ochrony usługi kluczowej.	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny.

				Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. Art. 14 ust. 3 wskazuje wprost, że SOC wprowadza zabezpieczenia zapewniające poufności,

				integralność, dostępność i autentyczność przetwarzanych informacji. Zabezpieczenia te wynikają z przeprowadzonego szacowania ryzyka. Przyjęte założenie jest oparte o koncepcję *risk based approach*.
13.	Konfederacja Lewiatan	Uwaga ogólna	Dalsze konsultacje projektu. Uwzględniając zakres podmiotów, na jakie może wpływać projektowana ustawa (wszystkie podmioty KSC) należy przygotować pełną listę interesariuszy i umożliwić ich rzeczywisty udział w konsultacjach, w tym obejmując w szczególności: organizacje samorządów terytorialnych, organizacje przedsiębiorców reprezentujących wszystkie kategorie operatorów usług kluczowych, organizacje konsumentów, instytucje odpowiedzialne za ochronę konkurencji i konsumenta, Radę Dialogu Społecznego. Zwracamy się również z uprzejmą prośbą o zorganizowanie przez Ministerstwo konferencji uzgodnieniowej oraz zaproszenie do udziału wszystkich interesariuszy, którzy wnieśli swoje uwagi. Nasze uwagi wynikają z faktu, że po wnikliwej analizie projektu zauważamy, że występują w nim pewne braki zarówno w warstwie merytorycznej, celowościowej, jak i techniczno-legislacyjnej skłaniają do jego krytycznej oceny. W pierwszej kolejności należy odnotować następujące kwestie: zakres zmian, ich wyraźne kolizje lub powielanie dotychczasowych regulacji (w tym tych dopiero projektowanych w ramach Prawa Komunikacji Elektronicznej), brak niezbędnej precyzji, lakoniczne uzasadnienie oraz pomijająca kluczowe zagadnienia Ocena Skutków Regulacji; budzące wątpliwości pod kątem proporcjonalności nowe, niemal kierownicze uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa czy Kolegium, a także brak rozważenia rozwiązań alternatywnych oraz brak oszacowania kosztów finansowych i organizacyjnych, które miałyby zostać poniesione w niezwykle krótkim czasie przez przedsiębiorców. Należy także odnotować, że wbrew uzasadnieniu projektu przedłożony projekt nie jest niezbędny dla	**Wyjaśnienie** Wszyscy interesariusze mogli wypowiedzieć się w ramach konsultacji publicznych.

			implementacji Europejskiego Kodeksu Łączności Elektronicznej (EKŁE), a może wręcz bardzo skomplikować terminowe wprowadzenie i wdrożenie Prawa Komunikacji Elektronicznej, które w swoim projekcie, co do zasady kompleksowo adresuje wszystkie wymagania dot. bezpieczeństwa, jakie wynikają z EKŁE. Jako uważni obserwatorzy obszaru polityki publicznej oraz legislacji, w zakresie m.in. bezpieczeństwa mamy oczywiście świadomość, że przedstawiony projekt ustawy jest realizacją unijnego „5G Toolbox", w zakresie mechanizmu oceny bezpieczeństwa rozwiązań dostawców dla sieci 5G. Projekt wydaje się jednak wykraczać poza ten zakres, co w zakresie samego mechanizmu oceny dostawców, oznacza, że nie ma on dotyczyć obszaru określonej kategorii sieci telekomunikacyjnej, ale wszystkich obszarów wchodzących do krajowego systemu cyberbezpieczeństwa. Tym samym, potencjalnie oceny takie mogłyby dotyczyć wszelkich dostawców, w tym z sektorów kluczowych w rozumieniu KSC tj. energii, transportu, bankowości i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej. Co więcej, skala zaproponowanych do pilnego wdrożenia reform, a szczególnie wzmocnienia uprawnień administracji publicznej i krajowych CSIRT zaskakuje szczególnie, że dotychczas jedną z kluczowych barier w sprawnym wdrażaniu ustawy KSC był faktyczny brak wystarczających kadr mających się zajmować w sektorze publicznym cyberbezpieczeństwem, a sytuacja w tym zakresie nie uległa w ostatnim okresie istotnej poprawie. System przeznaczony do współpracy jednostek w ramach krajowego systemu cyberbezpieczeństwa zgodnie ze Strategią Cyberbezpieczeństwa RP na lata 2019- 2024 ma dopiero zostać uruchomiony od 2021 r., a w ramach planowanych projektów UE, MC zakłada finansowanie ze środków publicznych wielu projektów z obszaru cyberbezpieczeństwa, które mają służyć budowie potencjału administracji. Jednocześnie, takich jak przewidziane w projekcie ustawy zmian nie zakłada wprost wspomniana Strategia Cyberbezpieczeństwa RP na lata 2019-2024. Dyrektywa NIS, która była podstawą dla ustawy KSC jest dopiero w toku szczegółowej rewizji. Jednocześnie przygotowanie do planowanych zmian wymagało będzie istotnych nakładów finansowych po stronie administracji już od momentu wejścia nowej ustawy w życie. Tymczasem środki finansowe na pokrycie	

			nowych zadań po stronie administracji publicznej zaplanowano dopiero od 2022 r., a oszacowania kosztów po stronie sektora prywatnego niestety nawet nie próbowano w OSR podjąć. Postulujemy zabezpieczenie środków finansowych na pokrycie zadań administracji publicznej w tym zakresie od 2021 r., a w przypadku braku takiej możliwości opóźnić wejście w życie ustawy do czasu kiedy faktyczna realizacja zadań będzie mogła być wykonywana. Na obecnym etapie, należałoby zrezygnować w projekcie z przepisów dotyczących objęcia przedsiębiorców komunikacji elektronicznej nowymi obowiązkami w ramach ustawy o krajowym systemie cyberbezpieczeństwa, w tym w zakresie włączenia ich do krajowego systemu cyberbezpieczeństwa oraz wprowadzenia nowego reżimu raportowego w zakresie incydentów, który miałby zostać wprowadzony mimo, że istnieje już właściwy dla takich podmiotów kanał raportowania do Prezesa Urzędu Komunikacji Elektronicznej. Właściwy tryb w tym zakresie został już przedstawiony w projekcie PKE, a jego ewentualne rozszerzenie wymaga pogłębionej dyskusji i czasu.	
14.	Konfederacja Lewiatan	Uwaga ogólna	Stanowisko w zakresie nowych obowiązków przedsiębiorców komunikacji elektronicznej. Projektowane przepisy rozdziału 4a, a także związany z nimi nowy art. 1, definicje oraz zamiar powołania CSIRT Telco stanowią propozycję pilnego wprowadzenia zupełnie nowego reżimu prawnego i organizacyjnego funkcjonowania przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa. Koncepcja ta zdaje się przy tym pomijać obiektywny fakt, że sektor ten jest i tak znacząco obciążony z uwagi na najpierw opóźnione, a ostatnio prowadzone w dużym tempie zmiany całego systemu prawnego w ramach przyjęcia nowego Prawa Komunikacji Elektronicznej, które, mimo, że wciąż jest na etapie prac rządowych, ma obowiązywać już od 21 grudnia br. Analiza przedłożonego projektu oraz uzasadnienia w tym zakresie wskazuje, że głównym celem i identyfikowanym brakiem jest deficyt odpowiedniej informacji o incydentach dotyczących komunikacji elektronicznej po stronie CSIRT krajowych oraz operatorów usług kluczowych. Takie wnioski są o tyle zastanawiające, że już dzisiaj w reżimie prawnym Prawa telekomunikacyjnego, przedsiębiorca telekomunikacyjny jest zgodnie z art. 175a ust. 1 obowiązany niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy

			lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych. Jednocześnie, w celu zapewnienia odpowiednich informacji dla podmiotów krajowego systemu cyberbezpieczeństwa, zgodnie z art. 175a ust. 1a dodanym właśnie ustawą o krajowym systemie cyberbezpieczeństwa z 2018 r., obowiązkiem Prezesa UKE, jest przekazywanie informacji o naruszeniach, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego. Co więcej, Prezes UKE ma możliwość korzystania z systemu informatycznego tworzonego na potrzeby krajowego systemu cyberbezpieczeństwa (art. 46 KSC). Konsultowany już projekt PKE utrzymuje te kluczowe rozwiązania i to one powinny być w pierwszej kolejności rozważane. Oznacza to, że już istnieje mechanizm raportowania i przekazywania informacji o incydentach w obszarze telekomunikacji, które mają wpływ na cyberbezpieczeństwo. Jeśli ten mechanizm nie funkcjonuje zgodnie z oczekiwaniami, należy rozważyć jego dostosowanie, a nie wprowadzanie drugiego, na poziomie przepisów potencjalnie zbliżonego mechanizmu raportowania przedsiębiorców do CSIRT. Zauważamy jednocześnie, że między definicjami incydentów w obu projektach występują istotne różnice, które nie pozwalają uznać, że mowa jest o identycznym zakresie raportowania. Takie działanie jest w naszej ocenie niezgodne m.in. z art. 67 pkt 1, 2 i 3, a przynajmniej częściowo także z art. 68 ustawy – Prawo przedsiębiorców, które nakazują, aby opracowując projekt aktu normatywnego określającego m.in. wykonywania działalności gospodarczej (a tego przepisy KSC dotyczą) kierować się zasadami proporcjonalności i adekwatności, a w szczególności dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągnięcia ich celów; dążyć do ograniczenia obowiązków informacyjnych, zwłaszcza, gdy wymagane informacje są przekazywane przez obowiązanych organom władzy publicznej na podstawie obowiązujących przepisów; implementując prawo Unii Europejskiej i prawo międzynarodowe, dążyć do nakładania wyłącznie obowiązków administracyjnych niezbędnych do osiągnięcia celów implementowanych przepisów. Tymczasem uzasadnienie i OSR ograniczają się jedynie do stwierdzeń, że przedsiębiorcy komunikacji	komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE. Dlatego potrzebne jest przeniesienie odpowiednich

			elektronicznej zostaną włączeni do KSC oraz otrzymają wsparcie CSIRT (o które według wiedzy naszej organizacji nie wnioskowali). Jednocześnie, niezrozumiałe, przynajmniej z uwagi na brak wcześniejszej dyskusji w tym temacie, są zawarte w OSR sformułowania wskazujące, że raportowanie przedsiębiorców telekomunikacyjnych miałoby odbywać się do CSIRT zamiast do UKE. Jakkolwiek utrzymanie jednego, podstawowego kanału komunikacji jest postulowanym rozwiązaniem, tak jednak CSIRT są podmiotami wyspecjalizowanymi w zakresie cyberbezpieczeństwa i nie są w naszej ocenie właściwe do zastąpienia UKE w realizacji zadań odnośnie całego obszaru bezpieczeństwa i integralności usług i infrastruktury telekomunikacyjnej, które dalece przekraczają same kwestie cyberbezpieczeństwa. System współpracy z UKE w tym zakresie jest ugruntowany od lat i jedyną dodatkową kwestią, jaka mogłaby zostać w tym zakresie dopracowana to ew. sposób kwalifikowania przez UKE naruszeń/incydentów jako takich, które są incydentami w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa oraz sprawność ich przekazywania do CSIRT zgodnie z obowiązującymi już, i utrzymywanymi w projekcie PKE przepisami. Kwestie te, jak się wydaje powinny zostać jednak zorganizowane przez samą administrację i nie powinny wpływać na zakres obowiązków przedsiębiorców telekomunikacyjnych. Ponadto, zauważamy, że planowany do wprowadzenia do KSC zakres przepisów dot. bezpieczeństwa jest wybiórczy i kopiowane z projektu PKE przepisy nie tworzą spójnego systemu odpowiedzialności przedsiębiorców komunikacji elektronicznej wobec CSiRT (niebędących same w sobie organami administracji), a nie Prezesa UKE. Istotne wątpliwości wiążą się również z praktycznym aspektem raportowania, tj. brakiem aktów wykonawczych dot. określenia progów istotności oraz wzoru formularza raportowego. Jakkolwiek utrzymanie w mocy dotychczasowych rozporządzeń dotyczących raportowania wobec UKE zostało przewidziane w projekcie PKE, tak w przypadku przeniesienia/zdublowania tych obowiązków w KSC i w relacji z CSIRT nie do pominięcia jest fakt, że rozporządzeń tych dla tego kanału zgłoszeń nie będzie już w systemie prawnym. A biorąc pod uwagę zakres planowanych zmian w upoważnieniu do wydania rozporządzenia dot. progów istotności zmiany, jakie musiałoby wprowadzić nowe rozporządzenie, mogą okazać się w praktyce bardzo znaczące pozostawiając podmioty obowiązane w	definicji z PKE do ustawy KSC.

			poważnej niepewności co do kształtu przyszłych obowiązków jakie miałyby obowiązywać już od 21 grudnia br. Wyłączenie dostawców usługi interpersonalnej niewykorzystującej numerów z zakresu rozdziału 4a Zgodnie z rozdziałem 4a pt. „obowiązki przedsiębiorców komunikacji elektronicznej" przedsiębiorcy komunikacji elektronicznej mają stać się częścią krajowego systemu cyberbezpieczeństwa. Należy zwrócić uwagę, że podmiotem obowiązków wskazanych w tym rozdziale jest „przedsiębiorca komunikacji elektronicznej". Tym samym projektowana ustawa o KSC odwołuje się w zakresie definicyjnym do pojęcia przedsiębiorcy telekomunikacyjnego z projektu ustawy o PKE, wedle którego zob. art. 2 pkt 41 projektu PKE) przedsiębiorca komunikacji elektronicznej to przedsiębiorca telekomunikacyjny lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów. Z kolej usługa komunikacji interpersonalnej niewykorzystująca numerów oznacza usługę umożliwiającą bezpośrednią interpersonalną i interaktywną wymianę informacji za pośrednictwem sieci telekomunikacyjnej między skończoną liczbą osób, gdzie osoby inicjujące połączenie lub uczestniczące w nim decydują o jego odbiorcy lub odbiorcach, z wyłączeniem usług, w których interpersonalna i interaktywna komunikacja stanowi wyłącznie funkcję podrzędną względem innej usługi podstawowej, w tym usługę, która nie umożliwia realizacji połączeń z numerami z planu numeracji krajowej lub międzynarodowych planów numeracji (art. 2 pkt 77 projektu PKE). Innymi słowy to ostatnie pojęcie oznacza usługę np. poczty elektronicznej czy czatów internetowych. Świadczy o tym choćby motyw 17 zd. 1 EKŁE, który wyraźnie wskazuje, że usługi łączności interpersonalnej obejmują wszystkie rodzaje poczty elektronicznej: „Usługi łączności interpersonalnej są to usługi, które umożliwiają interpersonalną i interaktywną wymianę informacji, obejmujące takie usługi, jak tradycyjne połączenia głosowe między dwiema osobami, lecz również wszystkie rodzaje poczty elektronicznej, usług przekazywania wiadomości lub czatów grupowych". Z powyższego wynika, że wykorzystanie w nowelizacji ustawy o KSC terminu „przedsiębiorcy komunikacji elektronicznej" powoduje, iż wskazane, obszerne i uciążliwie obowiązki będą musiały być stosowane także przez np. dostawców poczty elektronicznej. Takie podejście nie znajduje jednak uzasadnienia w charakterystyce usługi poczty	

			elektronicznej, która w zasadniczy sposób różni się od usługi telekomunikacyjnej. Niewątpliwie przepisy ustawy o KSC uwzględniając regulacje zawarte w EKŁE powinny w odmienny sposób traktować dostawców usług lub sieci telekomunikacyjnych oraz dostawców usług łączności interpersonalnej niewykorzystującej numerów. Takie stanowisko jest zgodne z motywem 95 EKŁE: „Z uwagi na rosnące znaczenie usług łączności interpersonalnej niewykorzystujących numerów należy zapewnić aby podlegały one również odpowiednim wymogom bezpieczeństwa zgodnie z ich specyficznym charakterem i istotną rolą w gospodarce. Dostawcy usług powinni również zapewnić poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Ze względu na to, że dostawcy usługi interpersonalnej łączności niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach, stopień ryzyka w przypadku takich usług można uznać za niższy pod pewnymi względami niż w przypadku tradycyjnych usług łączności elektronicznej. Dlatego też, jeżeli tylko jest to uzasadnione aktualną oceną ryzyka dla bezpieczeństwa, środki podejmowane przez dostawców usługi interpersonalnej łączności niewykorzystujące numerów powinny być łagodniejsze. Takie samo podejście powinno być stosowane odpowiednio do usług łączności interpersonalnej wykorzystującej numery, jeżeli dostawca nie sprawuje rzeczywistej kontroli nad transmisją sygnału”. Planowane w KSC regulacje nie powinny naruszać zasad wynikających z dyrektywy EKŁE, ponieważ całkowicie nieuzasadnione jest zrównywanie obowiązków w zakresie bezpieczeństwa sieci i usług dla wszystkich przedsiębiorców komunikacji elektronicznej, jeśli ich realny wpływ na wskazane bezpieczeństwo jest całkowicie różne. Co więcej, nałożenie na rodzimych dostawców wskazanych usług (np. poczty elektronicznej) dodatkowych obowiązków może naruszyć zasady konkurowania lokalnych dostawców z globalnymi graczami. Więcej, nałożenie na tych ostatnich szeregu nowych obowiązków będzie wymagało istotnego zwiększenia zatrudnienia, jak i doprowadzi do wzrostu innego rodzaju obciążeń, co w ostatecznym rezultacie może sprawić, że działalność wielu dostawców poczty elektronicznej może po prostu nie sprostać rachunkowi ekonomicznemu takiej działalności. Na marginesie, projekt KSC nie harmonizuje z projektem PKE. Dla przykładu, art. 20c ustawy o KSC przywołuje pojęcie	

			„przedsiębiorcy komunikacji elektronicznej”, o którym mowa w art. 47 ust. 1 projektu PKE. Jednakże wskazany przepis PKE odnosi się wyłącznie do przedsiębiorcy telekomunikacyjnego, który nie wyczerpuje całości kategorii „przedsiębiorców komunikacji elektronicznej”. Z tych względów postulujemy: 1) Usunięcie przepisów dot. włączenia przedsiębiorców komunikacji elektronicznej do KSC. 2) Przywrócenie wyłączenia przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania z obowiązków dot. bezpieczeństwa oraz zgłaszania incydentów. 3) Usunięcie Rozdziału 4a art. 20a-20f pt. „obowiązki przedsiębiorców komunikacji elektronicznej”, a także związanych z tymi obszarami definicji oraz zamiaru wprowadzenia CSIRT Telco. 4) Dyskusję na temat możliwości usprawnienia aktualnego systemu pod kątem potrzeb podmiotów KSC, w sposób, który nie będzie skutkował dodatkowymi obowiązkami przedsiębiorców oraz nie będzie rewolucjonizował w przyspieszony sposób dotychczasowego modelu działania. W naszej ocenie tak doniosłe zmiany nie powinny być wprowadzone bez dogłębnej i rzeczowej dyskusji z ich głównymi adresatami, a na pewno nie w zaproponowanym trybie i terminach. 5) Ponadto podtrzymujemy uwagi przedstawione w toku konsultacji PKE w zakresie przepisów, które zostały powtórzone w projekcie nowelizacji ustawy KSC. Usunięcie z projektu ustawy zakładanych zmian dotyczących włączenia przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa, usunięcie wyłączenia przedsiębiorców telekomunikacyjnych oraz dostawców usług zaufania z przewidzianych w ksc przepisów dot. bezpieczeństwa i zgłaszania incydentów, dodania nowego rozdziału 4a. dotyczącego obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa, a także związanych z tymi obszarami definicji oraz zamiaru wprowadzenia CSIRT Telco. W naszej ocenie tak doniosłe zmiany nie powinny być wprowadzone bez dogłębnej i rzeczowej dyskusji z ich głównymi adresatami, a na pewno nie w zaproponowanym trybie i terminach.	
15.	Konfederacja Lewiatan	Uwaga ogólna	W zakresie proponowanego modelu oceny bezpieczeństwa dostawców urządzeń lub oprogramowania, zakładamy, że proponowane rozwiązanie ma stanowić wdrożenie rekomendacji wynikających z tzw. „5G Security Toolbox”. Jednocześnie jednak należy brać pod uwagę, że skutki wydawanych ocen mogą	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione.

			de facto oznaczać wykluczenie wymiany handlowej między polskimi przedsiębiorstwami, a określonymi w ocenie dostawcami. W tym zakresie oceniamy także, że proponowane rozwiązania wydają się być bardziej restrykcyjne niż te, które rekomendowane są na poziomie UE. W naszej ocenie, projekt wymaga precyzyjnej oceny i rewizji pod kątem spełnienia podstawowych wzorców konstytucyjnych wywodzonych z kluczowej zasady demokratycznego państwa prawa, przepisów ustawy Prawo przedsiębiorców, a także obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Podobne obawy wiążą się z zachowaniem zasad przepisów unijnych na poziomie TFUE, dyrektywy o konkurencji, zasad swobodnego przepływu towarów czy zasady niedyskryminacji. Istotnym argumentem, który należy podnieść jest kwestia obowiązku notyfikacji uregulowanego na poziomie prawa krajowego w Rozporządzeniu Rady Ministrów z dnia 23 grudnia 2002 r. (w szczególności w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych). Przedmiotowy obowiązek jest także uregulowany w Dyrektywie 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego. Wreszcie, wątpliwości budzi zgodność z zasadami przyjętymi na poziomie WTO. Na tym etapie jednak nie przedstawiamy uszczegółowionego stanowiska w tym zakresie, zakładając, że w toku merytorycznego dialogu uda się wypracować rozwiązania, które będą racjonalne i służące faktycznej poprawie poziomu cyberbezpieczeństwa w Polsce. Wskazujemy jedynie, że z uwagi na istotne ryzyka, tak dla przedsiębiorców jak i budżetu państwa, przepisy w tym zakresie muszą być wyjątkowo precyzyjne, a procedura oparta o obiektywne, merytoryczne kryteria. Przede wszystkim jednak uważamy, że efektywne podejście do zwiększenia poziomu cyberbezpieczeństwa w obszarze urządzeń i oprogramowania wymaga podejścia spójnego na poziomie przynajmniej Unii Europejskiej, jeśli nie globalnym. Naszym zdaniem tym celom będą prawidłowo służyć opracowywane obecnie schematy certyfikacji europejskiej bazujące na	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie

			unijnym „Cybersecurity Act”. Już dzisiaj zapewnieniu bezpieczeństwa urządzeń służą narzędzia certyfikacyjne w ramach chociażby „Common Criteria”, Nesas czy same specyfikacje techniczne urządzeń, np. dla 5G przygotowywane przez 3GPP, które adresują już kwestie bezpieczeństwa. Dopiero po ich opracowaniu, wdrożeniu oraz zebraniu pierwszych doświadczeń, w tym wykryciu realnych zagrożeń, należałoby ewentualnie przejść do dalszych działań skutkujących wykluczaniem określonych podmiotów z rynku. Drugim aspektem jest fakt, że wdrażane obecnie przez poszczególne kraje europejskie rozwiązania nie są spójne, tj. posługują się różnymi narzędziami i kryteriami. Nie sprzyja to tworzeniu wspólnego potencjału w zakresie cyberbezpieczeństwa, a w przyszłości może generować niezbadane jeszcze problemy w warstwie technicznej interoperacyjności oraz konkurencji, szczególnie w przypadkach zastosować transgranicznych w stosujących różne podejście krajach sąsiednich. Stąd w pierwszej kolejności apelujemy o: Zintensyfikowanie prac na poziomie UE, w ramach, których precyzyjnie i klarownie powinno zostać określone wspólne podejście UE do kwestii bezpieczeństwa urządzeń i oprogramowania, które mają krytyczne znaczenie dla bezpieczeństwa. Oparcie planowanego do przyjęcia w Polsce mechanizmu oceny, o ocenę samych urządzeń i oprogramowania, a nie wyłącznie samych dostawców, w sposób bazujący na rzetelnych mechanizmach certyfikacji i oceny technicznej, w tym tj.: o NESAS: Określany wspólnie przez 3GPP i GSMA. Jest to dobrowolny program stosowany przez sektor telefonii komórkowej, zapewniający podstawowy i kompleksowy audyt bezpieczeństwa dowodzi, że sprzęt sieciowy spełnia wymogi bezpieczeństwa, a sprzedawcy sprzętu sieciowego – standardy bezpieczeństwa w procesie rozwoju produktów i cyklu życia. GSMA posiada radę akredytacyjną, która jest odpowiedzialna za monitorowanie i opracowywanie planów oraz udzielanie akredytacji. o ENISA: Unijne ramy certyfikacji bezpieczeństwa cybernetycznego mają na celu przyjęcie wspólnego podejścia i ustanowienie europejskich ram certyfikacji bezpieczeństwa cybernetycznego, które określają główne wymogi dla europejskich systemów bezpieczeństwa cybernetycznego i europejskich certyfikatów zgodności produktów ICT, usługi ICT lub procesów ICT, które mają być uznane i stosowane we wszystkich państwach członkowskich. Przyjęcie rozwiązań, które nie będą	prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty

			budziły wątpliwości w zakresie wymogów dotyczących dobrych praktyk legislacyjnych, jak i obowiązujących unijnych, umów międzynarodowych czy prawa krajowego. obowiązków przedsiębiorców komunikacji elektronicznej. Jednocześnie popieramy model szacowania ryzyka przez samego OUK b) Odnośnie zamiaru wprowadzenia obowiązku powołania SOC dla operatora usługi kluczowej w celu realizacji zadań operatora usługi kluczowej, w naszej ocenie rozwiązanie to nie odpowiada praktyce adresowania wymagań ustawy przez operatorów usług kluczowych. SOC to centrum operacyjne bezpieczeństwa. Wyraźne ograniczenie możliwości realizacji zadań tylko do takiej struktury byłoby realizowalne wyłącznie gdyby podmiot świadczący usługę kluczową miał tylko jedną usługę, byłaby nią usługa kluczowa, a jednocześnie byłaby ona związana wyłącznie z obszarem, na którego ciągłość może mieć wpływ zagrożenia cyberbezpieczeństwa (a nie np. katastrofa naturalna czy fizyczne uszkodzenie), a wszystkie zadania wynikające z KSC miałyby charakter operacyjny. Tymczasem działalność podmiotów będących operatorami usług kluczowych często daleko wykracza poza zakres usługi kluczowej. Jednocześnie działalność ta jest wielokrotnie realizowana w skali ogólnopolskiej. Tym samym infrastruktura i usługi są rozproszone. Jednocześnie rozproszone mogą być struktury bezpieczeństwa dla całej tej organizacji. W tym celu powoływane są wyspecjalizowane jednostki działające w obszarach analizy ryzyk, ciągłości działania, ochrony informacji, wykrywania incydentów, reakcji na nie itp.. W tym zakresie mogą być też powoływane SOC, które jednak są jedynie częścią większej struktury organizacyjnej w zakresie bezpieczeństwa. Tym samym to, czym w praktyce są istniejące już SOC nie odpowiada założeniom przedstawionym w nowelizacji. Skutkiem proponowanych zapisów byłoby natomiast wprowadzenie dodatkowego obciążenia w postaci konieczności powołania odrębnego SOC wyłącznie na potrzeby usługi kluczowej, co nie jest uzasadnione, ani z uwagi na troskę o bezpieczeństwo, ani koszty i efektywność. Tym samym, postulujemy utrzymanie dotychczasowego nazewnictwa tj. obowiązku powołania wewnętrznej struktury bezpieczeństwa lub zamówienia odpowiedniej usługi zewnętrznej w tym zakresie (także dla części zadań), która pozwala na zintegrowanie zabezpieczeń usługi kluczowej z istniejącymi już strukturami i	techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na

			procesami. Jednocześnie nie powinno być używane proponowane nazewnictwo (SOC), bowiem będzie mylące w świetle ugruntowanego już na rynku rozumienia zwrotu SOC. Zakres możliwości zamawiania usług zewnętrznych powinien być również uelastyczniony zgodnie z dalszymi postulatami. Ewentualnie należy wprowadzić dodatkowe zapisy wskazujące na możliwość realizacji zadań także w dotychczasowym trybie tj. poprzez wewnętrzną strukturę, która lepiej niż wydzielony SOC, odpowiada praktyce podejścia do zabezpieczenia usługi kluczowej, jako części większej działalności. c) Jeszcze dalej idące obawy wynikają z proponowanej konstrukcji art. 14 ust. 2, która w naszej ocenie będzie szkodliwa dla OUK, zarówno tych dobrze przygotowanych do swojej roli, jak i tych wciąż budujących ten potencjał. Przewidziano, bowiem tylko dwie możliwości tj. realizację zadań w ramach wewnętrznej struktury lub zamówienia całości usług, jako usług zewnętrznego „SOC". Pomijając już kwestie faktycznego znaczenia terminu SOC w świetle wymagań wskazanych w ustawie KSC, dla bardzo wielu praktycznych przypadków podstawowym i efektywnym modelem działania jest połączenie tych obu modeli tj. realizacja części zadań, w szczególności dotyczących działań typowo związanych z samą materią przedsiębiorstwa będącego OUK, w tym dot. bezpośrednio systemów odpowiedzialnych za usługę kluczową w ramach struktury wewnętrznej (przez istniejące już lub stworzone struktury bezpieczeństwa), a części zadań, jak np. tych związanych z wykrywaniem incydentów, monitorowaniem sieci oraz reakcją na cyberataki poprzez zamówienie usług zewnętrznych od wyspecjalizowanych podmiotów działających już na rynku. Taki model funkcjonuje już obecnie w praktyce. Co prawda, w redakcji przepisu użyto spójnika „lub", który jako alternatywa łączna może dopuszczać model mieszany, jednak faktyczna dopuszczalność takiego modelu, także w świetle dalszych przepisów dot. rejestru „SOC" dających kompleksową obsługę budzi nasze bardzo poważne wątpliwości. W naszej ocenie aktualny kształt rynku rozwiązań cyberbezpieczeństwa pozwala stwierdzić, że nie istnieją, lub bardzo ograniczona jest dostępność podmiotów, które mogłyby na wysokim poziomie jakości zapewnić OUK kompleksową, zewnętrzną obsługę w zakresie wszystkich jego zadań. W tym zakresie niezbędne byłoby powoływanie wielostronnych konsorcjów złożonych z podmiotów o różnych specjalizacjach, w których	wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3. W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie

			dodatkowo niezbędny byłby koordynator całości zadań. Brak odpowiedniego poziomu konkurencji na rynku w tym zakresie skazywałby jednocześnie OUK na korzystanie wyłączenie z bardzo drogich i „szytych na miarę" rozwiązań lub stwarzał ryzyko powstawania podmiotów, które dopiero na bazie nawiązanej z OUK relacji uczyłyby się zarządzania całością tej materii. Jednocześnie poważnie ograniczona, ze szkodą dla samych OUK, byłaby możliwość elastycznego zarządzania zamawianiem na zewnątrz realizacji tylko wybranych zadań. Z tych względów postulujemy nadanie przepisom kształtu dopuszczającego wyraźnie zamawianie przez OUK wybranych i wynikających z faktycznych potrzeb usług w zakresie realizacji zadań wskazanych w KSC, a nie tylko całości obsługi w ramach zewnętrznego „SOC". Odpowiednich modyfikacji, w przypadku ich utrzymania, wymagałyby też przepisy dot. rejestru, które powinny dopuszczać wpisywanie również podmiotów, które są wyspecjalizowane w określonych obszarach świadczenia usług dla OUK. d) W art. 14 ust. 5 należy doprecyzować, że zakres dostępu nie może naruszać tajemnic prawnie chronionych, w tym tajemnic przedsiębiorstwa świadczącego usługi na rzecz OUK. 2) życie zwrotu SOC, który nie jest zarezerwowany wyłącznie dla operatorów usług kluczowych czy podmiotów świadczących na ich rzecz usługi, ma swoje konsekwencje także w zakresie dalszych przepisów projektowanej ustawy, które w naszej ocenie wymagają następujących poprawek: a) W art. 14 ust. 6 aktualnie sformułowany obowiązek może być rozumiany tak, że każdy prowadzony w P podczas gdy jak zakładamy intencją było jedynie wprowadzenie obowiązku ogłaszania informacji o możliwości i potencjale podmiotu, który chce i może świadczyć tego typu usługi na rzecz operatorów usług kluczowych. Zapisy w tym zakresie należy więc przeredagować. b) W art. 14a dotyczącym prowadzenia rejestru SOC, należy odpowiednio zmodyfikować to odwołanie, aby nie mogło dotyczyć wszystkich SOC, ale jedynie podmiotów świadczących określone usługi na rzecz operatorów usług kluczowych. W ust. 3 należy odwołać się do art. 14 ust. 4, a nie do art. 14 ust. 2, bowiem to ust. 4 oznacza obowiązek przekazania informacji o zawarciu umowy z podmiotem zewnętrznym organowi właściwemu. c) W zakresie art. 14a ust. 7 wątpliwości budzi czy przesłanki wpisania z urzędu (jak rozumiemy na wniosek „SOC") mają być rozumiane łącznie, a dodatkowo w naszej ocenie nie jest uzasadnione tworzenie	sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za

			dodatkowych wymagań wobec podmiotów wpisywanych z urzędu/na wniosek wobec podmiotów, które po prostu zawarły umowę z OUKolsce SOC miałby podlegać obowiązkowi ogłoszenia na stronie internetowej,	dostawców wysokiego ryzyka. Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko

				kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego szacowania ryzyka przez operatora usługi kluczowej. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1. Art. 14 ust. 3 wskazuje wprost, że SOC wprowadza zabezpieczenia zapewniające poufności, integralność, dostępność i autentyczność

				przetwarzanych informacji. Zabezpieczenia te wynikają z przeprowadzonego szacowania ryzyka. Przyjęte założenie jest oparte o koncepcję risk based approach.
16.	Akademia Sztuki Wojennej	Art. 1 punkt 1 lit. a (art. 1 ust. 1 pkt 4 uKSC)	a) w ust. 1 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu: „4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej, o których mowa w ustawie z dnia ... – Prawo komunikacji elektronicznej (Dz. U. ...), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;" Projekt zakłada wprowadzenie do ustawy z dnia o Krajowym Systemie Cyberbezpieczeństwa (dalej jako uKSC) regulacji dotyczących obowiązków operatorów telekomunikacyjnych oraz dostawców usług zaufania z zakresu zapewnienia cyberbezpieczeństwa, co jest sprzeczne z dyrektywą Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS) (dalej jako dyrektywa NIS). Zgodnie z art. 1 tej dyrektywy regulacje dotyczące bezpieczeństwa i zgłaszania incydentów nie mają zastosowania do przedsiębiorstw telekomunikacyjnych, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywa ramowa) , ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającej dyrektywę 1999/93/WE . W związku z tym właściwymi aktami prawnymi do regulacji tych kwestii jest ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (dalej jako PT), a w przyszłości – ustawa Prawo o komunikacji elektronicznej; dalej jako PKE, mająca implementować postanowienia Kodeksu Łączności Elektronicznej - dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej

			2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (dalej jako KŁE). W związku z powyższym – przepis ten nie powinien znaleźć się w ustawie.	mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
17.		Art. 1 pkt 1 litera b (art 1 ust. 2 pkt 1 i 2u KSC)	Art. 1. b) w ust. 2 uchyla się pkt 1 i 2; „Art. 1. (…) 2. Ustawy nie stosuje się do: 1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz.U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875), w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów; 2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc

			sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257 z 28.08.2014, str. 73)" W związku z tym, co zostało napisane wyżej, przepisy art 1 ust. 2 pkt 1 i 2 uKSC, przewidujące wyłączenie z zakresu podmiotowego uKSC operatorów telekomunikacyjnych oraz dostawców usług zaufania powinny zostać zachowane.	poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa

				sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
18.		**Art. 1 pkt 2 litera a projektu (art. 2 pkt 3b uKSC)**	po pkt 3 dodaje się pkt 3a-3e w brzmieniu „3b) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej;” przepisy **art 1 ust. 2 pkt 1 i 2 uKSC, przewidujące wyłączenie z zakresu podmiotowego uKSC** operatorów telekomunikacyjnych oraz dostawców usług zaufania powinny zostać zachowane.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego

				świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
19.		Art. 1 pkt 2 litera b projektu (art. 2 pkt 8a KSC)	po pkt 8 dodaje się pkt 8a-8g w brzmieniu: „8a) incydent telekomunikacyjny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi komunikacji elektronicznej;” Wprowadzenie kolejnego rodzaju incydentu (incydentu telekomunikacyjnego) może doprowadzić do dalszych problemów z klasyfikacją incydentów. Na marginesie - nie wyodrębniono specjalnych kategorii incydentów dla innych sektorów.	**Wyjaśnienie** Jest to szczególny rodzaj incydentu związany z telekomunikacją. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc

				poprzez ustawę wprowadzającą PKE.
20.		Art. 1 pkt 4 litera a projektu (art. 4 pkt 2a i 5a uKSC:	„w art. 4: a) po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) przedsiębiorców komunikacji elektronicznej;”, b) po pkt 5 dodaje się pkt 5a w brzmieniu: „5a) CSIRT Telco;”, Przepisy te wiążą się z obowiązkami przedsiębiorców telekomunikacyjnych, w związku z czym nie ma dla nich miejsca w ustawie o KSC.	**Uwaga nieuwzględniona** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług

				kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
21.	Konfederacja Lewiatan	Art. 14	1) Art. 14 dot. obowiązku powołania SOC: a) W pierwszej kolejności zauważamy uwzględnienie zgłaszanego przez stronę społeczną postulatu, aby warunki techniczne i organizacyjne były ustalane na podstawie analizy ryzyka przeprowadzonej indywidualnie dla konkretnego operatora usług kluczowych. Nie sposób jednak nie zauważyć – co może być też refleksją dla planowanych obecnie zmian - że dwukrotnie wprowadzane rozporządzenia dot. warunków technicznych i organizacyjnych spowodowały już konieczność ponoszenia dodatkowych kosztów, które w normalnych uwarunkowaniach nie byłyby konieczne. Aktualna refleksja wskazująca, że rozporządzenie do art. 14 ust. 4 KSC w związku z usunięciem upoważnienia ustawowego byłoby uchylone, powinna być naszym zdaniem ostrzeżeniem przed tak daleko idącym jak planowane regulowaniem	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury

				odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Definicja SOC odnosi się do wieloletniej praktyki rynkowej, a skrót jest powszechnie rozpoznawalny. Wskazane w uwadze zakres działania SOC to nie tylko kwestie operacyjne czyli wykrywanie i reagowanie na incydenty lecz także zarządzanie jakością zabezpieczeń systemów, informacji powierzonych aktywów oraz aktualizowanie ryzyk, które mogą wpłynąć na reakcję na incydent. SOC zarządza kwestiami bezpieczeństwa w tym bezpieczeństwa osobowego, eksploatacji i architektury systemów na podstawie wyników przeprowadzonego

				szacowania ryzyka przez operatora usługi kluczowej.
22.	Akademia Sztuki Wojennej	Art. 1 pkt 12 projektu (rozdział 4a- art. 20a-20f uKSC)	Przepisy rozdziału 4a miałyby regulować obowiązki przedsiębiorców komunikacji elektronicznej (z uwagi na objętość rozdziału zrezygnowano z cytowania planowanych przepisów, zwłaszcza, że dla jasności opinii w tym zakresie nie jest to niezbędne). Jak była mowa na wstępie ,powinny się znaleźć w ustawie Prawo komunikacji elektronicznej, w szczególności, że częściowo się **pokrywają – por.** art. 20a opiniowanego projektu z z art. 39 projektu z dnia 29 lipca 2020 ustawy – Prawo komunikacji elektronicznej, przepisy art. 20e – przepisów art. 42 ust. 2 i 3 projektu ustawy – Prawo komunikacji elektronicznej, a przepis art. 20f – przepisu art. 44 ust. 1 projektu ustawy – Prawo komunikacji elektronicznej. Z kolei w art. 20a ust. 4 znajduje się delegacja dla ministra właściwego do spraw informatyzacji **identyczna** jak delegacja z art. 39 projektu ustawy – Prawo komunikacji elektronicznej. Analogiczna sytuacja ma miejsce w przypadku art. 20c ust. 4 omawianego projektu i art. 42 ust. 2 projektu ustawy – Prawo komunikacji elektronicznej.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców

				usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
23.	Akademia Sztuki Wojennej	Art. 1 pkt 29 projektu (art. 66a ust. 2-3 uKSC)	„2. Wniosek o sporządzenie oceny zawiera wskazanie: 1) danych identyfikujących dostawcę sprzętu lub oprogramowania; 2) możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. 3. Wniosek o sporządzenie oceny może określać: 1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub, 2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa - które uwzględnia się przy sporządzeniu oceny sprzętu lub oprogramowania.” Przy ocenie bezpieczeństwa sieci oraz usług powinien być przede wszystkim oceniany sprzęt, a nie przedsiębiorcy go dostarczający. Stąd należy zastąpić w powyższym przepisie odwołania do dostawcy, odwołaniami do sprzętu i oprogramowania. „2. Wniosek o sporządzenie oceny zawiera wskazanie:	**Uwaga nieuwzględniona** Przepisy nawiązują do Toolbox 5G, w którym to ocena ryzyka ma dotyczyć także aspektów nietechnicznych.

			1) danych identyfikujących dostawcę sprzętu lub oprogramowania; 2) możliwych obszarów działalności, w których ~~dostawca sprzętu lub oprogramowania~~ sprzęt lub oprogramowanie może stanowić zagrożenie dla bezpieczeństwa narodowego. 3. Wniosek o sporządzenie oceny może określać: 1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub, 2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa - które uwzględnia się przy sporządzeniu oceny ~~dostawcy~~ sprzętu lub oprogramowania.”	
24.	Akademia Sztuki Wojennej	Art. 1 pkt 29 projektu (art. 66a ust. 4 uKSC)	Proponowany art. 66a ust. 4 „W sporządzania oceny przeprowadza się w szczególności: 1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania; 2) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą: a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem, d) strukturę własnościową dostawcy sprzętu lub oprogramowania, e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;” Po pierwsze należy zmodyfikować pkt 1, bo jak wskazano wyżej - pod kątem zagrożeń należy ocenić sprzęt i oprogramowanie. Po drugie, interpretacja treści punktu 2 budzi szereg wątpliwości, związanych z użyciem szeregu nieostrych, niedookreślonych zwrotów– „wpływ”, „znajdować się pod wpływem”, „prawdopodobieństwo” (jak je określić? Powyżej jakie progu	**Uwaga częściowo uwzględniona** Przepisy nawiązują do Toolbox 5G, w którym to ocena ryzyka ma dotyczyć także aspektów nietechnicznych. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy

			dyskwalifikuje dostawcę?), „zdolność ingerencji państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania”. Dyskusyjne jest również podnoszenie kwestii oceny „prawodawstwa tego państwa w zakresie ochrony praw obywatelskich i praw człowieka” ze względu na ogólność, a co za tym idzie możliwość bardzo szerokie interpretacji. Po drugie, jak powszechnie wiadomo – państwo może z jednej strony w aktach prawnych gwarantować wysoki poziom ochrony praw człowieka i praw obywatelskich, a jednocześnie nie zapewniać skutecznych mechanizmów ich ochrony. Odnosząc się do kwestii weryfikacji dostawcy sprzętu i oprogramowania można sięgnąć do rozwiązań przyjętych w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych dotyczących przedsiębiorców zamierzających ubiegać się albo ubiegających się o zawarcie umów związanych z dostępem do informacji niejawnych lub wykonujących takie umowy albo wykonujących na podstawie przepisów prawa zadania związane z dostępem do informacji niejawnych. Zgodnie z art. 57 ust. 2 sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, obejmuje: 1) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową; 2) strukturę organizacyjną; 3) system ochrony informacji niejawnych, w tym środki bezpieczeństwa fizycznego; 4) wszystkie osoby wchodzące w skład organów zarządzających, kontrolnych oraz osoby działające z ich upoważnienia; 5) w szczególnie uzasadnionych przypadkach osoby posiadające poświadczenia bezpieczeństwa. W związku z powyższym wydaje się, że skoro wyżej wskazany zakres weryfikacji został przez ustawodawcę uznany za wystarczający przy dopuszczeniu przedsiębiorców do dostępu do informacji niejawnych, w przypadku dostawców sprzętu i oprogramowania powinno postąpić analogicznie, uzupełniając jednak o badanie regulacji w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,	dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka.

			„4. W sporządzania oceny przeprowadza się w szczególności: 1) analizę zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, kontrwywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi ~~dostawca sprzętu i oprogramowania~~ sprzęt i oprogramowanie; ~~2) prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą:~~ ~~a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem,~~ ~~b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka,~~ ~~c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,~~ ~~d) strukturę własnościową dostawcy sprzętu lub oprogramowania,~~ ~~e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;”~~ 2) sprawdzenie przedsiębiorcy, w tym na podstawie danych zawartych w rejestrach, ewidencjach, kartotekach, także niedostępnych powszechnie, które obejmuje: a) strukturę kapitału oraz powiązania kapitałowe przedsiębiorcy, źródła pochodzenia środków finansowych i sytuację finansową; b) strukturę organizacyjną; c) prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem,” Na zakończeniem należy jeszcze wspomnieć o nieprzewidzeniu przez ustawodawcę kwestii spełnienia przez sprzęt norm międzynarodowych (tworzonych przez ISO, ITU, IEC)	
25.	Akademia Sztuki Wojennej	Art. 1 pkt 29 projektu (art.	po art. 66 dodaje się art. 66a-66c w brzmieniu: „Art. 66a (…)	**Wyjaśnienie**

		66a ust. 5 uKSC)	5. Sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania określa: a) wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe, albo b) umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo c) niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowania stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy." Przyjęte rozwiązanie należy uznać za wadliwe. Brak w nim zachowania stopniowania zagrożenia w przypadku umiarkowanego i wysokiego ryzyka– w obu wypadkach jest to „poważne" ryzyko (pomijam w tym miejscu kwestie semantyczne – wydaje się, że „umiarkowane ryzyko" od „poważnego" dzieli znacznie więcej niż „niskie" od „umiarkowanego", a nadto zestawienie „umiarkowane ryzyko" i „poważne zagrożenie" nie prezentuje się najlepiej). Oba omawiane stopnie ryzyka ma odróżniać „możliwość zmniejszenia poziomu ryzyka przez wdrożenie środków technicznych lub organizacyjnych" – w przypadku ryzyka poważnego zdaniem ustawodawcy nie ma takiej możliwość. Trudno wskazać taką sytuację. Sądzę, że w rzeczywistości taki stan może nigdy nie zaistnieć. Jedynym rozwiązaniem jest rezygnacja z tego warunku i zastosowanie stopniowana zagrożenia. Czyli przyjąć należy, że wysoki stopień ryzyka charakteryzuje się bardzo poważnym (czy wyjątkowym, szczególnym lub znaczącym) zagrożeniem, poważny stopień (zamiast umiarkowany) ryzyka – poważnym zagrożeniem.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. W ramach postępowania administracyjnego minister właściwy do spraw informatyzacji wyda decyzję o uznaniu dostawcy za dostawcę wysokiego ryzyka, jeżeli zostanie stwierdzone poważne zagrożenie dla bezpieczeństwa państwa.
26.	Akademia Sztuki Wojennej	Art. 1 pkt 29 Projektu (art.	„Art. 66a (…) 7. W przypadku określenia umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego dotyczy ta ocena dostawcy sprzętu lub	**Wyjaśnienie**

		66a ust. 7 uKSC**)**	oprogramowania, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium może zmienić ocenę." Opiniowany przepis należy uzupełnić o wskazanie przypadku określenia wysokiego ryzyka (co jest konsekwencją ewentualnej zmiany art. 66a ust. 5 lit a projektu) oraz zastąpienie sformułowania „Kolegium może zmienić ocenę" frazą „Kolegium zmienia ocenę". W przypadku bowiem, gdy podmiot przedstawił Kolegium środki zaradcze i plan naprawczy, zmiana oceny powinna mieć charakter obligatoryjny. Ponadto należy usunąć **błąd w postaci powtórzonego** sformułowania „dostawcy sprzętu lub oprogramowania" W ten sposób omawiany przepis uzyskałby następujące brzmienie: „W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ta ocena ~~dostawcy sprzętu lub oprogramowania~~, może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ~~może zmienić~~ ocenę."	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.
27.	Akademia Sztuki Wojennej	Art. 1 pkt 29 projektu (art. 66 a ust. 8 uKSC)	Projektowany przepis 66a ust. 8 projektu ma następujące brzmienie- „Dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b." Komentując ten przepis należy w pierwszej kolejności wskazać, że pozbawia on prawa do weryfikacji decyzji organu I instancji części dostawców – prawo odwołania przyznano jedynie tym dostawcom sprzętu lub oprogramowania, których dotyczy ocena określająca wysokie ryzyko. Po drugie – w treści przepisu mowa jest o odwołaniu, a w rzeczywistości jest to wniosek o ponowne rozpatrzenie sprawy. Trzeba to wyraźnie wskazać, gdyż Kolegium nie znajduje się wśród organów wskazanych w art. 127 § 3 KPA (podmiotów, od których nie służy	Uwaga uwzględniona Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds.

			odwołanie, jednakże strona niezadowolona z decyzji może zwrócić się do tego organu z wnioskiem o ponowne rozpatrzenie sprawy). Dodatkowo postulowałbym umieszczenie stosownego odesłania do przepisów KPA (zob. uwagi do art. 67 opiniowanego projektu) Wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej nieodwracalne skutki. Zawsze pozostaje możliwość nadania rygoru na podstawie 108 § 1 KPA.	informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.
28.	Akademia Sztuki Wojennej	Artykuł 1 pkt 29 projektu (art. 66a u.KSC) – uwagi ogólne	Według projektowanego art. 66a ust. 1 – Kolegium może sporządzić, na wniosek członka Kolegium, ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Ustawodawca wprowadza zatem stosowne uprawnienie Kolegium, z którego jeżeli Kolegium skorzysta, to wówczas będzie to miało daleko idące konsekwencje dla dostawcy sprzętu lub oprogramowania. Art. 64 u.k.s.c. wyraźnie stanowi, że Przy Radzie Ministrów działa Kolegium, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. **Zatem Kolegium powinno być jedynie organem opiniodawczo-doradczym, a nie rozstrzygającym.** Do zadań Kolegium należy min. wyrażanie opinii w sprawach określonych w art. 65 ust. 1 u.k.s.c. oraz opracowywanie rekomendacji, o których mowa w art. 65 ust. 2 u.k.s.c. Jak stanowi projektowany art. 66a ust. 6 sporządzona przez Kolegium ocena ryzyka dostawcy sprzętu lub oprogramowania przekazywana jest Pełnomocnikowi, który ogłasza ją w postaci komunikatu w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Forma prawna oceny ryzyka przybiera zatem formę komunikatu, nie aktu powszechnie obowiązującego, czy też decyzji administracyjnej. **Ocena ryzyka jest aktem rozstrzygającym sprawę co do istoty i dotyczy dostawcy sprzętu lub oprogramowania, zatem powinna mieć formę decyzji administracyjnej.** Do postępowania w spawie oceny ryzyka powinny mieć zastosowanie administracyjne przepisy procesowe.	Uwaga uwzględniona Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu

			Konsekwencje, jakie wynikają z oceny ryzyka, określone zostały w projektowanym art. 66b. I tak W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; 2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; 2) mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania. Udział dostawcy sprzętu lub oprogramowania jako strony postępowania w sprawie oceny ryzyka jest przez ustawę nowelizującą znacznie ograniczony. Zasadniczo dotyczy działań *ex post*. W projektowanym art. 66a ust. 7 wyraźnie się stanowi, że w przypadku określenia umiarkowanego lub niskiego ryzyka, dostawca sprzętu lub oprogramowania, którego dotyczy ta ocena może przedstawić Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium może zmienić ocenę. Dostawca w postępowaniu w sprawie oceny ryzyka nie bierze udziału, chociaż jako strona postępowania powinien. Może on przedstawić Kolegium środki zaradcze i plan naprawczy ale w przypadku określenia umiarkowanego lub niskiego ryzyka, zatem gdy rozstrzygnięcie już zapadło, zatem niejako w drugiej instancji, chociaż jest to postępowanie przed tym samym organem, a nie organem wyższego stopnia. Według projektowanego art. 66a ust. 8 dostawca sprzętu lub oprogramowania którego dotyczy ocena określająca wysokie ryzyko może odwołać się w terminie 14 dni od publikacji komunikatu o sporządzonej ocenie do Kolegium. Kolegium rozpatruje odwołanie w ciągu 2 miesięcy od otrzymania. Wniesienie odwołania	administracyjnego na decyzję.

			nie wstrzymuje działań określonych w projektowanym art. 66b. Dostawca w pierwszej instancji nie korzysta z zasady czynnego udziału stron w postępowaniu, dopiero może wnieść odwołanie od oceny określającej wysokie ryzyko, ale rozpatruje je ten sam organ co sporządził ocenę, zatem Kolegium. W związku z powyższym nie będzie to organ wyższej instancji, niezależny a organ zainteresowany utrzymaniem w mocy zaskarżonej oceny.	
29.	Akademia Sztuki Wojennej	Artykuł 1 pkt 29 projektu (art. 66b uKSC)	„Art. 66b. 1. W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; 2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie. 2. W przypadku sporządzenia oceny określającej umiarkowane ryzyko dostawcy sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1) nie wprowadzają do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania; 2) mogą kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz rodzaju i liczby usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy sprzętu lub oprogramowania.”; W projektowanym art. 66b brak przepisów dotyczących odszkodowań, za zobowiązanie podmiotów krajowego systemu bezpieczeństwa, którego ryzyko oceniono jako wysokie do wycofania z użytkowania sprzętu, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 lat od dnia ogłoszenia komunikatu o ocenie (art. 66b ust. 1 pkt 2). Odszkodowania takie powinny również przysługiwać podmiotom, które zostaną zobowiązane do niewprowadzania do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania w	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw.

			wypadku, sprzęt ten, oprogramowanie lub usługi, zostały wykupione, ale nie zostały wprowadzone do eksploatacji (art. 67b ust. 1 pkt 1, art. 67 b ust. 2 pkt 1). Uzasadnieniem konieczności wprowadzenia powyższego rozwiązania jest okoliczność, że w wyniku działania państwa zgodnie z prawem, polegającym na wydaniu nowej regulacji, podmioty te poniosą niezawinione przez nie straty finansowe związane z koniecznością zakupu nowego sprzętu, oprogramowania i usług.	model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
30.	Akademia Sztuki Wojennej	Art. 1 pkt 12 projektu (rozdział 4a-art. 20a-20f uKSC)	Przepisy rozdziału 4a miałyby regulować obowiązki przedsiębiorców komunikacji elektronicznej (z uwagi na objętość rozdziału zrezygnowano z cytowania planowanych przepisów, zwłaszcza, że dla jasności opinii w tym zakresie nie jest to niezbędne). Jak była mowa na wstępie ,powinny się znaleźć w ustawie Prawo komunikacji elektronicznej, w szczególności, że częściowo się **pokrywają – por.** art. 20a opiniowanego projektu z z art. 39 projektu z dnia 29	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa

			lipca 2020 ustawy – Prawo komunikacji elektronicznej, przepisy art. 20e – przepisów art. 42 ust. 2 i 3 projektu ustawy – Prawo komunikacji elektronicznej, a przepis art. 20f – przepisu art. 44 ust. 1 projektu ustawy – Prawo komunikacji elektronicznej. Z kolei w art. 20a ust. 4 znajduje się delegacja dla ministra właściwego do spraw informatyzacji **identyczna** jak delegacja z art. 39 projektu ustawy – Prawo komunikacji elektronicznej. Analogiczna sytuacja ma miejsce w przypadku art. 20c ust. 4 omawianego projektu i art. 42 ust. 2 projektu ustawy – Prawo komunikacji elektronicznej.	sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa. Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa

				zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
31.	Akademia Sztuki Wojennej	Art. 1 pkt 29 projektu (art. 66a ust. 2-3 uKSC)	„2. Wniosek o sporządzenie oceny zawiera wskazanie: 1) danych identyfikujących dostawcę sprzętu lub oprogramowania; 2) możliwych obszarów działalności, w których dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. 3. Wniosek o sporządzenie oceny może określać: 1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub, 2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa - które uwzględnia się przy sporządzeniu oceny sprzętu lub oprogramowania.” Przy ocenie bezpieczeństwa sieci oraz usług powinien być przede wszystkim oceniany sprzęt, a nie przedsiębiorcy go dostarczający. Stąd należy zastąpić w powyższym przepisie odwołania do dostawcy, odwołaniami do sprzętu i oprogramowania. „2. Wniosek o sporządzenie oceny zawiera wskazanie: 1) danych identyfikujących dostawcę sprzętu lub oprogramowania; 2) możliwych obszarów działalności, w których ~~dostawca sprzętu lub oprogramowania~~ sprzęt lub oprogramowanie może stanowić zagrożenie dla bezpieczeństwa narodowego. 3. Wniosek o sporządzenie oceny może określać: 1) rodzaje sieci telekomunikacyjnych i systemów teleinformatycznych lub produktów, usług i procesów, o których mowa w art. 2 pkt 3e lub,	**Uwaga nieuwzględniona** Przepisy nawiązują do Toolbox 5G, w którym to ocena ryzyka ma dotyczyć także aspektów nietechnicznych.

			2) kategorie podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa - które uwzględnia się przy sporządzeniu oceny ~~dostawcy~~ sprzętu lub oprogramowania.”	
32.	Konfederacja Lewiatan	Art. 66a ust. 1–	Kolegium w ramach dokonywanej oceny jako organ o charakterze administracyjno-politycznym powinno obligatoryjnie korzystać z oceny technicznej wydawanej przez odpowiednio certyfikowane laboratorium. Zdaniem KL w skład Kolegium powinni wchodzić wysokiej rangi i posiadający wszechstronną wiedzę w temacie cyberbezpieczeństwa przedstawiciele biznesu. Ponadto uważamy, że ocena powinna dotyczyć przede wszystkich samych urządzeń i oprogramowania, a ewentualnie pomocniczo samego dostawcy. Zgodnie z Toolbox 5G, (str. 12) "Ocena profilu ryzyka dostawców i zastosowanie ograniczeń do dostawców uznanych za wysokiego ryzyka — ma następować w odniesieniu do kluczowych aktywów”. Projekt ustawy nie bierze natomiast pod uwagę kategorii aktywów z punktu widzenia bezpieczeństwa, wraz z poziomem wrażliwości i listą kluczowych elementów (kategorie elementów i funkcji). Niewłaściwe jest w naszej ocenie nakładanie takich samych zobowiązań na wszystkie aktywa. Ponadto zauważamy niezgodność ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox), również dlatego, że przewiduje się całościowe wyłączenie dostawcy. Toolbox 5G SM03 przewiduje natomiast możliwość wyłączenia, ale z wyłączeniem dostaw określonej infrastruktury (aktywa kluczowe) takie jak sprzęt i oprogramowanie dotyczące sieci rdzeniowej. Innymi słowy, polskie propozycje zawarte w projekcie wykraczają poza wymagania zawarte w Toolbox. Z tego względu proponujemy, aby art. 66a ust. 1 otrzymał następujące brzmienie: „1. Kolegium może, na wniosek członka lub członków Kolegium, sporządzić ocenę ryzyka związaną ze sprzętem lub oprogramowaniem o znaczeniu krytycznym, decydującym o sposobie zarządzania: przetwarzaniem informacji i przesyłania danych, mechanizmami kryptograficznymi, mechanizmami zarządzania wirtualizacją oraz interfejsami zapewniającymi uprawnionym podmiotom dostęp do przekazów nadawanych lub odbieranych w sieci podmiotów krajowego systemu bezpieczeństwa cybernetycznego. Wniosek o sporządzenie oceny może zostać złożony po: 1) stwierdzonym istotnym incydencie bezpieczeństwa	Uwaga częściowo uwzględniona Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie prowadzone przez ministra właściwego ds. informatyzacji. Ocena ryzyka będzie wydana w formie decyzji administracyjnej. Dostawcy będzie przysługiwać wniosek o ponowne rozpatrzenie sprawy i skarga do sądu administracyjnego na decyzję.

			lub integralności u podmiotów krajowego systemu cyberbezpieczeństwa lub dostawców usług komunikacji elektronicznej na poziomie krajowy, które zostało spowodowane przez sprzęt lub oprogramowanie danego dostawcy, w zakresie objętym incydentem, lub 2) wykryciu wysokiej podatności sprzętu lub oprogramowania zwiększającej istotnie poziom ryzyka wystąpienia incydentu bezpieczeństwa lub integralności u podmiotów krajowego systemu cyberbezpieczeństwa lub dostawców usług komunikacji elektronicznej w zakresie objętym wykrytą podatnością i kiedy podmiot u którego wystąpiła podatność poinformuje o braku możliwości wdrożenia rozwiązań technicznych lub organizacyjnych ograniczających ryzyko związane z wykrytą podatnością. Kryteria dotyczące oceny są nieprecyzyjne i uznaniowe. Uwaga 1: Tryb odwoławczy w zasadzie nie istnieje, o zmianę oceny MUSI wnosić Członek Kolegium. Uwaga 2: Zasady powinny mieć charakter obiektywny i techniczny, w szczególności dla sprzętu i oprogramowania typu Commercial-of-the-Shelf (COTS). Należy bowiem przyjąć, że te ostatnie nie są modyfikowane dla potrzeb wybranych klientów, a dostosowane są dla ogólnego charakteru. Uwaga 3: W przypadku takiego sprzętu i oprogramowania COTS jest możliwa sytuacja, że może nie spełniać kryteriów w konfiguracji podstawowej, ale po odpowiedniej konfiguracji (tzw. hardening) lub przy zastosowaniu dodatkowych środków ze strony producenta lub firm trzecich wypełnia wszystkie wymagania. Aktualny zapis nie przewiduje takiego scenariusza patrząc się na ten rodzaj sprzętu i oprogramowania jako zamkniętą całość pochodzącą od jednego producenta. Podsumowując: producenci sprzętu i oprogramowania, w szczególności tzw. COTS, a w zasadzie to użytkownicy takich rozwiązań (tak!) powinni mieć określoną jasną listę kryteriów do spełnienia i jeśli są one wypełnione to produkty i usługi mogą być wykorzystywane. Jednocześnie przy zmianie kryteriów lub ich podwyższeniu dotychczas wykorzystywane produkty/usługi powinny być w określonym czasie zmienione na nowe lub zastąpione.	
33.	Konfederacja Lewiatan	Art. 66a ust. 2 i 3 –	W pierwszej kolejności zauważamy, że zakres możliwych ocen znacząco wykracza poza pierwotnie dyskutowany obszar sieci 5G. W myśl projektowanych przepisów skutkami ocen mogłyby być objęte wszystkie podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych. Oznacza to, że każdorazowo niezbędne będzie zachowanie bardzo	**Uwaga nieuwzględniona** Krajowy system cyberbezpieczeństwa ma na celu zapewnienie

			wysokiej precyzji wniosku o dokonanie oceny oraz dokonania jeszcze przed jego złożeniem szczegółowej analizy wpływu i potencjalnych skutków, wraz z identyfikacją podmiotów, jakie mogą zostać objęte skutkami wydanej oceny. Wniosek o przeprowadzenie oceny wymaga bardzo istotnego doprecyzowania, w taki sposób, aby zawierał już kluczowe elementy planowanego rozstrzygnięcia, w szczególności w zakresie: Wskazania zakresu badania bezpieczeństwa określającego, jakie konkretnie kategorie urządzeń lub oprogramowania danego dostawcy, a także zakres ich stosowania mają zostać poddane badaniu. Określenie zakresu użytkowania danego typu urządzeń lub oprogramowania, w tym wskazanie podmiotów, które mogą być objęte potencjalnymi skutkami wydawanej oceny. Opis rynku dostawców urządzeń lub oprogramowania, które poddawane jest badaniu. Oceny skutków planowanej do wydania oceny, w tym w zakresie wpływu na konkurencję i konsumentów oraz koszty jej wdrożenia. Określenie poziomu proponowanej do wydania przez Kolegium oceny.	cyberbezpieczeństwa na poziomie krajowym, stąd też ocena ryzyka musi dotyczyć wszystkich rodzajów sieci.
34.	Konfederacja Lewiatan	Art. 66a ust. 4	Art. 66a ust. 4 – doprecyzowanie kryteriów oceny a) art. 66a ust. 4 pkt 1 KSC Nawiązując do powyższych postulatów dot. skupienia się na ocenie sprzętu i oprogramowania, w art. 66a ust. 4 pkt 1 postulujemy usunąć słowa „jakie stanowi dostawca sprzętu i oprogramowania”. b) art. 66 ust. 4 pkt 2 KSC Postulujemy usunięcie przepisu. Ocena musi być przeprowadzana na podstawie jasno określonych, jasnych, jednoznacznych i możliwych do zweryfikowania kryteriów. W przeciwnym razie nie będzie to obiektywna ocena, lecz ocena uznaniowa. W warstwie legislacyjnej jest to w naszej ocenie jest to sprzeczne z przepisami §6 rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie zasad techniki prawodawczej, który wskazuje, że: Przepisy prawa są tak sformułowane, że intencje prawodawcy są dokładnie wyrażone adresatom zawartych w nich norm. Przepisy te naruszają przepisy rozporządzenia, ponieważ są one niezrozumiałe i ni faktyczne znaczenie zwrotu "prawdopodobieństwo wpływu dostawcy sprzętu lub oprogramowania na kraj spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego”.e jest możliwe określenie ich treści. W szczególności trudno ustalić Art. 66a ust. 4 pkt 2-5: Kryteria oceny dostawcy W naszej ocenie kryteria oceny powinny zostać uzupełnione o: Ocenę wpływu na konkurencyjność rynku (w tym ocena tego,	**Uwaga nieuwzględniona** Kryteria oceny nawiązują do kryteriów wskazanych w Toolbox 5G

			czy ograniczona liczba dostawców nie przyczyni się do wzrostu cen czy opóźnień w realizacji dostaw), konsumentów, koszty oraz możliwość zapewnienia ciągłości działania usług przez podmioty będące aktualnie użytkownikami urządzeń lub oprogramowania poddanego badaniu, w szczególności jeśli wydawana byłaby ocena dot. wysokiego lub umiarkowanego ryzyka. Kryteria techniczne oceny, w tym dot. odniesienia do zgodności urządzeń lub oprogramowania z dokumentami standaryzacyjnymi, a także w zakresie posiadanych przez badane urządzenia lub oprogramowanie certyfikatów bezpieczeństwa. Należy również odnieść się do budowanego obecnie schematu certyfikacji dla 5G w ramach Cybersecurity Act, który wydaje się, że powinien być kluczowym narzędziem do profesjonalnego badania bezpieczeństwa. W procesie oceny należy uwzględnić opinie certyfikowanych laboratoriów. Uzyskanie opinii użytkowników urządzeń lub oprogramowania poddawanych ocenie. Poniżej przedstawiamy propozycję zmiany w zakresie art. 66a ust. 4 pkt 2 w sposób, który w naszej ocenie będzie charakteryzował się obiektywizmem w zakresie weryfikacji kryteriów oraz bardzo wysokim stopniem profesjonalizacji weryfikacji, co zapewni poprawność wyników stosowanych kryteriów oceny. Kryteria nietechnologicznie są często niezdefiniowane i bardzo trudno jest zweryfikować i ocenić niejasne pojęcia, ale nie powinny odgrywać kluczowej roli, gdyż mogą prowadzić do błędnych wniosków. „2) analizę sposobu i zakres wdrożenia przez dostawców środków technicznych i organizacyjnych, zwanych dalej „środkami”, w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług, a w szczególności: a) uzyskanie certyfikatu (takich jak ISO27001, Common Criteria, Network Equipment Security Scheme, unijny program certyfikacji cyberbezpieczeństwa) dla sprzętu lub oprogramowania o znaczeniu krytycznym, które mogą podlegać ocenie Kolegium, o której mowa w art. 66 a ust. 1 KSC, b) posiadanie deklaracji wiarygodności zawierającej zobowiązania do: pełnej współpracy w zakresie bezpieczeństwa z użytkownikami sprzętu lub oprogramowania; nieprzekazywania wbrew zawartym umowom danych i informacji osobom trzecim; wyrażenia zgody i odpowiedniego wsparcia w zakresie kontroli bezpieczeństwa i analiz penetracyjnych jego produktu w wymaganym zakresie; potwierdzenia, że sprzęt lub oprogramowanie nie posiadają celowo	

			wdrożonych i wrażliwych pod względem bezpieczeństwa funkcjonalności i że nie zostaną one wbudowane w późniejszym czasie; niezwłocznego powiadomienia przedsiębiorcy o wszelkich znanych mu lub wykrytych zagrożeniach dla zapewnienia bezpieczeństwa, c) poziom zapewnianej przez dostawcę integralności sprzętu lub oprogramowania, a w szczególności zapewnienie ich użytkownikom: możliwości weryfikacji integralności nabytych składników krytycznych w każdym czasie; możliwości weryfikacji czy dane składniki krytyczne nie zostały podczas dostawy zmanipulowane, naruszone lub w inny sposób zmienione; prowadzonego przez dostawcę monitoringu bezpieczeństwa w celu zidentyfikowania zagrożeń bezpieczeństwa oraz podejmowania środków zapobiegawczych;”	
35.	Konfederacja Lewiatan	Art. 66a ust. 5	Art. 66a ust. 5 - gradacja ryzyk Jak już wskazano wyżej, w naszej ocenie proponowana konstrukcja nie jest zgodna ze środkiem SM03 Toolbox (strony 12 i 21 Toolbox) dlatego, że przewiduje całościowe wyłączenie dostawcy bez odniesienia do konkretnych „krytycznych aktywów”. Toolbox przewiduje możliwość wyłączenia, ale w zakresie określonej infrastruktury. Innymi słowy, projekt wydaje się wykraczać poza ramy określone w europejskich rekomendacjach. Wątpliwości budzi także przyjęta w art. 66a ust. 5 Projektu gradacja ryzyk, a ściśle ich definiowanie. Chodzi o różnicę pomiędzy wysokim ryzykiem a ryzykiem umiarkowanym. W przypadku bowiem obu definicji jest to poważne zagrożenie a różnica polega na tym, że w przypadku wysokiego ryzyka zmniejszenie tego ryzyka nie jest możliwe a w przypadku umiarkowanego jest możliwe. Tymczasem poziomy powinny wyraźnie (art. 66a ust. 5 lit a-b Projektu) różnić się gradacją, tak jak się różnią ryzyka opisane w art. 66a ust. 5 lit b-d Projektu, a nie wyłącznie oceną czy można to ryzyko zmniejszyć czy też nie. Jednocześnie należałoby przyjąć, że zawsze można poziom takiego ryzyka zmniejszyć, a przynajmniej powinno się stworzyć możliwość dla dostawcy podjęcia próby jego zmniejszenia. Poważne, więc zastrzeżenia budzi przyjęcie z góry założenia, że w przypadku „wysokiego ryzyka” zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe. Tym samym sposób opisu poziomów ryzyka wydaje się zbyt ogólny, a w świetle braku uwypuklenia w kryteriach oceny kwestii technicznych, istotne wątpliwości budzi także w jaki sposób miałoby być weryfikowane czy dla	**Wyjaśnienie** Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.

			danego przypadku możliwe jest wdrożenie dodatkowych rozwiązań technicznych lub organizacyjnych uzasadniających nadanie danemu dostawcy oceny ryzyka umiarkowanej, a nie wysokiej. Tym samym w zakresie ryzyk wysokiego i umiarkowanego: Postulujemy wykreślenie odniesienia do oceny dostawcy, na rzecz oceny sprzętu lub oprogramowania. W ryzyku wysokim postulujemy wskazanie, że oznacza ono bardzo poważne (a nie tylko poważne) zagrożenie.	
36.	Konfederacja Lewiatan	art. 66a ust. 5 lit a	Przepis art. 66a ust. 5 lit a Projektu powinien otrzymać następujące brzmienie: a) wysokie ryzyko, jeżeli dostawca sprzętu lub oprogramowaniea stanowi bardzo poważne zagrożenie dla cyberbezpieczeństwa państwa i zmniejszenie poziomu tego ryzyka przez wdrożenie środków technicznych lub organizacyjnych nie jest możliwe". b) umiarkowane ryzyko, jeżeli dostawca sprzętu lub oprogramowaniae stanowi poważne zagrożenie dla cyberbezpieczeństwa państwa a zmniejszenie poziomu tego ryzyka możliwe jest przez wdrożenie środków technicznych lub organizacyjnych, albo c) niskie ryzyko, jeżeli dostawca sprzętu lub oprogramowaniae stanowi niewielkie zagrożenie dla cyberbezpieczeństwa państwa, albo d) brak zidentyfikowanego poziomu ryzyka, jeżeli nie stwierdzono zagrożenia dla cyberbezpieczeństwa państwa lub jego poziom jest znikomy.	**Wyjaśnienie** Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.
37.	Konfederacja Lewiatan	Art. 66a ust. 7	Art. 66a ust. 7 KSC – plan naprawczy w przypadku uzyskania określonej oceny ryzyka W naszej ocenie uprawnienie do przedstawienia środków naprawczych powinno przysługiwać także w przypadku określenia wysokiego poziomu ryzyka, a Kolegium będzie miało uprawnienie do oceny takich propozycji. Jednocześnie, konsekwentnie postulujemy rezygnację z oceny samego dostawcy, na rzecz oceny urządzeń lub oprogramowania. Postulujemy więc nadanie art. 66a ust. 7 Projektu następującego brzmienia: 7. W przypadku określenia wysokiego, umiarkowanego lub niskiego ryzyka dostawca sprzętu lub oprogramowania, którego sprzętu lub oprogramowania dotyczy ocena może prz Kolegium środki zaradcze i plan naprawczy. W przypadku akceptacji tych środków zaradczych i planu naprawczego, Kolegium zmienia ocenę.edstawić	**Wyjaśnienie** Zrezygnowano z planów napraczych
38.	Konfederacja Lewiatan	Art. 66 a ust. 5 i 8	Art. 66 a ust. 5 i 8 KSC - forma Komunikatu oraz brak administracyjnej ścieżki odwoławczej od oceny Dostawcy W zakresie planowanej formy ogłoszenia	Uwaga uwzględniona

			oceny tj. Komunikatu, mamy istotne wątpliwości, co do adekwatności takiego sposobu działania. Komunikat będzie miał bardzo istotne skutki dla potencjalnie szerokiego kręgu adresatów, którzy aktualnie wykorzystują urządzenia lub oprogramowanie ocenianych dostawców. Nie powinno ulegać wątpliwości, że krąg tych adresatów Kolegium powinno określić precyzyjnie w toku prowadzonego postępowania dot. oceny bezpieczeństwa. Skoro to wpływ na bezpieczeństwo, w tym bezpieczeństwo narodowe miałby być badany to również skala i rodzaj działalności podmiotów korzystających lub mogących korzystać z danych rozwiązań musi zostać uwzględniona. Sam Komunikat, będzie jednocześnie rodził dla nich określone obowiązki i ograniczenia, doniosłe także w sferze prawa cywilnego (np. zawarte umowy długoterminowe), a przede wszystkim w zakresie własnej organizacji i sposobu prowadzenia działalności. W tym ujęciu Komunikat posiada cechy indywidualnego aktu o skutkach zbliżonych dla decyzji administracyjnej lub wręcz określenia praw i obowiązków, które co do zasady powinny być nakładane w drodze ustawy. W tym zakresie uważamy, że forma ogłoszenia powinna zostać zrewidowana, a w szczególności zapewniać możliwość udziału w procesie oceny także podmiotom, których dotkną skutki dokonanej oceny, przynajmniej w formie konsultacji dot. możliwości redukcji poziomu ryzyka oraz identyfikowanego przez nie aktualnego poziomu ryzyka, a także w formie środków odwoławczych od takich rozstrzygnięć. Od rozstrzygnięcia Kolegium powinna być zapewniona możliwość wniesienia środków odwoławczych przez podmiot niezadowolony z rozstrzygnięcia (dokonanej oceny ryzyka dostawcy) do organów sprawujących wymiar sprawiedliwości, niezależnie, do jakiej kategorii ryzyka, o którym mowa w art. 66a ust. 5 Projektu zaliczony zostanie dostawca sprzętu lub oprogramowania. Nie powinna być bowiem dokonywana gradacja środków odwoławczych w zależności od tego, czy rozstrzygnięcie (ocena) jest bardziej lub mniej dotkliwe. Obecna konstrukcja art. 66a ust. 8 Projektu w zakresie środków odwoławczych, pomimo że używa się w tym przepisie słowa „odwołanie” jest pozorowana, pozbawiająca podstawowych praw podmiotów zainteresowanych weryfikacją dokonanej oceny przez Kolegium w sposób obiektywny i niezależny przez sąd. Przyjęta konstrukcja pozwala na to, że Kolegium będzie „sędzią we własnej sprawie” tj. będzie	Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub

			sprawdzało własną decyzję. Ogólne przepisy prawne, przewidują oczywiście konstrukcję wniosku o ponowne rozpoznanie sprawy przez organ, który wydał decyzję, ale zawsze przysługują także środki odwoławcze do sądu od takiego ponownego rozpoznania sprawy. Potwierdzeniem tezy o pozorowanej konstrukcji odwołania, jest także okoliczność, że zgodnie z obecnym brzmieniem art. 66a ust. 8 Projektu, zdanie ostatnie: Wniesienie odwołania nie wstrzymuje działań określonych w art. 66b. W praktyce oznacza to, więc, że przewidziane w tym przepisie „odwołanie" nie ma praktycznego znaczenia, skoro pomimo jego wniesienia będą podejmowane praktycznie nieodwracalne w swoich skutkach decyzje w zakresie np. wycofania sprzętu z sieci operatora czy utraty kontaktu na sprzedaż infrastruktury telekomunikacyjnej. W tym ujęciu oznacza to, że nawet niezasadna decyzja Kolegium może wywołać taki skutek, jaki wywołałoby jej utrzymanie. Ponadto przedstawiamy poniższą propozycje zmiany brzmienia przepisów: a) Przepis art. 66a ust. 8 Projektu otrzymuje brzmienie: „8. Dostawcy sprzętu lub oprogramowania, którego dotyczy ocena, przysługuje wniosek do Kolegium o ponowne rozpoznanie sprawy w zakresie oceny. Przepisy działu 2 rozdziału 10 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego w zakresie odwołań od decyzji stosuje się odpowiednio. Od decyzji Kolegium wydanej po rozpoznaniu wniosku o ponowne rozpoznanie sprawy przysługuje skarga do Wojewódzkiego Sądu Administracyjnego." b) W Art. 66a Projektu należy dodać nowy ust. 10: „Postępowanie przed Kolegium prowadzone jest zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego" Postanowienia k.p.a. regulują tryb postępowania i wydawanie decyzji przez organy państwowe. Obecnie projektowane przepisy odrębnie regulują te kwestie za pomocą zaledwie kilku przepisów, które można uznać za posiadające charakter proceduralny. Przepisy te nie mogą jednak zastąpić odpowiednich regulacji k.p.a. Uwagi te dotyczą także projektowanych wymogów, jakie elementy powinna zawierać ocena Kolegium (art. 66a ust. 5 Projektu), w tym zakresie przedstawienia uzasadnienia oceny.	oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).
39.	Konfederacja Lewiatan	Art. 66a ust. 7 i 9	Art. 66a ust. 7 i 9 KSC – ostateczność Komunikatu Jednocześnie nNiezależnie od uwag dot. formy Komunikatu oraz możliwości odwołania, nasze praktyczne wątpliwości budzi możliwość modyfikacji Komunikatu po jego ogłoszeniu w	Przepisy art. 66a-66c zostaną zmienione.

			wyniku odwołania lub przedstawienia środków naprawczych przez dostawcę. Aby ograniczyć ryzyko związane ze zbyt szybkim wejściem w życie publikowanego Komunikatu należy przewidzieć w nim odpowiedni okres przejściowy, w którym możliwe są jeszcze zmiany w wyniku przewidzianych w projekcie środków odwoławczych. Z perspektywy podmiotów, które mają mieć obowiązek dostosowania się do treści Komunikatu nie jest akceptowalna sytuacja, w której tak ważne rozstrzygnięcie będzie skuteczne, mimo, że jeszcze nie jest ostateczne i może zostać zweryfikowane. Ewentualnie środki odwoławcze/konsultacyjne należy zintegrować z procedurą oceny tak, aby w życie wprowadzana była ostateczna ocena.	Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie

				prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).
40.	Konfederacja Lewiatan	Art. 66b	1) Art. 66b – ocena ryzyka Jednocześnie nasze wątpliwości budzi możliwość modyfikacji Komunikatu po jego ogłoszeniu w wyniku odwołania lub przedstawienia środków naprawczych przez dostawcę. Aby ograniczyć ryzyko związane ze zbyt szybkim wejściem w życie publikowanego Komunikatu należy przewidzieć w nim odpowiedni okres przejściowy, w którym możliwe są jeszcze zmiany w wyniku przewidzianych w projekcie środków odwoławczych. Z perspektywy podmiotów, które mają mieć obowiązek dostosowania się do treści Komunikatu nie jest akceptowalna sytuacja, w której tak ważne rozstrzygnięcie będzie skuteczne mimo, że jeszcze nie jest ostateczne i może zostać zweryfikowane. Ewentualnie środki odwoławcze/konsultacyjne należy zintegrować z procedurą oceny tak aby w życie wprowadzana była ostateczna ocena. Art. 66b – ocena ryzyka a) Jak wskazaliśmy wyżej, skuteczność Komunikatu musi następować od jego wejścia w życie w formie ostatecznej, a nie od wskazanego w projekcie ustawy „sporządzenia” oceny, co jest czynnością faktyczną kończącą pewien etap oceny. b) Postulujemy wykreślenie odniesienia do oceny dostawcy, na rzecz oceny sprzętu lub oprogramowania. a) W zakresie określenia ryzyka, jako wysokiego należy doprecyzować skutki poprzez wskazanie, że w okresie na wycofanie urządzeń lub oprogramowania możliwe jest też dokonywanie zakupów lub wdrożeń mających na celu	Uwaga częściowo uwzględniona Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds.

			utrzymanie funkcjonowania dotychczasowych funkcjonalności, a w szczególności utrzymanie ciągłości świadczenia usług. Ma to absolutnie kluczowe znaczenie dla możliwości reakcji na awarie i uszkodzenia. Ponadto okres na wycofanie należy wydłużyć do 10 lat co ma na celu poszanowanie praw nabytych użytkowników urządzeń lub infrastruktury i umożliwienie im korzystania z danych rozwiązań przynajmniej w pełnym okresie ich amortyzacji i podstawowej przydatności technicznej. Ewentualnie postulujemy, aby Kolegium dokonywało oceny, jaki okres jest niezbędny na dostosowanie (po zasięgnięciu opinii użytkowników), przy czym nie powinien on być w żadnym przypadku krótszy niż 7-letni podstawowy okres amortyzacji dla niektórych kategorii urządzeń stosowanych w sieciach telekomunikacyjnych. b) W Projekcie nie ma różnicy pomiędzy skutkami oceny wysokiego ryzyka (art. 66b ust. 1 pkt 1 Projektu) oraz skutkami oceny umiarkowanego ryzyka (art. 66b ust. 2 pkt 1 Projektu). Skutki te, w przypadku umiarkowanego ryzyka powinny być mniej dotkliwe niż w przypadku wysokiego ryzyka. Propozycja przewiduje dwojakiego rodzaju skutki i obowiązki. Pierwszy realizuje postanowienia 5G Toolbox i polega na dywersyfikacji dostawców, identycznie jak w w § 3 ust. 1 pkt 2 rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych oraz metod, jakie przedsiębiorcy telekomunikacyjni są obowiązani stosować w celu zapewnienia bezpieczeństwa lub integralności sieci lub usług (Dz.U. z 2020 r. poz. 1130). Drugi obowiązek związany jest z realizacją postanowień art. 66a ust. 7, w postaci podjęcia odpowiednich działań naprawczych w celu usunięcia stwierdzonych uchybień, podejmowanych przez obie strony tj. przez podmioty krajowego systemu cyberbezpieczeństwa oraz dostawców, co gwarantuje skuteczność działań w zakresie poprawy bezpieczeństwa. W przypadku braku wprowadzenia przepisów zapewniających wymaganą elastyczność w zakresie uwzględniania oceny Kolegium, za zasadne uznajemy wprowadzenie mechanizmów finansowej rekompensaty z tytułu poniesionych kosztów i strat związanych z wydaniem oceny. Projekt przepisu: Art. 66 b ust. 1 KSC – ocena ryzyka na poziomie wysokim „W przypadku sporządzenia oceny ryzyka określającej wysokie ryzyko określonego krytycznego sprzętu lub oprogramowania podmioty krajowego systemu cyberbezpieczeństwa: 1) nie	Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany,

			wprowadzają do użytkowania sprzętu, oprogramowania i usług infrastruktury krytycznych określonych w ocenie danego dostawcy sprzętu lub oprogramowania, z wyjątkiem sytuacji kiedy dokonanie zakupów lub wdrożeń jest niezbędne dla funkcjonowania ich sieci, infrastruktury lub usług, a także naprawy awarii lub uszkodzeń; 2) wycofują z użytkowania sprzęt, oprogramowanie i usługi określone w ocenie danego dostawcy sprzętu lub oprogramowania nie później niż 5 10 lat od dnia ogłoszenia komunikatu o ocenie.” Projekt przepisu: Art. 66b ust. 2 KSC– ocena ryzyka na poziomie umiarkowanym W przypadku sporządzenia oceny określającej umiarkowane ryzyko określonego krytycznego sprzętu lub oprogramowania, podmiotu krajowego systemu cyberbezpieczeństwa stosują strategię skutkującą brakiem uzależnienia od jednego dostawcy poszczególnych elementów sieci telekomunikacyjnej a dostawcy sprzętu lub oprogramowania wprowadzają środki zaradcze oraz plan naprawczy, o których mowa w art. 66a ust. 7”	brak zidentyfikowanego ryzyka.
41.	Konfederacja Lewiatan	Art. 66 b	Art. 66 b : propozycja rekompensat: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2: 3. dotychczasowi użytkownicy sprzętu lub oprogramowania otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania; 4. rekompensata jest obliczana na podstawie wydatków poniesionych na zakup sprzętu lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni. Uzasadnienie: Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie” operatorów z posiadanego Sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby nie wprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie

				docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.

42.	Konfederacja Lewiatan	Art. 66c punkt 1	Art. 66c punkt 1 „Plan naprawczy” Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania lub sprzętu, a nie w stosunku do dostawców. Propozycja zmiany: „W szczególnie uzasadnionych przypadkach Pełnomocnik może zobowiązać podmiot krajowego systemu cyberbezpieczeństwa lub przedsiębiorcę komunikacji elektronicznej, do którego zastosowanie ma ocena, do sporządzenia i dostarczenia w ciągu 3 miesięcy roku planu i harmonogramu wycofania z użytkowania sprzętu, oprogramowania i usług dostawcy sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.”	**Wyjaśnienie** Zrezygnowano z planów naprawczych
43.		Art. 1 pkt 30 Projektu:(art. 67a uKSC)	„Art. 67a. 1. Pełnomocnik może wydać: 1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium. 2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu. (…) 8. W przypadku odmowy zatwierdzenia przez Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.” Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. W tym wypadku znaleźć powinny zastosowanie przepisy art. 106 i art. 106a KPA, regulujące kwestię współdziałania organów.	**Uwaga częściowo uwzględniona** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis

			W związku z powyższym konieczne jest przeprowadzenie następujących zmian w projektowanym art. 67a uKSC: „Art. 67a. 1. Pełnomocnik może wydać: 1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego ~~– po zatwierdzeniu~~ **wyrażeniu opinii** przez Kolegium. ~~2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu~~. 8. W przypadku odmowy zatwierdzenia przez wyrażenia negatywnej opinii Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.”	art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać

				rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok

				przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest

				kluczowa w procesie ograniczenia skutków tego incydentu.
44.		Art. 1 pkt 30 Projektu (art. 67c KSC ust. 1 uKSC)	„Art. 67c. 1. Pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu.” Wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej możliwe nieodwracalne skutki. Zawsze pozostaje możliwość nadania rygoru na podstawie 108 § 1 KPA.	**Uwaga nieuwzględniona** Natychmiastowa wykonalność polecenia zabezpieczającego jest niezbędna ze względu na bezpieczeństwo narodowe.
45.			Propozycja dodania przepisu odsyłającego do KPA Przewidziane w projekcie ustawy przepisy nie tworzą kompletnej regulacji postępowania się przed Pełnomocnikiem lub Kolegium (brak np. regulacji trybu odwoławczego). W związku z powyższym, by uniknąć niejasności przy interpretacji, wskazane jest odesłanie do przepisów KPA, poprzez dodanie odpowiedniego przepisu, np.: „Art. 67d. W sprawach nieuregulowanych w ustawie do postępowania przed Pełnomocnikiem lub Kolegium stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.”	Uwaga uwzględniona
46.		Art. 1 pkt 30 Projektu:(art. 67a uKSC)	„Art. 67a. 1. Pełnomocnik może wydać: 1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium. 2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu.	**Uwaga częściowo uwzględniona** Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza,

			(…) 8. W przypadku odmowy zatwierdzenia przez Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające." Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. W tym wypadku znaleźć powinny zastosowanie przepisy art. 106 i art. 106a KPA, regulujące kwestię współdziałania organów. W związku z powyższym konieczne jest przeprowadzenie następujących zmian w projektowanym art. 67a uKSC: „Art. 67a. 1. Pełnomocnik może wydać: 1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego ~~– po zatwierdzeniu~~ **wyrażeniu opinii** przez Kolegium. ~~2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu~~. 8. W przypadku odmowy zatwierdzenia przez wyrażenia negatywnej opinii Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające."	że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art. 26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia

				ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z

				prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których

				dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
47.		Art. 1 pkt 30 Projektu (art. 67c KSC ust. 1 uKSC)	„Art. 67c. 1. Pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu.” Wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej możliwe nieodwracalne skutki. Zawsze pozostaje możliwość nadania rygoru na podstawie 108 § 1 KPA.	**Uwaga nieuwzględniona** Natychmiastowa wykonalność polecenia zabezpieczającego jest niezbędna ze względu na bezpieczeństwo narodowe.
48.			Propozycja dodania przepisu odsyłającego do KPA Przewidziane w projekcie ustawy przepisy nie tworzą kompletnej regulacji postępowania się przed Pełnomocnikiem lub Kolegium (brak np. regulacji trybu odwoławczego). W związku z powyższym, by uniknąć niejasności przy interpretacji, wskazane jest odesłanie do przepisów KPA, poprzez dodanie odpowiedniego przepisu, np.: „Art. 67d. W sprawach nieuregulowanych w ustawie do postępowania przed Pełnomocnikiem lub Kolegium stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego.”	Uwaga uwzględniona
49.		Art. 1 pkt 30 Projektu:(art. 67a uKSC)	„Art. 67a. 1. Pełnomocnik może wydać:	**Uwaga częściowo uwzględniona**

			1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego – po zatwierdzeniu przez Kolegium. 2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu. (…) 8. W przypadku odmowy zatwierdzenia przez Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.” Zgodnie z art. 67a ust. 1 Projektu Pełnomocnik może wydać ostrzeżenia i polecenia zabezpieczające we współdziałaniu z Kolegium. W tym wypadku znaleźć powinny zastosowanie przepisy art. 106 i art. 106a KPA, regulujące kwestię współdziałania organów. W związku z powyższym konieczne jest przeprowadzenie następujących zmian w projektowanym art. 67a uKSC: „Art. 67a. 1. Pełnomocnik może wydać: 1) ostrzeżenie - w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, 2) polecenie zabezpieczające - w przypadku wystąpienia incydentu krytycznego ~~– po zatwierdzeniu~~ **wyrażeniu opinii** przez Kolegium. ~~2. W szczególnie uzasadnionych przypadkach, na wniosek Zespołu, Pełnomocnik może wydać ostrzeżenie lub polecenie zabezpieczające, które nie zostało zatwierdzone przez Kolegium. Pełnomocnik niezwłocznie informuje Kolegium o zastosowanych ostrzeżeniach lub poleceniach zabezpieczających. Ogłoszone~~	Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art.

			~~ostrzeżenia lub polecenia zabezpieczające wymagają zatwierdzenia przez Kolegium na najbliższym posiedzeniu~~. 8. W przypadku odmowy zatwierdzenia przez wyrażenia negatywnej opinii Kolegium Pełnomocnik odwołuje ostrzeżenie lub polecenie zabezpieczające w części lub w całości albo stosuje wydaje inne ostrzeżenie lub polecenie zabezpieczające.”	26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane

				zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu

				krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
50.		Art. 1 pkt 30 Projektu (art. 67c KSC ust. 1 uKSC)	„Art. 67c. 1. Pełnomocnik wydaje polecenie zabezpieczające w drodze decyzji administracyjnej. Decyzja podlega natychmiastowemu wykonaniu.” Wskazana jest rezygnacja z rygoru natychmiastowej wykonalności decyzji z mocy prawa z uwagi na jej możliwe nieodwracalne skutki. Zawsze pozostaje możliwość nadania rygoru na podstawie 108 § 1 KPA.	**Uwaga nieuwzględniona** Natychmiastowa wykonalność polecenia zabezpieczającego jest niezbędna ze względu na bezpieczeństwo narodowe.
51.	Konfederacja Lewiatan	Art. 67a	Art. 67a – ostrzeżenia i polecenia zabezpieczające a) Instytucja ostrzeżenia powinna zostać zmodyfikowana do formy zgodnej ze swoją nazwą. Należy więc wykreślić z przepisów wszelkie odniesienia wskazujące na skutki ostrzeżenia	**Uwaga częściowo uwzględniona**

			jako „polecenia”, „nakazu”, „zakazu”. Obecnie bowiem, niezależnie od procesu opiniowania przez Kolegium, już samo ostrzeżenie, mogłoby skutkować wykluczeniem wskazanych w nim dostawców. Takie uprawnienie rodzi bardzo daleko idące obawy potencjalnych adresatów tych ostrzeżeń. Tym samym ostrzeżenie, jeśli miałoby zostać utrzymane musi otrzymać charakter, w którym w przypadku identyfikacji wystąpienia ryzyka incydentu krytycznego odpowiednie podmioty byłyby o tym informowane oraz otrzymywały informacje w sprawie możliwych działań. Aktualna formuła może być stosowana jedynie do podmiotów publicznych, a nie sektora prywatnego, wobec, którego rozwiązanie takie miałoby charakter nadania Pełnomocnikowi uprawnień o charakterze kierowniczym wobec podmiotów prywatnych, w tym spółek giełdowych. b) 2-letni okres, na jaki mają być wydawane ostrzeżenia lub polecenia zabezpieczające jest zdecydowanie zbyt długi i musi zostać ograniczony do okresu faktycznego zagrożenia, który powinien być liczony w dniach, a nie latach. c) Zgodnie z art. 67c ust. 1 Projektu: Polecenie zabezpieczające wydaje się w formie decyzji administracyjnej. Analogiczny przepis powinien obowiązywać w przypadku wydania ostrzeżenia tj. art. 67c pkt 1 powinien otrzymać brzmienie: "Pełnomocnik wydaje ostrzeżenia i polecenia zabezpieczające w formie decyzji administracyjnej". d) Kluczowy bowiem element zarówno ostrzeżenia, jak polecenia zabezpieczającego, tj. „określone zachowanie”, jest taki sam. Przepis art. 67c ust. 4 pkt 1 Projektu dotyczący polecenia zabezpieczającego, odsyła w zakresie „określonego zachowania” do art. 67b ust. 3 Projektu, który szczegółowo reguluje elementy określonego zachowania w przypadku wydawania ostrzeżenia. e) Brak odniesienia do postępowania administracyjnego w stosunku do czynności podejmowanych przez Pełnomocnika. Propozycja: Po ustępie 8 dodać ustęp 9: "Postępowanie przed pełnomocnikiem toczy się w oparciu o przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ostrzeżenie ma formę decyzji administracyjnej." f) W przypadku utrzymania tych narzędzi w pierwotnym kształcie, Pełnomocnik powinien zwracać koszty i ewentualne straty wynikające z wdrożenia rozwiązań wynikających z ostrzeżeń i poleceń zabezpieczających.	Przepisy art. 67a -67c zostaną zmienione. Ostrzeżenia w dalszym ciągu będzie wydawał Pełnomocnik. Natomiast polecenia zabezpieczające będą wydawane w formie decyzji administracyjnej przez ministra wł. ds. informatyzacji, co oznacza, że podmiot będzie mógł odwołać się od danej decyzji. Zatem także minister właściwy ds. informatyzacji będzie podejmował decyzje o ewentualnych karach także w formie decyzji administracyjnej. Przepis art. 73 zostanie uzupełniony o wysokość kary za nie zastosowanie się do polecenia zabezpieczającego. W myśl art. 26 ust. 3 pkt 4 zespoły CSIRT poziomu krajowego mogą wydać jedynie komunikaty o zidentyfikowanych zagrożeniach cyberbezpieczeństwa. Komunikat, o którym w art.

				26 ust 3 pkt 4 nie może być ostrzeżeniem, gdyż ostrzeżenie będzie dotyczyło możliwości wystąpienia incydentu krytycznego. W ostrzeżeniu Pełnomocnik nie tylko wskaże potencjalne zagrożenie, ale również zaleci sposób ograniczenia ryzyka wystąpienia incydentu krytycznego. Do tej pory ani Pełnomocnik ani zespoły CSIRT nie mogły wydawać ostrzeżeń w formie proponowanej w nowelizacji. Pełnomocnik może wydawać rekomendacje dla podmiotów krajowego systemu cyberbezpieczeństwa na podstawie art. 33 ustawy o ksc. Ostrzeżenie wydawane przez Pełnomocnika wskaże rodzaj zagrożenia, które uprawdopodobni wystąpienie incydentu krytycznego. Ponadto w ostrzeżeniu wskazane

				zostanie zakres podmiotowy, czyli Pełnomocnik określi, które podmioty dane ostrzeżenie dotyczy. Ostrzeżenie będzie zawierało także listę zalecanych działań, które podmioty powinny wdrożyć w celu ograniczenia ryzyk związanych z prawdopodobieństwem wystąpienia incydentu krytycznego. Przykładem takich zaleceń jest np. zwrócenie uwagi na określony typ zachowań czy incydentów. Pełnomocnik będzie przeprowadzał nie rzadziej niż raz na rok przegląd wydanych ostrzeżeń w celu ustalenia czy spełniają ustawową przesłankę ich wydania. Natomiast polecenie zabezpieczające odnosi się do sytuacji związanej z wystąpieniem incydentu krytycznego. Minister właściwy ds. informatyzacji w oparciu o informacje otrzymywane od m.in. zespoły CSIRT poziomu

				krajowego oraz ustalenia podjęte na Zepole ds. Incydentów Krytycznych będzie mógł podjąć decyzję o podjęciu konkretnych działań w związku z reagowaniem na incydent krytyczny. M. in. Nakaz określonego zachowania przez podmioty, których dotyczy polecenie w tym np. zabezpieczenie określonych informacji czy zakaz instalacji określonej wersji oprogramowania. Należy podkreślić, że szybkość reakcji w przypadku wystąpienia incydentu krytycznego jest kluczowa w procesie ograniczenia skutków tego incydentu.
52.	Konfederacja Lewiatan	Art. 67c	Art. 67c – polecenie zabezpieczające Z uwagi na nieodwracalne skutki wykonania polecenia zabezpieczającego z rygorem natychmiastowej wykonalności, ten rygor powinien być usunięty.	**Uwaga nieuwzględniona**, natychmiastowa wykonalnosc polecenia jest niezbędna, dla zapewnienia skuteczności polecenia.
53.	Izba Gospodarki Elektronicznej	Art. 66a-66c	Na podstawie projektowanych przepisów Kolegium do spraw cyberbezpieczeństwa będzie uprawnione do oceny ryzyka dostawcy sprzętu i oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. W przypadku, jeżeli dokonana ocena będzie wskazywała na istnienie wysokiego ryzyka, podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły wprowadzić do użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy. Będą także zobowiązane wycofać ten sprzęt lub oprogramowanie nie później niż w 5 lat	**Uwaga nieuwzględniona** Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania

			od dnia ogłoszenia komunikatu o ocenie. Takie rozwiązanie, niesie ze sobą daleko idące skutki i ważne jest zapewnienie rozwiązań, które pozwolą na niezakłócanie działalności przedsiębiorcy i nie będą powodować nadmiernego wzrostu kosztów prowadzenia działalności. Członkowie e-Izby postulują dodanie takich rozwiązań do Projektu.	technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci

				najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.
54.	Izba Gospodarki Elektronicznej	Art. 67a-67c	Proponujemy także, by Pełnomocnik Rządu ds. Cyberbezpieczeństwa przed wydaniem ostrzeżenia lub polecenia zabezpieczającego, o których mowa w projektowanym art. 67a, prowadził uprzednie konsultacje z podmiotami, na które działania te miałyby wpływ. Pozwoliłoby to na uzyskanie pełnego obrazu sytuacji, w tym poznanie racji zobowiązanego podmiotu.	**Uwaga nieuwzględniona**. Ostrzeżenie będzie niewiążącym zaleceniem podjęcia konkretnych działań ograniczających ryzyko zaistnienia incydentu krytycznego. Z kolei polecenie zabezpieczające będzie miało charakter decyzji administracyjnej a podmiot do którego zostało skierowane będzie mógł wnosić środki zaskarżenia.
55.	Izba Gospodarki Elektronicznej	Art. 73	Sankcje przewidziane w Projekcie są niezwykle dotkliwe. Ich nałożenie może w wielu przypadkach prowadzić do uniemożliwienia prowadzenia dalszego działania przez podmiot, na który nałożona będzie taka sankcja. Dlatego postulujemy weryfikację wysokości tych sankcji oraz określenie okoliczności,	Uawaga nieuwzględniona Kary, których wymiar odnosi się do obrotu światowego, są niezbędne

			które powinny być brane pod uwagę przy określaniu wysokości kar pieniężnych.	dla zapewnienia skuteczności przepisów, które mają na celu zwiększenie bezpieczeństwa narodowego.
56.	Konfederacja Lewiatan	Art. 73 ust. 2a	art. 2 pkt 31 projektu: Art. 73 ust. 2a Zaproponowany poziom kar pieniężnych jest zdecydowanie zbyt wysoki, a jednocześnie uderzająca jest dysproporcja możliwych kar nakładanych na sektor prywatny wobec kar, jakie za takie same naruszenia mogą obciążać podmioty publiczne -szczególnie w sytuacji, kiedy to w szczególności podmioty publiczne odpowiedzialne są za zapewnienie bezpieczeństwa w kluczowych obszarach definiowanych w aktualnej ustawie o krajowym systemie cyberbezpieczeństwa. Jednocześnie należy wykreślić odwołanie do obrotu „światowego". W przypadku działających w Polsce podmiotów, podlegających krajowym przepisom wysokość ewentualnych kar powinna odnosić się działalności tego podmiotu, a nie rodzić wątpliwości co do uwzględniania także skali działalności jego właścicieli, udziałowców lub akcjonariuszy realizowanej w ramach odrębnych formalnie podmiotów działających poza Polską.	Uawaga nieuwzględniona Kary, których wymiar odnosi się do obrotu światowego, są niezbędne dla zapewnienia skuteczności przepisów, które mają na celu zwiększenie bezpieczeństwa narodowego.
57.	Konfederacja Lewiatan	OSR	Uzupełnienie Oceny Skutków Regulacji W przedstawionym OSR nie została opisana kompleksowa i szczegółowa ocena skutków regulacji. Jednocześnie, za nieuzasadnione uznajemy tutaj potencjalne przyjęcie założenia, że ustawa sama w sobie nie prowadzi do wykluczenia jakichkolwiek dostawców. Ustawa daje do takich rozwiązań narzędzia, a sama możliwość ich zastosowania powinna zostać oceniona pod kątem możliwego wpływu. Każda, bowiem ocena skutków, musi odnosić się właśnie do potencjalnych skutków zastosowania wprowadzanych przepisów. W innym, bowiem przypadku zupełnie umyka sens jej prowadzenia. W tym ujęciu w naszej ocenie projekt ustawy będzie miał istotny wpływ na operatorów i dostawców (własność, ciągłość działalności, otoczenie biznesu, wolna konkurencja, gospodarka krajowa). 1) Potencjalny wpływ projektu ustawy na dostawców: a. Należy przeprowadzić i przedstawić analizę potencjalnego stosowania ustawy w zakresie rynku dostawców. b. Skrajne oceny mogą w związku z faktycznym wykluczeniem z rynku oznaczać istotną zmianę warunków konkurencji oraz dyskryminację niektórych	Uwaga częściowo uwzględniona, OSR zostanie uzupełniony. Często przywoływany jest argument, że operatorzy telekomunikacyjni w momencie wdrażania technologii sieci 5G (i kolejnych generacji) poniosą znaczne wydatki związane z ewentualnym zastąpieniem sprzętu lub oprogramowania pochodzącego od

			podmiotów. c. Zagrożenie to jest bardzo realne, szczególnie w kontekście zaproponowanych kryteriów oceny, które są ogólne i niewystarczająco oparte na normach technicznych i certyfikacji, takich jak NESAS i ENISA. d. Stąd, postulujemy doprecyzowanie mechanizmów oceny, w tym poprzez skupienie się na badaniu technicznych aspektów sprzętu i oprogramowania. 2) Potencjalny wpływ projektu ustawy na operatorów telekomunikacyjnych, w zakresie dot. oceny dostawców: a. Istotne zwiększenie poziomu niestabilności otoczenia prawnego i regulacyjnego, wpływające na zakres i tempo realizowanych inwestycji. b. Konieczność poniesienia kosztów finansowych i organizacyjnych związanych z potencjalnym wydaniem opinii przez Kolegium. c. Ograniczone tempo i zwiększenie kosztów realizacji inwestycji w sieć 5G, przede wszystkim z uwagi na brak jasnych i przewidywalnych w długim horyzoncie warunków dla realizacji inwestycji. d. Zwiększenie poziomu niepewności w zakresie procedur alokacji częstotliwości oraz ich warunków, w tym w zakresie kosztów i możliwości wykonania ewentualnych zobowiązań. Ryzyko dalszych opóźnień w obszarze pilnej wciąż potrzeby alokacji pasma C. e. Istotne ryzyko ograniczenia konkurencji na rynku dostawców urządzeń i oprogramowania wywoła naturalne dla takich sytuacji zwiększenie kosztów oraz ograniczenie możliwości negocjacji w toku procedur zakupowych. W efekcie spodziewany jest wzrost kosztów urządzeń i oprogramowania, wydłużenie okresów dostaw, a także ogólne pogorszenie warunków współpracy z dostawcami, których pozycja w wyniku stosowania ustawy może zostać wzmocniona. f. Nieodpowiednie, nieostrożne oraz niedostoswane do przedstawionych w niniejszym stanowisku postulatów stosowanie projektowanych przepisów, może w skrajnych przypadkach powodować ryzyko konieczności ograniczenia lub wręcz zaprzestania świadczenia usług telekomunikacyjnych przez konkretne podmioty na rynku. Skutki takich sytuacji mogą być dramatyczne zarówno w zakresie wpływu na dane przedsiębiorstwo, jak i wpływu na ciągłość świadczenia usług, w tym usług o kluczowym znaczeniu dla bezpieczeństwa państwa i obywateli. g. Wpływ na zawarte i obowiązujące, także wieloletnie umowy z dostawcami, które w wyniku opinii Kolegium musiałyby zostać rozwiązane lub zmienione. h. Operatorzy, jako podmioty prawa krajowego, niezależnie od oceny docelowych rozwiązań prawnych będą	dostawców wysokiego ryzyka. Należy wskazać, że w obecnej chwili żaden z operatorów w Polsce nie zapewnia łączności 5 generacji przy wykorzystaniu wyłącznie docelowych urządzeń lub oprogramowania, lecz bazuje na istniejącej infrastrukturze wykorzystywanej m.in. do łączności 4G (jest to tzw. model non-stand alone). Obecna infrastruktura nie jest wystarczająca do wykorzystania w pełni możliwości oferowanych przez technologie sieci 5G, w tym ultra-szybkiej wymiany danych. Ponadto, obecna infrastruktura podlega procesowi zużycia i docelowo będzie zastępowana rozwiązaniami dedykowanymi dla sieci najnowszej generacji (tzw. model stand alone). Przedsiębiorcy telekomunikacyjni zatem muszą w swoich planach inwestycyjnych już teraz uwzględniać koszty nie tylko

			zmuszeni do poddania się nowym regulacjom, co nie zamyka oczywiście drogi do możliwego kwestionowania wprowadzonych przepisów oraz związanych z tym konsekwencji, również o charakterze finansowym. i. W efekcie, ostatecznymi „beneficjentami" zastosowania projektowanych przepisów będą niestety użytkownicy usług telekomunikacyjnych, a także krajowa gospodarka, dla których usługi, szczególnie w zakresie sieci 5G będą dostępne później i bardzo prawdopodobne, że po wyższej cenie. j. Jednocześnie, w związku z projektem ustawy nie jest spodziewany wzrost bezpieczeństwa/cyberbezpieczeństwa na poziomie świadczonych usług telekomunikacyjnych. Głównym wektorem zagrożeń w tym zakresie są przede wszystkim aplikacje, złośliwe oprogramowanie oraz celowe działania przestępcze prowadzone przez jednostki lub podmioty zupełnie odrębne od samych dostawców urządzeń i oprogramowania sieciowego. Projekt ustawy nie adresuje jednak tych zagadnień. 3) Potencjalny wpływ projektu ustawy na konkurencję: a. Polska ma ograniczoną liczbę dostawców sieci. Jeśli jeden z dostawców zostanie wyłączony, będzie to szkodzić innowacjom w technologii i może odroczyć digitalizację Polski. b. Realny jest również wpływ na ceny i warunki współpracy z dopuszczonymi dostawcami, tj. wzrost kosztów urządzeń i oprogramowania, wydłużone okresy dostaw, utrudnienia w zakresie bieżącej obsługi. c. Rozważone powinny zostać również kwestie możliwego wpływu na koszty i jakość usług świadczonych konsumentom i innym odbiorcom. W każdym przypadku ograniczenie rynku wiąże się ze wzrostem cen, które ostatecznie będą obciążać użytkowników końcowych. 4) Potencjalny wpływ projektu ustawy na budżet Polski i gospodarkę krajową: a. potencjalna strata wskutek opóźnienia implementacji sieci 5G o 3 lata jest liczona w miliardach euro, ,w tym objęłaby ona wartość utraconych korzyści operacyjnych, korzyści konsumentów oraz innych podmiotów działających w sektorach takich jak przemysł samochodowy, służba zdrowia, transport oraz dostawy mediów. b. Utrzymujący się brak precyzyjnych ustaleń dot. bezpieczeństwa sieci, może mieć negatywny wpływ na przebieg i spodziewane efekty procedur alokacji częstotliwości radiowych. c. Potencjalne roszczenia o odszkodowanie wobec rządu polskiego podniesione przez dostawców zostaną ostatecznie wypłacone przez podatników i konsumentów. d. Negatywny wpływ na życie i pracę	wymiany infrastruktury, która kończy swój okres bezpiecznego użytkowania, lecz także muszą mieć plan wdrożenia infrastruktury dedykowanej sieci 5G.

			podczas pandemii i po pandemii: jeśli Polska opóźni wdrożenie 5G, straci możliwość stworzenia nowych miejsc pracy 5) Potencjalny wpływ projektu ustawy na postęp technologiczny: Wyłączenie któregokolwiek dostawcy, zwłaszcza w sytuacji ograniczonej podaży, spowoduje opóźnienie postępu w całym ekosystemie rozwoju cyfrowego. W naszej ocenie projekt ustawy będzie miał negatywny wpływ na rozwój Przemysłu 4.0. Opóźniona zostanie budowa niezbędnych kompetencji w obszarze samochodów podłączonych do sieci 5G, produkcji 5G, high-tech, rolnictwa 5G, usług portowych, zdalnej edukacji, sprzętu medycznego 5G, itp.	
58.	Osoba fizyczna	Art. 14 ust. 2	Czy powołanie SOC powinno nastąpić ponownie jeżeli powołano WSOC na mocy aktualnej ustawy?	**Uwaga nieuwzględniona** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi.

59.	Osoba fizyczna	Art. 14 ust 4	jeżeli OUK powołał wewnętrzny SOC, ale korzysta z niektórych usług utrzymania IT częściowo pokrywających się z wymaganiami dotyczącymi SOC (np. w zakresie aktualizowania systemów), to czy tego typu umowa podlega zgłoszeniu jako "prowadzenie SOC". Czy można uznać że w przypadku ust. 4 chodzi o pełne (lub pełniejsze – jakie?) powierzenie realizowania obowiązków OUK w zakresie wymaganym przez UKSC?	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator zawrze umowę na świadczenie tego typu usługi. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.

60.	Osoba fizyczna	Art. 14 stary ustęp 4	Czy celowo pominięto delegację ustawową do wydania rozporządzenia o warunkach organizacyjnych i technicznych ...?	**Wyjaśnienie** Od tej pory operatorzy usług kluczowych będą wdrażać zabezpieczenia na podstawie *risk based approach.*
61.	Osoba fizyczna	Art. 14 ust. 6	Zapis nie obejmuje SOC wewnętrznego. Czy nie warto zapewnić systemowo chociaż udostępniania kluczy publicznych wewnętrznych SOC i zasad szyfrowania komunikacji z podmiotami KSC?	**Wyjaśnienie** Kwestia wymiany informacji u operatora usługi kluczowej w tym w SOC operatora jest kwestią ustaleń wewnętrznych.
62.	Osoba fizyczna	Art. 14 ust 4	jeżeli OUK powołał wewnętrzny SOC, ale korzysta z niektórych usług utrzymania IT częściowo pokrywających się z wymaganiami dotyczącymi SOC (np. w zakresie aktualizowania systemów), to czy tego typu umowa podlega zgłoszeniu jako "prowadzenie SOC". Czy można uznać że w przypadku ust. 4 chodzi o pełne (lub pełniejsze – jakie?) powierzenie realizowania obowiązków OUK w zakresie wymaganym przez UKSC?	**Wyjaśnienie** Zespoły SOC są doprecyzowaniem aktualnie funkcjonującym „wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo” oraz zastępuje określenie „podmioty świadczące usługi na rzecz cyberbezpieczeństwa”. SOC będą realizowały zadania, które obecnie są realizowane przez wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którymi dany operator

				zawrze umowę na świadczenie tego typu usługi. Operator usługi kluczowej może zawrzeć umowę z kilkoma podmiotami realizujących inne zadania o których mowa w art. 14 ust.1.
63.	Osoba fizyczna	Art. 14 stary ustęp 4	Czy celowo pominięto delegację ustawową do wydania rozporządzenia o warunkach organizacyjnych i technicznych ...?	**Wyjaśnienie** Od tej pory operatorzy usług kluczowych będą wdrażać zabezpieczenia na podstawie *risk based approach.*
64.	Osoba fizyczna	Art. 14 ust. 6	Zapis nie obejmuje SOC wewnętrznego. Czy nie warto zapewnić systemowo chociaż udostępniania kluczy publicznych wewnętrznych SOC i zasad szyfrowania komunikacji z podmiotami KSC?	**Wyjaśnienie** Kwestia wymiany informacji u operatora usługi kluczowej w tym w SOC operatora jest kwestią ustaleń wewnętrznych.
65.	Osoba fizyczna	Art. 14a ust. 3	Ust. 3 - zakłada uzyskanie informacji o której mowa w art. 14 ust. 2, który nie przewiduje przekazywania informacji (w szczególności od OUK powołujących wewnętrzne SOC).	**Wyjaśnienie** Kwestia informowania organów właściwych przez operatorów usług kluczowych w sprawie zawarcia umowy na świadczenie usług cyberbezpieczeństwa z podmiotem zewnętrznym jest już uregulowana w

				ustawie o KSC w art. 14 ust. 3.
66.	Osoba fizyczna	Art. 20f	Brak określenia kontekstu w jakim miałoby dochodzić do stwierdzenia przesyłania komunikatów zagrażających bezpieczeństwu może implikować różne interpretacje w zakresie podmiotu uprawnionego do takiego stwierdzenia i podstawy analizy zawartości komunikatów (czy np. sam art. 20f daje podstawę do takiego analizowania komunikatów i oceny przedsiębiorcy komunikacji elektronicznej i w jakim zakresie).	**Uwaga nieuwzględniona** Podobny przepis funkcjonuje obecnie, jako art. 180 Prawa telekomunikacyjnego. Takie działanie możliwe jest w przypadku stwierdzenia zagrożenia dla bezpieczeństwa sieci i usług oraz tylko w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny zagrożenia. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
67.	Osoba fizyczna	Art. 66b ust. 1 pkt 2	Ust. 1 pkt. 2) mówi o wycofywaniu z użytkowania sprzętu, oprogramowania i usług określonych w ocenie danego dostawcy sprzętu lub oprogramowania w	**Wyjaśnienie**

			terminie 5 lat. Taka konstrukcja w ogólności może być podatna na wiele nadużyć. Z jednej strony może wystarczyć zmiana oprogramowania i nazwy linii produktowej np. po 4 latach od wydania opinii, by argumentować że nie są to przedmioty objęte opinią. Z drugiej strony taki zapis może oznaczać systemowe akceptowanie wysokiego ryzyka przez 5 lat.	Decyzja o uznaniu danego dostawcę za dostawcę wysokiego ryzyka będzie natychmiastowo wykonalna. Zawsze minister właściwy do spraw informatyzacji z urzędu lub na wniosek Przewodniczącego Kolegium będzie mógł wszcząć kolejne postępowanie administracyjne
68.	Osoba fizyczna	Art. 96 PZP	Ust. 1 i 2: w związku z dodaniem pkt. 3) do art. 96 ust. 2, zasadne byłoby rozszerzenie ust. 1 o aspekt bezpieczeństwa/cyberbezpieczeństwa.	**Wyjaśnienie** W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych.
69.	Osoba fizyczna	OSR Sekcja 6	W sekcji 6 opisano Budowę CSIRT sektorowych i CSIRT Telco, następnie wskazano zakładany katalog usług z roboczogodzinami. Po katalogu usług wskazano usługi SOCowe, etaty w SOC, koszty sprzętu w SOC itd. Czy wyliczenia te dotyczą budowy CSIRT sektorowych i CSIRT Telco czy zakładanego kosztu powoływania SOC o których mowa m.in. w art. 14 ustawy. Zakres i skala działalności SOC nie została aż tak precyzyjnie określona w samej UKSC jak w OSR (chyba że chodziło jednak o usługi i szacowane koszty organizacji CSIRT sektorowych na przykładzie kosztów usług SOC – niefortunnie będących słowem kluczowym na poziomie samej ustawy)?	**Wyjaśnienie** Chodzi o usługi SOC w ramach CSIRT sektorowych.

Zbiorcza tabela uwag do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (poprzedni tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa (UD68).

Nazwa projektu dokumentu: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (poprzedni tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, ustawy – Prawo telekomunikacyjne oraz ustawy – Ordynacja podatkowa (UD68).				
L.p.	**Podmiot wnoszący uwagi**	**Jednostka redakcyjna, do której wnoszone są uwagi**	**Zgłoszone uwagi**	**Stanowisko MC/DC**
1.	Biuro Bezpieczeństwa Narodowego	Uwaga ogólna	BBN pozytywnie opiniuje projekt ustawy	**Uwaga uwzględniona**
2.	Biuro Bezpieczeństwa Narodowego	Uwaga ogólna	Propozycja ustanowienia norm prawnych dla funkcjonowania centrów wymiany i analiz informacji (tzw. ISAC) i wpisania tych podmiotów w krajowy system cyberbezpieczeństwa zasługuje na akceptację. Współpraca podmiotów prywatnych z państwowymi przyczyni się do poprawy stanu cyberbezpieczeństwa.	**Uwaga uwzględniona**
3.	Biuro Bezpieczeństwa Narodowego	Uwaga ogólna	Za zasadne należy uznać także przyznanie Kolegium do Spraw Cyberbezpieczeństwa kompetencji do dokonywania oceny ryzyka dostawców sprzętu i oprogramowania (np. w odniesieniu do budowy sieci 5G w Polsce) pod katem zagrożenia dla bezpieczeństwa narodowego (nowy pkt 7 w art. 65 ust. 1 oraz art. 66a i 66b). W skład Kolegium wchodzą bowiem kluczowe organy administracji państwowej właściwe w zakresie bezpieczeństwa państwa i ich wspólne stanowisko w zakresie dopuszczenia na polski rynek określonego	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie

			sprzętu i oprogramowania powinno być kluczowe.	mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub

				oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
4.	Biuro Bezpieczeństwa Narodowego	Uwaga ogólna	Należy zauważyć także, ze elementy wymienione w dodawanym art. 66 ust. 4 pkt 2 ustawy, które będą brane pod uwagę przy sporządzeniu takiej oceny w stosunku do dostawców pochodzących z państw spoza Unii	**Wyjaśnienie** Tak taki był zamiar.

			Europejskiej lub NATO są zgodne z *Zaleceniami Komisji (UE) 2019/534 z dnia 26 marca 2019 r. - Cyberbezpieczeństwo sieci 5G* (Dz. U. L 88 z 29.3.2019, s. 42). Komisja Europejska wskazuje, ze działania państw członkowskich UE majce na celu wyeliminowanie zagrożeń dla cyberbezpieczenstwa w sieciach 5G powinny uwzględniać czynniki techniczne oraz czynniki innego rodzaju, takie jak m.in. ogólne ryzyko wywierania wpływu przez państwo trzecie, zwłaszcza w świetle funkcjonującego w nim modelu sprawowania rządów, brak porozumień między UE a danym państwem trzecim o wsp61pracy w zakresie cyberbezpieczeństwa, czy tez dotyczących ochrony danych osobowych oraz zwalczania cyberprzestąpczosci. Wedlug pkt 2.37 *Unijnej skoordynowanej oceny ryzyka* z 9 pazdziemika 2019 r. *(EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks)* ryzyka poszczególnych dostawców państwa UE mogą ocenić w oparciu o szereg czynników. Należy brać pod uwagę fakt, iż określony dostawca może podlegać silnym niekorzystnym wpływom państwa spoza UE, wynikającym z powiązania tego dostawcy z rządem takiego państwa np. z uwagi na jego strukturę własnościową.	
5.	Biuro Bezpieczeństwa Narodowego	Uwaga ogólna	W ocenie Biura Bezpieczeństwa Narodowego uzasadnione jest również wyposażenie Pełnomocnika do spraw Cyberbezpieczeństwa w nowe narzędzie prawne jakim jest możliwość wydawania ostrzeżeń i poleceń zabezpieczających	**Wyjaśnienie** Ostrzeżenie jako miękki środek będzie wydawał Pełnomocnik

			(projektowany art. 67a i następne ustawy o krajowym systemie cyberbezpieczeństwa).	
6.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	W związku z pracami nad projektem ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych, w celu uniknięcia wprowadzenia sprzecznych uregulowań z dotyczącymi bezpieczeństwa sieci i usług, zawartymi w projekt ustawy - Prawo komunikacji elektronicznej, zwracam się z uprzejmą prośbą o określenie w sposób kompleksowy, jednoznaczny oraz spójny, w jednym akcie prawnym, kwestii z zakresu: bezpieczeństwa sieci i usług oraz cyberbezpieczeństwa odnośnie mikro przedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej.	**Wyjaśnienie** Kwestie dotyczące bezpieczeństwa sieci i usług komunikacji elektronicznej oraz cyberbezpieczeństwa docelowo znajdą się w jednym akcie prawnym – w ustawie o krajowym systemie cyberbezpieczeństwa. Przepisy dotyczące przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług komunikacji elektronicznej zostaną dodane do uKSC za pomocą ustawy wprowadzającej PKE.
7.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Jednocześnie zwracam się z uprzejmą prosbą o pilne uzupełnienie dostrzeżonych braków w Projekcie. Pragnę wskazać, ze przy opracowaniu Projektu pominięto istotne wymogi dotyczące tworzenia przepisów prawa wynikające z ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Konstytucja Biznesu)": Art. 66 ust 1 pkt 2, który stanowi, ze „Przed rozpoczęciem prac nad opracowaniem projektu aktu normatywnego określającego zasady podejmowania, wykonywania ub zakończenia działalności gospodarczej dokonuje się oceny przewidywanych skutków społeczno-gospodarczych, w tym oceny wpływu na mikroprzedsiębiorców, małych i średnich przedsiębiorców oraz analizy zgodności projektowanych regulacji z przepisami ustawy".	**Uwaga uwzględniona,** zostanie to uzupełnione w OSR.

			Ponadto zgodnie z art. 66 ust 2: „ Wyniki oceny i analiz, o których mowa w ust. 1, zamieszcza się w uzasadnieniu do projektu aktu normatywnego lub w ocenie skutków regulacji, *stanowiącej odrębną część uzasadnienia projektu aktu normatywnego ".* Konstytucja Biznesu ma charakter gwarancyjny dla ok. 6000 mikro przedsiębiorców, małych i średnich przedsiębiorców z branży telekomunikacyjnej. W przypadku stwierdzenia wpływu projektu aktu normatywnego na najmniejsze firmy *„przy opracowaniu projektu aktu normatywnego dąży się do proporcjonalnego ograniczania obowiązków administracyjnych wobec tych przedsiębiorców albo uzasadnia brak możliwości zastosowania takich ograniczeń"* (art. 68 Prawa przedsiębiorców), co należy powiązać z zasadami proporcjonalności i adekwatności, a w szczególności należy: *„dążyć do nienakładania nowych obowiązków administracyjnych, a jeżeli nie jest to możliwe, dążyć do ich nakładania jedynie w stopniu koniecznym do osiągniecia ich celów"* (art. 67 pkt 1 Prawa przedsiębiorców).	
8.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Dodatkowo w art. 40 ust. 1 Europejskiego kodeksu łączności elektronicznej wskazuje się, na konieczność uwzględniania we wprowadzanych uregulowaniach zasady proporcjonalności przez Państwa członkowskie w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Art. 40 ust. 2 EKLE stanowi, ze aby określić istotność wpływu danego incydentu związanego z bezpieczeństwem, uwzględnia się w	**Wyjaśnienie** Przedsiębiorcy komunikacji elektronicznej zostaną zobowiązani do wdrożenia adekwatnych (proporcjonalnych) do oszacowanego ryzyka środków technicznych lub organizacyjnych mających zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorcy ci będą musieli obsługiwać incydent telekomunikacyjny (co jest

			szczególności następujące parametry, gdy są dostępne: a) liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem; b) czas trwania incydentu związanego z bezpieczeństwem; geograficzny zasięg obszaru dotkniętego incydentem związanym z bezpieczeństwem; d) zakres wpływu na funkcjonowanie sieci lub usługi; e) zakres wpływu na działalność ekonomiczną i społeczną.	w ich dobrym interesie) a zgłaszać do CSIRT Telco i CSIRT poziomu krajowego te incydenty telekomunikacyjne, które będą spełniać progi incydentu.
9.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Dotychczas wprowadzane obowiązki w zakresie obowiązku sporządzania i posiadania planu działań w sytuacjach szczególnego zagrożenia nie obejmują mikroprzedsiębiorcow. Uregulowania te powinny zyskać rangę ustawową, ponieważ w obecnej wersji projektu zmiany ustawy o krajowym systemie cyberbezpieczeństwa brak jednoznacznego odniesienia dotyczącego konieczności kontynuacji tych wyłączeń wobec najmniejszych firm. Dodatkowego rozważenia wymagałaby możliwość objęcia tymi włączeniami małych i średnich przedsiębiorców oraz zastosowania ww. wyłączenia w powiązanych regulacjach dotyczących bezpieczeństwa sieci i usług.	**Uwaga bezprzedmiotowa.** Uwaga ta dotyczy ustawy Prawo komunikacji elektronicznej, która reguluje te kwestie.
10.	Rzecznik Małych i Średnich Przedsiębiorców	Uwaga ogólna	Nakłady związane z bezpieczeństwem sieci, usług i cyberbezpieczeństwem należą do istotnie obciążających najmniejsze krajowe firmy, które posiadają mniej rozbudowane struktury	**Wyjaśnienie** Przepisy prawa o których mowa w uwadze zostały przeniesione do ustawy wprowadzającej PKE.

			administracyjne niż międzynarodowe korporacje. Istnienie tych najmniejszych firm gwarantuje jednak istnienie realnej konkurencji na rynku usług komunikacji elektronicznej (w przeciwieństwie do większości państw europejskich, co przekłada się na niższe ceny i wyższą jakość usług oferowanym konsumentom. Jak stwierdzono w uzasadnieniu do samego projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych (UD68) (str. 33): *„Poprzez nałożenie różnych obowiązków na przedsiębiorców będących podmiotami tego systemu ogranicza się konstytucyjną wolność gospodarczą. Zobowiązuje bowiem tych przedsiębiorców do dbania o cyberbezpieczeństwo. Po stronie przedsiębiorców powoduje to koszty związane z koniecznością dostosowania się do wymogów ustawy ".* W związku z powyższym wymagana jest modyfikacja stwierdzenia na str. 44 uzasadnienia do projektu ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy - Prawo zamówień publicznych, że: „ *Zawarte w projekcie regulacje nie będą miały wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców zgodnie z art. 66 ust. 2 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców (Dz. U. 2019r. poz. 1292, z poźń. zm.)."* i wprowadzenie stosownych uzupełnień z rozważeniem możliwych wyłączeń lub ograniczeń obowiązków nakładanych na najmniejsze firmy.	

11.	Prezes Urzędu Komunikacji Elektronicznej	Uwaga ogólna	W nawiązaniu do projektowanej regulacji, która m.in. dokonuje wdrożenia części przepisów dyrektywy 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (dalej: EKŁE), należy wskazać na przepisy art. 40 i 41 tej dyrektywy, określające zarówno obowiązki podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej, jak i obowiązki właściwych organów krajowych w zakresie bezpieczeństwa sieci i usług. Obowiązki te dotyczą w szczególności: • informowania właściwych organów innych państw członkowskich oraz ENISA w przypadku istotnych incydentów bezpieczeństwa, • podawania informacji o incydencie do wiadomości publicznej, jeśli będzie leżało to w interesie publicznym, • przekazywania rocznego sprawozdania podsumowującego otrzymane zgłoszenia i podjęte działania w związku z zaistniałymi incydentami do Komisji Europejskiej i ENISA. W celu realizacji powyższych obowiązków niezbędne jest posiadanie przez właściwy organ krajowy informacji o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług, przekazywanych przez podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej.	**Wyjaśnienie** Implementacja dyrektywy EKŁE zostanie zrealizowana poprzez ustawę PKE oraz dokonanie odpowiednich zmian w ustawie o ksc (kwestie dotyczące bezpieczeństwa sieci i usług oraz włączenie przedsiębiorców komunikacji elektronicznej do podmiotów ksc). Kwestia właściwej implementacji EKŁE jest zsynchronizowana.

			EKŁE nie wskazuje czy właściwym organem krajowym powinien być regulator rynku telekomunikacyjnego czy inny organ. Projekt ustawy - Prawo komunikacji elektronicznej (dalej: projekt Pke), przekazany w dniu 29 lipca br. do uzgodnień międzyresortowych, konsultacji publicznych i opiniowania przewidywał model, w którym rolę właściwego organu spełniał regulator rynku, a podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej przekazywały mu informacje niezbędne do realizacji nałożonych obowiązków. Natomiast w przedstawionej do zaopiniowania nowelizacji zamieszczono szereg przepisów dotyczących przekazywania informacji o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług (co najprawdopodobniej będzie wiązało się z usunięciem z projektu Pke m.in. art. 39, 42, 43 ust. 2 i 3 oraz art. 44). Zgodnie z przepisami ustawy o krajowym systemie cyberbezpieczeństwa (dalej: UKSC), w brzmieniu nadawanym projektowaną ustawą, głównymi podmiotami, do których będą wpływać informacje o incydentach są CSIRT TELCO (projektowany art. 20c ust. 3 UKSC) oraz CSIRT MON, CSIRT NASK i CSIRT GOV (projektowany art. 20c ust. 1 pkt 2 UKSC). Ponadto informacje mogą być uzupełniane na żądanie ww. CSIRT (projektowany art. 20d ust. 4 UKSC). Brak jest w tych przepisach obowiązku przekazywania informacji Prezesowi UKE; w projektowanym art.	

			34a UKSC wskazano jedynie, iż CSIRT współpracują z Prezesem UKE, a informacje o incydencie otrzymuje on wyłącznie na żądanie (w tym kontekście niejasna jest wytyczna do wydania rozporządzenia wskazana w projektowanym art. 20c ust. 4 UKSC). Należy przy tym zaznaczyć, że część przepisów dotyczących obowiązków właściwego organu krajowego nadal pozostanie w projekcie Pke i będą to obowiązki Prezesa UKE (np. określone w art. 40 i 46 projektu Pke). Pojawia się zatem wątpliwość czy taki model transpozycji EKŁE do krajowego porządku prawnego zapewni możliwość właściwego wykonywania obowiązków przez Prezesa UKE.	
12.	Prezes Urzędu Komunikacji Elektronicznej	Uwaga ogólna	Należy poddać pod wątpliwość zasadność przeniesienia z projektu Pke do UKSC definicji pojęcia „bezpieczeństwo sieci i usług”, niezwiązanej z wprowadzanym projektowaną ustawą do UKSC pojęciem „incydent telekomunikacyjny” (w Pke definicję tę związano z pojęciem incydentu bezpieczeństwa). Opcjonalnym rozwiązaniem jest zmiana zaproponowanej definicji incydentu telekomunikacyjnego w ten sposób by odpowiadał on definicji incydentu bezpieczeństwa z projektu PKE. Definicje incydentu bezpieczeństwa i bezpieczeństwa sieci i usług w projekcie Pke zostały zaprojektowane z uwzględnieniem definicji EKŁE (tak by były ze sobą powiązane) i po długotrwałych dyskusjach, mających na celu harmonizację transpozycji narodowych tych pojęć, prowadzonych przez	**Uwaga uwzględniona, definicja incydentu telekomunikacyjnego zostanie poprawiona na wzór definicji incydentu z EKŁE.**

			grupę roboczą do spraw art. 13 w ramach ENISA. Wprowadzenie nowego pojęcia „incydent telekomunikacyjny" niezgodnego z pojęciem „incydent bezpieczeństwa", zaproponowanym w Pke, może spowodować nieprawidłową transpozycję EKŁE (problemy interpretacyjne, niewłaściwe raportowanie incydentów przez zobowiązane podmioty, utrudnienia we współpracy europejskiej w zakresie informowania o incydentach innych państw członkowskich i ENISA);	
13.	Prezes Urzędu Komunikacji Elektronicznej	Uwaga ogólna	Należy wskazać na brak jednoznacznie przypisanej właściwości CSIRT sektorowych i CSIRT Telco w odniesieniu do przedsiębiorców telekomunikacyjnych wchodzących w skład innych sektorów, np. sektora Infrastruktura Cyfrowa (dot. operatorów IXP). Ustawa wprowadza obowiązek utworzenia CSIRT sektorowego, więc dla tych przedsiębiorców telekomunikacyjnych będzie właściwy zarówno CSIRT IC, jak i CSIRT Telco.	**Uwaga nieuwzględniona** CSIRT Telco będzie właściwy dla przedsiębiorców komunikacji elektronicznej w zakresie incydentów dotyczących bezpieczeństwa sieci i usług komunikacji elektronicznej. Innym zakresem będzie dotyczyć właściwość CSIRT sektorowego dla sektora infrastruktury cyfrowej.
14.	Agencja Wywiadu	Uwaga ogólna	Ponadto, Agencja Wywiadu poddaje pod rozwagę ewentualne doprecyzowanie roli i funkcji CSIRT sektorowego. Należy bowiem zauważyć, że w świetle projektowanych przepisów CSIRT sektorowy nie ma możliwości zlecenia pełnienia swoich zadań podmiotom spoza administracji rządowej, np. spółkom z udziałem Skarbu Państwa.	**Uwaga nieuwzględniona** CSIRT sektorowy ma być powołany przez organ właściwy dla danego sektora lub podsektora Ten organ będzie decydował która z jednostek przez niego nadzorowanych lub mu podlegająca będzie wykonywać zadania CSIRT sektorowego. Będzie miał także możliwość wyznaczenia innego podmiotu. Innymi słowy to organ właściwy ma zdecydować który podmiot ma pełnić funkcję CSIRT sektorowego. Sam CSIRT nie powinien zlecać

				pełnienia swoich zadań innym podmiotom.Dla zapewnienia sprawności działania CSIRT ważne jest, aby zadania SOC i CERT były realizowane w ramach jednego podmiotu, a nie w modelu rozproszonym.
15.	Prezes Urzędu Ochrony Danych Osobowych	Art. 1 pkt 5	Z punktu widzenia unormowań *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.1)), powoływanego dalej z zastosowaniem skrótu „RODO", **doprecyzowania wymagają wprowadzane przez projekt ustawy nowelizującej – przepisy dotyczące danych kontaktowych**. Skoro bowiem – stosownie do dyspozycji art. 5 ust. 1 lit. c RODO – dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"), to – celem zagwarantowania zgodności z tą zasadą dotyczącą przetwarzania danych osobowych – zachodzi potrzeba wskazania katalogu danych, które Projektodawca uznaje za „dane kontaktowe" osoby reprezentującej ISAC zamieszczone w wykazie ISAC [art. 4a ust. 3 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369).	**Uwaga uwzględniona, przepis zostanie doprecyzowany.**

16.	Prezes Urzędu Ochrony Danych Osobowych	Art. 1 pkt 10	Za wprowadzeniem do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (przez odpowiednią zmianę tej ustawy przewidzianą w przepisach projektu ustawy nowelizującej) katalogu danych uznawanych przez Projektodawcę za „dane kontaktowe" przemawia przy tym okoliczność, iż w art. 14 ust. 6 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (w brzmieniu nadanym przez art. 1 pkt 10 projektu ustawy nowelizującej) pojęcie „danych kontaktowych" zostało potraktowane przez Projektodawcę jako pojęcie otwarte. Takie rozumienie pojęcia „danych kontaktowych", na gruncie – przytaczanej wyżej – zasady minimalizacji danych, organ właściwy w sprawie ochrony danych osobowych uznaje za niewłaściwe i dlatego wskazuje potrzebę doprecyzowania przepisów dotyczących danych kontaktowych. Jeśli zaś zamiarem Projektodawcy jest wprowadzenie w poszczególnych przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa różnych katalogów danych składających się na pojęcie „danych kontaktowych" (w konkretnym przepisie tej ustawy), to takie rozwiązanie musi również znaleźć odzwierciedlenie w projekcie ustawy nowelizującej.	**Uwaga uwzględniona, przepis zostanie doprecyzowany**
17.	Prezes Urzędu Ochrony Danych Osobowych	Art. 1 pkt 14	**Doprecyzowania wymaga sformułowanie „dane kontaktowe" osób z poszczególnych podmiotów publicznych w województwie, wskazanych przez kierownictwo tych podmiotów, do współpracy z właściwymi CSIRT MON, CSIRT NASK lub CSIRT GOV** (art. 24a	**Uwaga uwzględniona, przepis zostanie doprecyzowany.**

			pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa	
18.	Komisja Nadzoru Finansowego	Art. 2 pkt 8f	8f) bezpieczeństwo sieci i usług -– zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania ~~wszelkich~~ działań naruszających dostępność, autentyczność, integralność lub poufność: (…) Użycie słowa ***wszelkich*** (za słownikiem PWN: *wszelki – każdy, jaki tylko istnieje, każdy bez wyjątku, każdy możliwy*) jest w opinii KNF zbyt daleko idące, ponieważ powoduje, że w takim rozumieniu żadna sieć i usługi nie byłyby uznane za bezpieczne. Proponujemy wykreślenie słowa ***wszelkich***, co byłoby zgodne z terminem przywołanym w uzasadnieniu projektu do zmiany ustawy (str. 35).	**Uwaga nieuwzględniona.** Przepis nie mówi o tym, że sieci mają być odporne na wszelkie działania tylko, że mają mieć zdolność do odpierania. Nie jest zamiarem projektodawcy, żeby stworzyć sieci lub usługi, w których nigdy nie dojdzie do negatywnego zdarzenia, bo jest to niemożliwe. Celem jest nałożenie obowiązków stosowania metod i narzędzi służących do odpierania tych zdarzeń.
19.	Najwyższa Izba Kontroli	Art. 4	Proponuję dodać do art. 4 ustawy o KSC Państwowe Gospodarstwo Wodne Wody Polskie, które jest państwową osobą prawną jak Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej. PGW WP utworzone zostało z dniem 1 stycznia 2018 r.	**Uwaga uwzględniona**
20.	Biuro Bezpieczeństwa Narodowego	Art. 4a	Wymaga dopracowania pod względem prawnym i legislacyjnym. w szczególności: 1) należałoby wskazać, iż ISAC „funkcjonuje" w ramach krajowego systemu cyberbezpieczeństwa, zamiast „może funkcjonować". ISAC może być utworzony (fakultatywnie, bo nie przewiduje się obowiązku działania), ale gdy już powstanie powinien	**Uwaga nieuwzględniona** ISAC są inicjatywą dobrowolną. Ustawa celowo nie nakłada wiele obowiązków na ISAC aby były łatwe do utworzenia i dodania w ramach KSC. Podkreślić należy, że do tej pory można było tworzyć ISAC w różnych formach prawnych – ustawa daje tylko możliwość dodania ISAC do KSC.

			obligatoryjnie funkcjonować w krajowym systemie cyberbezpieczeństwa; 2) czy nie byłoby wskazane określenie w przepisach ustawy formy prawnej, w jakiej funkcjonuje ISAC: czy podmioty te tworzone są na podstawie umowy między przedsiębiorcami? Jak i kto je tworzy? Z omawianego projektu ustawy wynika, ze wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych wykazie ISAC jest czynnością materialno-techniczną. Zatem wpis do wykazu nie tworzy tego podmiotu i *de facto* nie ma znaczenia dla jego statusu; 3) nie jest jasne dlaczego w art. 4a ust. 3 pkt 3-5 dopuszcza się fakultatywność posiadania przez ISAC siedziby i adresu, NIP oraz numeru w rejestrze.	Wykaz ISAC ma zawierać dane w tym numer rejestru (np. numer KRS), jeżeli został nadany.
21.	Komisja Nadzoru Finansowego	Art. 4a ust 4	**Propozycja zmiany:** Wpisanie do wykazu ISAC i wykreślenie z tego wykazu następuje na wniosek podmiotu prowadzącego ISAC po uzyskaniu pozytywnej opinii CSIRT MON, CSIRT NASK lub CSIRT GOV oraz **organu właściwego dla sektora, w którym będzie działał ISAC.** **Uzasadnienie:** Uwzględnienie przez ministra właściwego do spraw informatyzacji opinii organu właściwego wyspecjalizowanego w funkcjonowaniu sektora, w którym planuje działać ISAC. Ponadto konieczne jest zdefiniowanie przez Ustawodawcę kryteriów oceny dokonywanej przez zespoły CSIRT i OW. Zgodnie z zaproponowanymi zmianami do Ustawy informacje przedstawione	**Uwaga częściowo uwzględniona** ISAC mogą działać na rzecz podmiotów z różnych sektorów jak również podmiotów spoza krajowego systemu cyberbezpieczeństwa. W nowej wersji projektu zrezygnowano z opiniowania ISAC przez CSIRT poziomu krajowego natomiast będą opiniować wszystkie organy właściwe do spraw cyberbezpieczeństwa.

			przez podmiot ubiegający się o statut ISAC zawierają jedynie dane teleadresowe co nie daje podstaw do wydania pozytywnej opinii przez CISRTy oraz OW.	
22.	Komisja Nadzoru Finansowego	Art. 4a ust. 9	**Propozycja zmiany:** ISAC współpracują z CSIRT MON, CSIRT NASK, CSIRT GOV **i CSIRT sektorowymi oraz organem właściwym dla danego sektora, a także** przedkładają ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy. **Uzasadnienie:** Uzasadnione wydaje się rozszerzenie katalogu podmiotów, z którymi możliwa będzie współpraca ISAC w ramach krajowego systemu cyberbezpieczeństwa.	**Uwaga uwzględniona,** przepis zostanie zmieniony.
23.	Komisja Nadzoru Finansowego	Art. 14 ust. 6	**Propozycja zmiany:** Podmiot niebędący operatorem usługi kluczowej, prowadzący SOC udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności: 1) nazwa SOC i posiadanych przez SOC kompetencji; 2) zakres właściwości, w tym: a) oferowany rodzaj wsparcia, b) zasady współpracy i wymiany informacji, c) politykę komunikacji i uwierzytelniania informacji; 3) oferowane usługi, w tym politykę obsługi incydentów i koordynacji incydentów;	**Uwaga częściowo uwzględniona** Projekt nawiązuje do praktyki rynkowej – udostępniania informacji według wzoru dokumentu RFC 2350. Sformułowanie *zakres właściwości* zostało zastąpione sformułowaniem *zakres obszaru działania.*

			4) dane kontaktowe, w tym: a) adres ze wskazaniem strefy czasowej, b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC, c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC, d) sposoby kontaktu z SOC, w tym sposób zgłaszania incydentów. **Uzasadnienie:** Ta regulacja jest sprzeczna z podstawowymi zasadami ochrony informacji wrażliwych. W opinii UKNF, Ustawa powinna wręcz zakazywać podmiotom świadczącym usługi SOC udostępnianie na stronie internetowej tak szerokiego katalogu informacji, oraz obligować OUK do wprowadzenia do umów zawieranych z takimi podmiotami obowiązku ochrony informacji oraz zachowania pełnego NDA. Informacje o tym, który operator SOC świadczy usługi dla OUK w prostej drodze prowadzi do wykorzystania tych informacji jako wektora ataków, ukierunkowanego w pierwszej kolejności na SOC, a na dalszym etapie na OUK. W sytuacji, w której SOC będzie świadczył swoje usługi więcej niż jednemu OUK (istnieje również możliwość, że będą to OUK z różnych sektorów gospodarki) generuje to w opinii UKNF wysokie ryzyko ukierunkowania działań cyberprzestępczych na te podmioty.	

24.	Najwyższa Izba Kontroli	Pkt 12 - art. 20a ust. 3, art. 20 c ust. 1 pkt 1	Dopisać – „ustawa z dnia ... - Prawo komunikacji elektronicznej".	**Uwaga uwzględniona**
25.	Najwyższa Izba Kontroli	pkt 15 - art. 26 ust.2, ust. 3 pkt 21; pkt 16 - art.32 ust. 4; pkt 26 - art. 46 ust. 2b oraz pkt 29 - art. 66c ust.1	Zostało wprowadzone pojęcie „podmiot krajowego systemu cyberbezpieczeństwa", które to podmioty wymienione są w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa (zwana dalej „ustawa o KSC"). Projektodawca w ww. przepisach nie odnosi się konkretnie, których podmiotów - wymienionych w art. 4 ustawy **o** KSC – dotyczą te przepisy. Czy dotyczy to wszystkich wymienionych w art. 4 ustawy o KSC czy tez niektóre podmioty powinny zostać wyłączone? Ponadto np. z pkt 15 - art. 26 ust.2 i ust. 3 pkt 21; pkt 16 - art. 32 ust. 4 niniejszego projektu CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i CSIRT Telco, które są podmiotami objętymi krajowym systemem cyberbezpieczeństwa, wynika jakby nie byty one tymi podmiotami. Natomiast w pkt 30 - art. 67a ust. 4 pkt 1 odniesiono się do konkretnych punktów w art. 4 ustawy o KSC. W świetle powyższego należy się zastanowić, czy może zastosować we wszystkich przepisach, do których jest odniesienie do podmiotów objętych krajowym systemem cyberbezpieczeństwa zasadę, ze przywoływany jest art. 4 ze stosownymi punktami. Należy również rozważyć wprowadzenia zamiast pojęcia „podmiot krajowego systemu cyberbezpieczeństwa" pojęcie „podmiot objęty	**Wyjaśnienie** Użyte sformułowanie *podmiot krajowego systemu cyberbezpieczeństwa* odnosi się do katalogu podmiotów określonego w art. 4.

			krajowym systemem cyberbezpieczeństwa", co byłoby zgodne z art. 4 ustawy o KSC.	
26.	Najwyższa Izba Kontroli		W pkt 15 lit. d - należy dodać art. 42 ust. 8 - pkt 23 niniejszego projektu i zamiast lit. d) w tym punkcie utworzyć nowy punkt, bowiem odnosi się nie tylko do art. 26, albo wyłączyć z pkt 15 lit. d art, 49 ust. 3 pkt 2 i po pkt 26 utworzyć nowy punkt.	**Uwaga uwzględniona**
27.	Najwyższa Izba Kontroli	Art. 1 pkt 24 lit c - art. 44 ust. 6 i art. 2 PZP	W danych promulgacyjnych dopisać Dz. U. z 2020 r. poz. 288 i 1492.	**Uwaga uwzględniona**
28.	Prezes Urzędu Komunikacji Elektronicznej	Art. 20a	Niejasny jest cel przeniesienia przepisów art. 39 projektu Pke do projektowanego art. 20a UKSC. Przepisy te stanowią całość i są tematycznie związane z dalszymi przepisami projektu Pke, a w szczególności z art. 40 i 41 projektu Pke.	**Wyjaśnienie** Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Celem ustawy jest ujednolicenie kwestii raportowania o incydentach na poziomie krajowych. EKŁE stanowi w art. 40 ust. 2, że przedsiębiorcy komunikacji elektronicznej mają zgłaszać incydenty do właściwych organów, które mogą być inne niż krajowe organy regulacyjne. Usługi świadczone przez przedsiębiorców komunikacji elektronicznej mają kluczowe znaczenie dla niezakłóconego świadczenia usług przez operatorów usług kluczowych, dostawców usług cyfrowych czy też administrację publiczną czyli innych podmiotów krajowego systemu cyberbezpieczeństwa.

				Stąd też do ustawy o krajowym systemie cyberbezpieczeństwa zostały dodane obowiązki przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci i usług oraz zgłaszania incydentów. Pozostałe obowiązki przedsiębiorców pozostały w PKE.
29.	Prezes Urzędu Komunikacji Elektronicznej	Art. 34a Art. 20a Art. 20c Art. 46	Proponuje się uzupełnienie projektu o wymóg niezwłocznego informowania Prezesa UKE o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług – w taki sposób, aby było to dokonywane przez CSIRT TELCO albo przez podmioty zobowiązane równocześnie z poinformowaniem CSIRT TELCO. Proponuje się także dodanie przepisów obligujących podmioty zobowiązane do przekazywania informacji uzupełniających o incydentach na żądanie Prezesa UKE. Należy bowiem zaznaczyć, że zaproponowane rozwiązanie (projektowany art. 34a UKSC), polegające na przekazywaniu przez CSIRT'y Prezesowi UKE informacji o incydentach jedynie na jego żądanie, przy jednoczesnym pozostawieniu w projekcie Pke rozwiązań nakładających na Prezesa UKE obowiązek informowania innych państw członkowskich, Komisji Europejskiej i ENISA o incydentach (art. 46 projektu Pke), czyni obowiązek Prezesa UKE trudnym do wykonania lub wręcz niewykonalnym. Ponadto zaproponowane w projekcie UKSC rozwiązanie polegające na przeniesieniu z projektu Pke obowiązków przedsiębiorców komunikacji elektronicznej do	**Wyjaśnienie** Procedura przekazywania informacji o incydencie telekomunikacyjnym zostanie ustalona przez CSIRT krajowe i CSIRT Telco oraz Prezesa UKE. Incydenty zgłaszane przez przedsiębiorców komunikacji elektronicznej będą zgłaszane do CSIRTu Telco, który zapewni bezpośrednie wsparcie w reagowaniu na incydent telekomunikacyjny oraz równocześnie do właściwego CSIRT poziomu krajowego, który zapewni koordynację obsługi tego incydentu. Należy podkreślić, że CSIRT poziomu krajowego dysponuje najpełniejszą wiedzą o poziomie ryzyka w skali kraju, stąd też jest w stanie ocenić, czy dany incydent telekomunikacyjny jest jednocześnie incydentem krytycznym. Prezes UKE nie ma kompetencji operacyjnych. CSIRT Telco oraz CSIRT poziomu krajowego będą przekazywać informacje Prezesowi UKE o incydentach telekomunikacyjnych, w celu wypełnienia obowiązku informowania organów innych państw o istotnych incydentach oraz

			podejmowania określonych środków i przekazywania informacji o incydentach telekomunikacyjnych (projektowane art. 20a i 20c UKSC) przy jednoczesnym pozostawieniu w projekcie Pke kompetencji Prezesa UKE do ich kontroli i penalizacji (art. 385 i art. 409 projektu Pke) czyni tę kompetencję Prezesa UKE wątpliwą pod względem efektywnej realizacji.	obowiązku sprawozdawczego wobec m.in. ENISA.
30.	Komisja Nadzoru Finansowego	Art. 41 pkt 4	**Propozycja zmiany:** dla sektora bankowego i infrastruktury rynków finansowych - **Komisja Nadzoru Finansowego;** **Uzasadnienie:** Organem właściwym dla sektora bankowego i infrastruktury rynków finansowych powinna zostać **Komisja Nadzoru Finansowego. Zgodnie z art. 3 ust. 1 ustawy o nadzorze nad rynkiem finansowym „**Urząd Komisji *Nadzoru Finansowego*, zwany dalej "Urzędem Komisji", jest państwową osobą prawną, której zadaniem jest zapewnienie obsługi Komisji *Nadzoru Finansowego* i Przewodniczącego Komisji *Nadzoru Finansowego”*. Organem uprawnionym do wykonywania władzy publicznej jest KNF, dlatego tylko KNF może być organem właściwym dla sektora bankowego i infrastruktury rynków finansowych.	**Uwaga uwzględniona.**
31.	Komisja Nadzoru Finansowego	Art. 41 pkt 12 Propozycja KNF	**Propozycja zmiany:** 12) dla SOC wykonujących usługi na zlecenie operatora usług kluczowych - minister właściwy do spraw informatyzacji. **Uzasadnienie:**	**Uwaga uwzględniona**

			W opinii KNF to minister właściwy do spraw informatyzacji powinien zostać wskazany jako organ właściwy dla SOC świadczących usługi na zlecenie OUK. Koreluje to z dalszą propozycją zmiany art. 74 ust. 1a pkt. 4 (nakładanie kar). Brak określenia w art. 41 organu właściwego dla „zewnętrznych" SOC, działających na zlecenie OUK, może w pewnych warunkach generować problemy natury formalnej – opisane poniżej. Dodany do projektu art. 14a określa, że minister właściwy do spraw informatyzacji prowadzi wykaz SOC. Wpisanie do wykazu SOC i wykreślenie z tego wykazu, a także zmiana danych (choć w tym ostatnim przypadku nie ujęto tego wprost), następowałoby na wniosek organu właściwego do spraw cyberbezpieczeństwa po uzyskaniu informacji od OUK. Można przyjąć, że wniosek składałby organ właściwy dla OUK, ponieważ to do niego OUK wysyła informację, zgodnie z art. 14 ust. 4. Może pojawić się okoliczność, w której SOC będzie świadczył usługi dla kilku OUK z różnych sektorów, które będą podlegały pod różne organy właściwe. Wobec tego kolejny organ właściwy usiłowałby złożyć wniosek o wpisanie SOC, z którym OUK zawarł umowę, do wykazu SOC, choć ten już by w wykazie istniał. Problem ujawnia się także w kwestii nakładania kar na SOC przez organ właściwy (według właściwości dla OUK), uregulowanego w art. 74 ust. 1a projektu. Mogłoby to powodować, że różne organy właściwe mogłyby chcieć nakładać na SOC kary za te same nieprawidłowości.	

			Art. 4 pkt. 16 określa, że krajowy system cyberbezpieczeństwa obejmuje m.in. SOC. Dlatego art. 41 powinien wskazywać organ właściwy również dla SOC wykonujących usługi dla operatorów usług kluczowych.	
32.	Komisja Nadzoru Finansowego	Art. 42 ust. 1 pkt 7	**Propozycja zmiany:** 7) wzywa na wniosek CSIRT NASK, CSIRT GOV, CSIRT MON lub **CSIRT sektorowego** operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego; **Uzasadnienie:** Analogicznie do treści art. 42 ust. 1 pkt 5, KNF sugeruje dodanie również CSIRTsektorowego. Wynika to niejako z regulacji pkt. 5, w którym organ właściwy we współpracy również z CSIRT sektorowymi przygotowuje rekomendacje dot. cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów.	**Uwaga uwzględniona, przepis zostanie zmieniony.**
33.	Komisja Nadzoru Finansowego	Art. 44 ust 1 pkt 5	**Propozycja zmiany:** Współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV, **a także CSIRT sektorowymi oraz ISAC,** w zakresie wymiany informacji i reagowania na incydenty poważne i krytyczne oraz wymianę informacji o zagrożeniach. **Uzasadnienie:** Zasadne jest rozszerzenie podmiotów, z którymi może współpracować CSIRT sektorowy w ramach realizacji swoich zadań.	**Uwaga nieuwzględniona** ISAC nie jest jednostką operacyjną. Nie będzie miał żadnych kompetencji w kontekście zgłaszania incydentów.

34.	Urząd Zamówień Publicznych	Art. 44 ust. 6	Niezależnie od uwag UZP dotyczących zmian projektowanych w ustawie Pzp, należy zwrócić uwagę na art. 1 pkt 24 lit. c projektu ustawy, w którym proponuje się dodanie m.in. ust. 6 do art. 44 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Projektowany przepis przewiduje, że w przypadku braku możliwości realizacji zadań CSIRT sektorowego w trybie określonym w ust. 1 lub ust. 5 art. 44, organ właściwy może, po zasięgnięciu opinii Pełnomocnika, powierzyć realizację zadań CSIRT sektorowego podmiotowi, o którym mowa w art. 4 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. poz. 2019), oraz określić szczegółowy zakres realizowanych przez niego zadań, biorąc pod uwagę: 1) wymóg posiadania przez ten podmiot przygotowania technicznego i przeszkolonego personelu oraz doświadczenia w zakresie reagowania na incydenty, analizowania incydentów poważnych, wyszukiwania powiązań pomiędzy incydentami oraz opracowywania wniosków z obsługi incydentu, a także mając na względzie; 2) konieczność współpracy tego podmiotu z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV; 3) poziom cyberbezpieczeństwa i liczbę podmiotów w danym sektorze oraz incydenty, które w nim wystąpiły. W związku z powyższym, odpowiednio do intencji projektodawcy, wnoszę o uzupełnienie projektowanego przepisu o wymóg, aby powierzenie zadania, o którym w nim mowa, następowało w oparciu o przepisy Pzp, albo o odpowiednie uzupełnienie uzasadnienia	**Wyjaśnienie** Odesłanie do Prawa zamówień publicznych dotyczy wskazania podmiotów, nie chodzi o stosowanie trybu powierzenia wykonania zadania publicznego.

			projektu ustawy o wskazanie podstawy wyłączenia stosowania przepisów ustawy Pzp	
35.	Komisja Nadzoru Finansowego	Art. 44a ust. 4 pkt 5	**Propozycja zmiany:** współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV**, a także CSIRT sektorowymi oraz ISAC,** w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymianę informacji o zagrożeniach. **Uzasadnienie:** Zasadne jest rozszerzenie podmiotów, z którymi może współpracować CSIRT Telco (jako również „sektorowy") w ramach realizacji swoich zadań.	**Uwaga nieuwzględniona** ISAC nie jest jednostką operacyjną. Nie będzie miał żadnych kompetencji w kontekście zgłaszania incydentów. Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE.
36.	Agencja Wywiadu	Art. 66a	W odniesieniu do proponowanego brzmienia art. 66a ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, sam fakt wprowadzenia w ust. 1 tego przepisu możliwości sporządzenia przez Kolegium, na wniosek członka Kolegium, oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, należy ocenić pozytywnie i podkreślić, iż przyznanie ww. uprawnienia Kolegium jest zasadne.	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony

				dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej

				dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
37.	Agencja Wywiadu	Art. 66a	W odniesieniu do projektowanego art. 66a ww. ustawy Agencja Wywiadu zwraca także uwagę, iż w ww. przepisie nie został wskazany zakres czasowy w jakim Kolegium może sporządzić ocenę ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Jedyne ramy czasowe jakie ujęto w ww. przepisie odnoszą się do terminu (14 dni od publikacji komunikatu o sporządzonej ocenie) na odwołanie się dostawcy	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez

			sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko. Termin na rozpatrzenie odwołania przez Kolegium również został określony i ma wynosić 2 miesiące.	ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in.

				prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
38.	Agencja Wywiadu	Art. 66a ust. 2 pkt 2	W zawartym w projekcie brzmieniu art. 66a ust. 2 w pkt 2 ww. ustawy przewidziano, że wniosek o sporządzenie oceny ma zawierać wskazanie możliwych obszarów działalności, w których	**Uwaga nieuwzględniona** Według powszechnego stanowiska doktryny pojęcie bezpieczeństwa narodowego obejmuje

			dostawca sprzętu lub oprogramowania może stanowić zagrożenie dla bezpieczeństwa narodowego. Należy jednak zaznaczyć, że na gruncie prawa krajowego, ani w systemie prawnym Unii Europejskiej nie istnieje definicja legalna pojęcia „bezpieczeństwo narodowe". Przedmiotowe pojęcie występuje w art. 4 ust. 2 Traktatu o Unii Europejskiej, który stanowi, że *„Unia szanuje równość Państw Członkowskich wobec Traktatów, jak również ich tożsamość narodową, nierozerwalnie związaną z ich podstawowymi strukturami politycznymi i konstytucyjnymi, w tym* w *odniesieniu do samorządu regionalnego i lokalnego. Szanuje podstawowe funkcje państwa, zwłaszcza funkcje mające na celu zapewnienie jego integralności terytorialnej, utrzymanie porządku publicznego oraz ochronę bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostaje w zakresie wyłącznej odpowiedzialności każdego Państwa Członkowskiego.".* Należy podkreślić, iż ostatnie zdanie przywołanej powyżej regulacji Traktatu budzi wiele kontrowersji, jeśli chodzi o zakres kompetencji wyłącznej Państw Członkowskich w odniesieniu do sfery bezpieczeństwa narodowego, w szczególności biorąc pod uwagę tendencję do „zawłaszczania" tych kompetencji przez Unię Europejską. Mając powyższe na uwadze, zdaniem Agencji Wywiadu, należy rozważyć zastąpienie w proponowanym brzmieniu art. 66a ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie	bezpieczeństwo wewnętrzne i zewnętrzne Państwa.

			cyberbezpieczeństwa określenia „bezpieczeństwo narodowe" wyrażeniem „bezpieczeństwo wewnętrzne i zewnętrzne państwa, o których mowa w art. 1 i 2 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2020 poz. 27)".	
39.	Agencja Wywiadu	Art. 66a ust. 4 pkt 2	Ponadto, w ocenie Agencji Wywiadu, należy rozważyć czy w zawartym w projekcie brzmieniu art. 66a ust. 4 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa właściwe jest użycie sformułowania, „prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego (...)". Ww. kryterium jest wysoce nieprecyzyjne i może budzić wątpliwości w toku sporządzania oceny. W opinii Agencji Wywiadu zasadnym wydaje się zmiana tego określenia na bardziej konkretne i precyzyjnie określające relację dostawcy sprzętu lub oprogramowania z danym państwem. W nawiązaniu do powyższego, w projektowanym brzmieniu art. 66a ust. 4 pkt 2 w lit c przywołanej wyżej ustawy, Agencja Wywiadu poddaje pod rozwagę możliwość doprecyzowania tego przepisu poprzez zastąpienie wyrazów „porozumień w zakresie ochrony danych miedzy UE i danym państwem" wyrazami „porozumień w zakresie ochrony danych osobowych między UE a państwami spoza UE". Zdaniem Agencji Wywiadu, zasadne byłoby również doprecyzowanie zawartego w projekcie brzmienia art. 66a ust. 4 pkt 2 ww. ustawy także lit. d poprzez wskazanie,	**Uwaga nieuwzględniona** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa).

			iż w sporządzaniu oceny uwzględnia się, oprócz struktury własnościowej dostawcy sprzętu lub oprogramowania, także powiązania kapitałowe i organizacyjne tego dostawcy.	Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy

				telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
40.	Prezes Urzędu Komunikacji Elektronicznej	Art. 66b ust. 1 pkt 1	Zaproponowany w projektowanym art. 66b ust. 1 pkt 1 UKSC obowiązek niewprowadzania do użytkowania przez podmioty krajowego systemu cyberbezpieczeństwa, sprzętu, oprogramowania i usług od dostawcy, który uzyskał wysoką ocenę ryzyka, nie uwzględnia okresu eksploatacji sprzętu co może wpłynąć znacząco na obciążenia finansowe przedsiębiorców.	**Wyjasnienie** W zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W projekcie jest mowa o 7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.

41.	Agencja Wywiadu	Art. 66b ust. 1 pkt 2 Art. 66b ust. 2	Ponadto, w ocenie Agencji Wywiadu, warte rozważenia byłoby również doprecyzowanie, czy w świetle projektowanego przepisu art. 66b ust. 1 pkt 2 oraz ust. 2 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, podmioty krajowego systemu cyberbezpieczeństwa będą mogły kontynuować użytkowanie dotychczas posiadanych egzemplarzy sprzętu, oprogramowania oraz usług wykorzystywanych przed opublikowaniem komunikatu o ocenie danego dostawcy, w przypadku gdy wskutek wystąpienia nowych okoliczności mogących mieć wpływ na ocenę ryzyka tego dostawcy, ocena ta zostanie zmieniona przez Kolegium z oceny określającej wysokie ryzyko ww. dostawcy na ocenę określającą umiarkowane ryzyko dostawcy (*vide* art. 66a ust. 9).	**Uwaga nieuwzględniona** Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. W takiej sytuacji, jak opisana w uwadze będzie miał zastosowanie art. 145 KPA. Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka.
42.	Prezes Urzędu Ochrony Konkurencji i Konsumentów	Art. 66a-66c Art. 1 pkt 29 Projektu	Należy zwrócić uwagę, iż przyznanie Kolegium ds. Cyberbezpieczeństwa (dalej jako: „**Kolegium”**) kompetencji do oceny stopnia ryzyka dla cyberbezpieczeństwa Państwa u dostawców sprzętu, oprogramowania czy usług przy wykorzystaniu nieostrych kryteriów klarowności (art. 1 pkt 29 Projektu) może prowadzić do powstania ograniczeń konkurencji na rynku usług telekomunikacyjnych w Polsce. W przypadku bowiem gdy ocena Kolegium wykaże wysokie ryzyko dla cyberbezpieczeństwa Państwa u konkretnego dostawcy, podmioty krajowego systemu cyberbezpieczeństwa nie będą mogły nabywać od takiego dostawcy sprzętu, oprogramowania czy też usług, zaś w ciągu 5 lat	**Wyjaśnienie** Przepisy art. 66a-66c zostaną zmienione. Procedura oceny ryzyka dostawcy sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa będzie oparta o przepisy Kodeksu postępowania administracyjnego. Postępowanie administracyjne będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Kolegium ds. Cyberbezpieczeństwa. W ramach postępowania prowadzonego przez ministra właściwego ds. informatyzacji będzie mogła być wydana decyzja administracyjna w sprawie uznania dostawcy sprzętu lub

			od ogłoszenia komunikatu o ocenie, będą musiały taki sprzęt, oprogramowanie czy też usługi wycofać z użytkowania, co de facto spowoduje wyeliminowanie danego przedsiębiorcy z rynku, a w konsekwencji wpłynie na poziom konkurencji w Polsce. Tym samym zwracam uwagę, iż zasadne wydaje się sformułowanie wyżej wskazanych kryteriów w sposób na tyle konkretny i przejrzysty aby wyeliminować potencjalne wątpliwości w wyżej wymienionym zakresie. Należy przy tym zauważyć, że wpływ tego ograniczenia na konkurencję jest dziś trudny do oszacowania z uwagi na dynamikę tego rynku i stały rozwój technologiczny a także powstawanie nowych przedsiębiorców świadczących usługi z tego zakresu.	oprogramowania za dostawcę wysokiego ryzyka. Podstawą do wydania decyzji będzie stwierdzenie poważnego zagrożenia dla bezpieczeństwa narodowego ze strony dostawcy sprzętu lub oprogramowania. Dostawca wobec którego będzie prowadzona postępowanie o ryzyka zostanie poinformowany o wszczęciu postępowania. Ponadto dostawca będzie miał zapewniony dostęp do materiałów zgromadzonych w aktach spraw za wyjątkiem materiałów, które organ prowadzący sprawę wyłączy ze względu na ważny interes państwowy (art. 74 Kpa). Zrezygnowano z poziomów ryzyka: niski, umiarkowany, brak zidentyfikowanego ryzyka. Kolegium będzie wydawało opinię, która zostanie przekazana do ministra właściwego ds. informatyzacji. Zostaną określone w przepisach zadania poszczególnych członków Kolegium w zakresie przygotowywanych wkładów do opinii. Ponadto zostaną określone terminy oraz procedury opisujące wydanie przez Kolegium opinii. W ramach postępowania będą badane aspekty techniczne i nietechniczne. Elementem postępowania może być analiza dotychczas wydanych rekomendacji na podstawie art. 33 ustawy o ksc. Jednocześnie podczas postępowania bada się aspekty nietechniczne związane z samym dostawcą m. in. prawdopodobieństwo, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji

				Traktatu Północnoatlantyckiego, struktura własnościowa dostawcy sprzętu lub oprogramowania, zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Zrezygnowaliśmy z oceny prawodawstwa państwa pochodzenia dostawcy pod kątem ochrony praw człowieka. Ponadto zmieniony zostanie termin określony na wycofanie sprzętu lub oprogramowania od dostawcy sprzętu lub oprogramowania uznanego za dostawcę wysokiego ryzyka (z 5 na 7 lat). Natomiast przedsiębiorcy telekomunikacyjni sporządzający plany działań w sytuacji szczególnego zagrożenia będą musieli wycofać w ciągu 5 lat od wydania przez ministra właściwego ds. informatyzacji decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, sprzęt lub oprogramowanie wskazany w decyzji oraz wchodzący w ramach kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku do ustawy. Zakres funkcji krytycznych zostanie dołączony do ustawy jako załącznik nr 3.
43.	Polski Komitet Normalizacyjny	Art. 67a ust. 4 pkt 5	**Proponowana zmiana:** „4. Ostrzeżenie i polecenie zabezpieczające może dotyczyć: (..) 5) dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23	**Uwag uwzględniona**

			lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z poźn. zm.) oraz dostawców środków identyfikacji elektronicznej, o których mowa w art. 3. pkt. 2 tego rozporządzenia. Na bezpieczeństwo obrotu prawnego prowadzonego za pomocą środków komunikacji elektronicznej w coraz większej skali wpływ ma nie tylko poziom wiarygodności kwalifikowanych usług zaufania, ale także niekwalifikowanych usług zaufania. Te ostanie usługi, szczególnie o statusie zaawansowanym, mogą być również szeroko wykorzystywane jako alternatywa do usług kwalifikowanych i ich wpływ na obniżenie bezpieczeństwa krajowego systemu cyberbezpieczeństwa może być też być istotny. Dlatego warto przewidzieć prawną możliwość oddziaływania również na niekwalifikowane usługi zaufania. Podobna argumentacja przemawia za objęciem omawianym przepisem dostawców środków identyfikacji elektronicznej, z której coraz częściej i to na dużą skalę będą korzystać dostawcy usług świadczonych drogą elektroniczną.	
44.	Prezes Urzędu Komunikacji Elektronicznej	Art. 74 ust. 1a pkt 1	Projektowany art. 74 ust. 1a pkt 1 UKSC – w odniesieniu do tego przepisu należy zauważyć, że w art. 41-44 UKSC określono kompetencje i uprawnienia organów właściwych w poszczególnych sektorach, wśród których są	Uwaga częściowo uwzględniona Przepisy dotyczące obowiązków przedsiębiorców komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług

			wymienione także monitorowanie stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych oraz kontrola tych podmiotów. Z kolei w art. 53 -59 UKSC określone są zasady sprawowania nadzoru i kontroli operatorów usług kluczowych i dostawców usług cyfrowych przez organy właściwe w poszczególnych sektorach. Przepisy powyższe nie mają zastosowania do większości przedsiębiorców telekomunikacyjnych (załącznik nr 1 do ustawy nie wyodrębnia sektora telekomunikacyjnego) i nie stanowią podstawy do działania Prezesa UKE (nie jest on organem właściwym do spraw cyberbezpieczeństwa). Również przepisy Prawa telekomunikacyjnego i projektu Pke nie określają kompetencji nadzorczych i kontrolnych Prezesa UKE w obszarze cyberbezpieczeństwa. Ponadto, Prezes UKE nie dysponuje pracownikami posiadającymi wiedzę ekspercką w zakresie wymaganym od organów zajmujących się sprawami cyberbezpieczeństwa. Brak jest również podstaw do budowy takich zasobów kadrowych, skoro Prezes UKE nie jest organem właściwym do spraw cyberbezpieczeństwa. Wobec powyższego przewidziana w projektowanym art. 74 ust. 1a pkt 3 UKSC kompetencja Prezesa UKE do nakładania kar na przedsiębiorców komunikacji elektronicznej niestosujących się do zakazu wprowadzania do użytkowania sprzętu, oprogramowania i usług lub nakazu ich wycofania (projektowany art. 66b UKSC) byłaby bardzo trudna do realizacji i powinna być pozostawiona	komunikacji elektronicznej oraz przepisy o CSIRT Telco zostaną dodane do ustawy o ksc poprzez ustawę wprowadzającą PKE. Uzupełniono przepisy dot. nadzoru Prezesa UKE nad przedsiębiorcami komunikacji elektronicznej w kontekście przestrzegania wymagań z zakresu bezpieczeństwa sieci i usług.

			we właściwości ministra właściwego do spraw informatyzacji. Abstrahując od powyższego należy zauważyć, że projektowana regulacja jest niepełna, bo nie reguluje sytuacji, w której strona nie osiągnęła obrotu (przychodu) w poprzednim roku obrotowym lub nie można go ustalić, ani nie określa wysokości minimalnych kar (które jednak są przewidziane w projektowanym art. 73 ust. 4 UKSC dla pozostałych przypadków naruszeń). Brakuje także przepisów dających podstawę do wzywania strony do przedstawienia danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.	
45.	Komisja Nadzoru Finansowego	Art. 73 ust. 1	**Propozycja zmiany:** „Można nałożyć karę pieniężną na operatora usługi kluczowej, który: (…)". **Uzasadnienie:** **1) Uznaniowość karania** Sformułowania użyte przez ustawodawcę w art. 73 ust. 1 i ust. 2, art. 73 ust. 5 i art. 74 ust. 1 UKSC („karze pieniężnej podlega", organ właściwy „nakłada") mogą prowadzić do wniosku, że nałożenie kary pieniężnej na podstawie powołanych przepisów ma charakter obligatoryjny. W przedmiotowym przypadku brak jest uzasadnienia dla obligatoryjności nakładania kary pieniężnej. W związku z powyższym zasadne jest zastąpienie sformułowania *„karze pieniężnej podlega"* na *„może nałożyć karę pieniężną"* oraz zastąpienie sformułowania *„nakłada"* na *„może nałożyć".* Dokonanie przedmiotowej zmiany pozwoli KNF na zastosowanie uznania administracyjnego w odniesieniu do każdego	**Uwaga nieuwzględniona** **Ad. 1 Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej.** **Ad. 2 Uwaga wykracza poza zakres przedmiotowy objęty nowelizacją.**

			przypadku naruszenia przepisów prawa. Zmiany te są zgodne z Dyrektywą 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Zgodnie z treścią art. 21 ww. Dyrektywy *„Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.”* Przywołana Dyrektywa **nie wymaga** zatem od Państw Członkowskich UE wprowadzenia obligatoryjności karania. Za brakiem obligatoryjności karania przemawia także uzasadnienie do UKSC. W uzasadnieniu do projektu ustawy wskazano bowiem, cyt.: *„W rozdziale 14 zawarto przepisy regulujące nakładanie administracyjnych kar pieniężnych. Przewiduje się, iż organ właściwy dla danego sektora **będzie mógł nałożyć** na operatorów usług kluczowych administracyjną karę pieniężną za brak realizacji obowiązków wynikających z ustawy. Przykładowo administracyjną karą pieniężną **będzie mógł zostać ukarany** operator usługi kluczowej, który nie wdrożył środków*	

			technicznych i operacyjnych, nie zgłasza incydentów poważnych, nie zapewnia ich obsługi, w tym nie współdziała w trakcie realizacji tych czynności z właściwym CSIRT." Intencją ustawodawcy było zatem wprowadzenie uznania administracyjnego w zakresie nakładania kar pieniężnych. Proponowane zmiany w UKSC są podyktowane zapewnieniem spójności rozwiązań obowiązujących w różnych sektorach rynku finansowego. Zmiany przyczynią się do zwiększenia efektywności postępowań oraz są wyrazem pragmatycznego podejścia. Wymierzanie sankcji administracyjnej w ramach uznania administracyjnego jest właściwszą formą oddziaływania nadzorczego i powinno być przyjęte jako reguła w postępowaniu z podmiotami nadzorowanymi. Uznanie administracyjne pozwala na rozważenie, czy w danych okolicznościach sprawy zasadne i celowe jest sięgnięcie po środki o charakterze sankcyjnym, czy też cel nadzorczy może zostać osiągnięty przy użyciu innych, mniej dolegliwych dla podmiotów nadzorczych, środków nadzorczych o charakterze nie sankcyjnym. Obligatoryjność stosowania sankcji administracyjnych powinna być wyjątkiem, zastrzeżonym dla przypadków, w których charakter naruszeń lub dobro, które ma być chronione, wymagają w każdym przypadku stwierdzenia naruszeń, zastosowania dolegliwych środków nadzorczych. Wprowadzenie uznania administracyjnego umożliwi Komisji stosowanie	

			środka nadzorczego adekwatnego do stwierdzonego naruszenia. **2) Wysokość kar pieniężnych** W chwili obecnej kary zdefiniowane w UKSC (art. 73 ust. 3 i ust. 5 ww. ustawy) są rażąco niskie, nie mają charakteru odstraszającego i nie spełniają wymogów dyrektywy 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: dyrektywa NIS) w zakresie działania prewencyjnego i represyjnego. Artykuł 21 tej dyrektywy stanowi, że: *„Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą”.* Operatorem usługi kluczowej zgodnie z UKSC może być m. in. bank krajowy czy instytucja kredytowa, tj. podmioty profesjonalne o znaczących aktywach i przychodach. Kary zaproponowane w UKSC dla tych podmiotów są nieadekwatne do kar pieniężnych przewidzianych w innych ustawach regulujących funkcjonowanie tych podmiotów np. ustawa Prawo bankowe	

			przewiduje karę pieniężną w maksymalnej wysokości do 10% wartości przychodów banku (co może sięgać nawet kilku czy kilkudziesięciu mln złotych). Kara pieniężna, aby móc pełnić swoje funkcje represyjne i prewencyjne, musi mieć charakter odstraszający. Celem zastosowania przez organ nadzoru kary pieniężnej jest przede wszystkim zapewnienie przestrzegania przez adresatów norm prawnych obowiązków w obszarach uznanych za szczególnie istotne przez ustawodawcę. Sankcja nie może być oderwana od stwierdzonych nieprawidłowości i ma pozostawać z nimi w ścisłym związku przyczynowo - skutkowym, tak by w pełni odzwierciedlała stopień naganności zachowania jednostki w stosowaniu obowiązującego prawa. Administracyjne kary pieniężne mają na celu mobilizowanie podmiotów do działania zgodnego z przepisami prawa. Kary te, stosowane z mocy prawa, mają przede wszystkim znaczenie prewencyjne. Przez zapowiedź negatywnych konsekwencji, jakie nastąpią w wypadku naruszenia obowiązków określonych w ustawie, motywują adresatów określonych tam norm, do wykonywania ustawowych obowiązków. Tym samym kara administracyjna nie jest wyłącznie represją za naruszenie prawa, ale przede wszystkim stanowi środek przymusu, który ma służyć zapewnieniu wykonywania obowiązków nałożonych przez obowiązujące przepisy prawa (wyrok Trybunału Konstytucyjnego z dnia 25marca 2010 r., sygn. akt P 9/08). Celem kary jest również zapobieżenie podobnym	

			naruszeniom w przyszłości i efektywniejsze wykonywanie przez podmioty nadzorowane przepisów prawa. Warto również przytoczyć stanowisko Trybunału Konstytucyjnego, który w wyroku z dnia 1 marca 1994 r. (sygn. akt: U 7/93) wskazał, iż kary pieniężne są środkami służącymi mobilizowaniu podmiotów do terminowego i prawidłowego wykonywania obowiązków na rzecz państwa. Kara administracyjna ma charakter środka przymusu, służącego zapewnieniu realizacji wykonawczo-zarządzających zadań administracji, agregowanych przez pojęcie interesu publicznego (por. wyrok Trybunału Konstytucyjnego z dnia 31 marca 2008 r., sygn. akt: SK 75/06). Zatem kluczowym powinno być dostosowanie art. 73 ust. 3 i ust. 5 UKSC do wymogów dyrektywy NIS poprzez znaczne zwiększenie wysokości kar, które mogą zostać nałożone na operatora usług kluczowych, w ten sposób, aby spełniały one warunek „odstraszania" (mając na uwadze status podmiotów mogących pełnić funkcję operatora usług kluczowych). Tak niskie kary jak przewidziane w UKSC (w porównaniu do kar pieniężnych możliwych do nałożenia na podstawie innych ustaw), mogą prowadzić do sytuacji, w której bardziej opłacalne będzie dla podmiotu uiszczenie kary pieniężnej, niż przestrzeganie wymogów i obowiązków nałożonych UKSC. Administracyjna kara pieniężna powinna być skutecznym środkiem do wymuszania na adresatach norm administracyjnych	

			określonych zachowań. W obecnym brzmieniu przepisów art. 73 ust. 3 i ust. 4 UKSC, tj. w sytuacji gdy w z jednej strony Podsumowując, aby spełnić wymóg art. 21 Dyrektywy NIS uregulowane w przepisach UKSC maksymalne kary pieniężne powinny być rygorystyczne, a KNF powinien mieć możliwość nałożenia kary w ramach, lecz nie być do nałożenia kary bezwzględnie zobowiązanym (uznanie administracyjne). Taka nowa regulacja pozwoli, aby KNF skupił się na nakładaniu sankcji za istotne naruszenia prawa.	
46.	Komisja Nadzoru Finansowego	Art. 73 ust. 2	**Propozycja zmiany:** „Można nałożyć karę pieniężną na dostawcę usługi cyfrowej, który: (…)”. **Uzasadnienie:** Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji.	**Uwaga nieuwzględniona** Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej.
47.	Komisja Nadzoru Finansowego	Art. 73 ust. 5 zdanie 1	**Propozycja zmiany:** „Jeżeli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych - organ właściwy do spraw	**Uwaga nieuwzględniona** Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej.

			cyberbezpieczeństwa może nałożyć karę w wysokości do 1 000 000 zł.” **Uzasadnienie:** Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji.	
48.	Komisja Nadzoru Finansowego	Art. 74 ust. 1	**Propozycja zmiany:** „Karę pieniężną, o której mowa w art. 73, może nałożyć, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa” **Uzasadnienie:** Zmiana podyktowana utrzymania spójnego, fakultatywnego systemu sankcji.	**Uwaga nieuwzględniona** Na podstawie art. 189f KPA organ może odstąpić od nałożenia administracyjnej kary pieniężnej.
49.	Komisja Nadzoru Finansowego	Art. 74 ust. 1a pkt 4	**Propozycja zmiany:** 4) w przypadku podmiotów wpisanych do wykazu SOC, wykonujących usługi na zlecenie operatora usług kluczowych – minister właściwy do spraw informatyzacji. **Uzasadnienie:** Zmiana ma związek z wyżej proponowaną zmianą art. 41 pkt 12 (organy właściwe). Może pojawić się okoliczność, w której SOC będzie świadczył usługi dla kilku OUK z różnych sektorów, które będą podlegały pod różne organy właściwe. Wówczas ujawnia się problem w kwestii nakładania kar na SOC przez organ właściwy (jeśli miałby być to organ według właściwości dla OUK). Mogłoby to powodować, że różne organy właściwe mogłyby chcieć nakładać na SOC kary za te same nieprawidłowości. KNF zwraca uwagę, że mogą się pojawić wątpliwości interpretacyjne co do użycia słowa ***wpisanych*** w przypadku, gdy podmiot nie jest (jeszcze) wpisany do wykazu SOC.	**Uwaga uwzględniona**

50.	Urząd Zamówień Publicznych	Art. 96 ust. 2 pkt 3 PZP	W myśl projektowanego pkt 3 w art. 96 ust. 2 Pzp zamawiający może określić w ogłoszeniu o zamówieniu lub dokumentach zamówienia wymagania związane z realizacją zamówienia, które mogą dotyczyć w szczególności poziomu ryzyka, jaki stanowi dostawca sprzętu lub oprogramowania, stwierdzonego oceną, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369). Zaproponowana redakcja przepisu nie wydaje się dostatecznie czytelna. Przepis powinien być doprecyzowany w zakresie wskazania czego konkretnie mają dotyczyć wymagania związane z realizacją zamówienia, o których mowa projektowanym przepisie, a w szczególności w związku z jakimi okolicznościami ocena, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ma być przeprowadzana trakcie realizacji zamówienia.	**Wyjaśnienie** W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych.
51.	Urząd Zamówień Publicznych	Art. 109 ust. 1 pkt 11 PZP	Projekt dodaje pkt 11 w art. 109 ust. 1 Pzp, zgodnie z którym z postępowania o udzielenie zamówienia zamawiający może wykluczyć wykonawcę, który jest dostawcą sprzętu lub oprogramowania, wobec którego stwierdzono wysokie ryzyko, w ramach oceny, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Jeżeli zamówienie jest zamówieniem w dziedzinach obronności i bezpieczeństwa proponowana fakultatywna podstawa wykluczenia odpowiada podstawie wykluczenia wykonawcy przewidzianej w art. 39 ust. 2 lit. e) dyrektywy 2009/81/WE,	**Wyjaśnienie** W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych.

			zgodnie z którym w przypadku zamówień udzielanych w dziedzinie obronności i bezpieczeństwa zamawiający może wykluczyć każdego wykonawcę, który na podstawie dowolnych środków dowodowych, w tym chronionych źródeł danych, został uznany za nieposiadającego wiarygodności niezbędnej do wykluczenia zagrożenia dla bezpieczeństwa państwa członkowskiego. Ten przepis dyrektywy 2009/81/WE został wdrożony w art. 405 ust. 2 pkt 3 Pzp. Zastosowanie szczególnych przesłanek wykluczenia jest możliwe również w oparciu o art. 393 ust. 1 Pzp w odniesieniu do zamówień sektorowych.	
52.	Urząd Zamówień Publicznych	Art. 110 ust. 2 PZP	Proponuję wykreślenie projektowanej zmiany w art. 110 ust. 2 Pzp. Przepis ten miałby umożliwiać wykonawcy, w związku z zaistnieniem w stosunku do niego podstawy wykluczenia określonej w projektowanym art. 109 ust. 1 pkt 11 Pzp, podjęcia działań naprawczych i zapobiegawczych w ramach procedury samooczyszczenia. Dodatkowo należy zwrócić uwagę, iż ocena, o której mowa w art. 66a ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, obejmuje m.in. analizę prawdopodobieństwa, czy dostawca sprzętu lub oprogramowania znajduje się pod wpływem państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, uwzględniającą: a) stopień i rodzaj powiązań pomiędzy dostawcą sprzętu lub oprogramowania i tym państwem, b) prawodawstwo tego państwa w zakresie ochrony praw obywatelskich i praw człowieka, c)	**Wyjaśnienie** W toku prac legislacyjnych zrezygnowano z nowelizacji Prawa zamówień publicznych.

			prawodawstwo w zakresie ochrony danych osobowych, zwłaszcza tam gdzie nie ma porozumień w zakresie ochrony danych między UE i danym państwem, d) strukturę własnościową dostawcy sprzętu lub oprogramowania, e) zdolność ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania. Okoliczności wskazane w lit. b, c i e są okolicznościami niezależnymi od wykonawcy, co wyklucza jak się wydaje, możliwość podjęcia przez wykonawcę skutecznych działań naprawczych oraz zapobiegawczych z przyczyn, które nie leżą po stronie wykonawcy. Wdrożenie tego przepisu mogłoby sprawiać, że możliwość skorzystania przez wykonawcę z procedury samooczyszczenia w odniesieniu do projektowanej podstawy wykluczenia stawałaby się czynnością pozorną.	
53.	NASK	OSR	Mając na uwadze stały wzrost liczby procesów oraz poszerzający się katalog działań skierowanych do podmiotów znajdujących się w obszarze odpowiedzialności CSIRT NASK, zachodzi konieczność zrewidowania kosztów funkcjonowania CSIRT NASK. Budżet przewidziany w Ustawie na dotację podmiotową na rzecz NASK PIB już obecnie nie jest wystarczający do realizacji przez CSIRT NASK działań ustawowych. W związku z tym, konieczne jest jego zwiększenie, zgodnie z estymacją kosztów przekazaną w piśmie NASK PIB o nr ZZP.051.200034.2020.ASI [OSR-KSC-2021+] z dnia	**Uwaga uwzględniona,** OSR zostanie uzupełniony o koszty dla NASK.

			2 lipca 2020 roku. Estymacja ta została przygotowana z uwzględnieniem doświadczeń ekspertów NASK PIB oraz danych finansowych NASK PIB dotyczących wydatków poniesionych na realizację zadań wynikających z Ustawy w latach 2018-2020. Równocześnie podkreślam, że zaproponowane przez Ministerstwo zmiany w Ustawie jeszcze zwiększają zakres zadań CSIRT NASK (m.in. w zakresie zadań wykonywanych na rzecz Pełnomocnika oraz objęcia zakresem Ustawy sektora telekomunikacyjnego, co także zwiększa zakres działania CSIRT NASK). W związku z powyższym konieczne jest zwiększenie finansowania na potrzeby tych nowych działań CSIRT NASK. Dodatkowo, NASK PIB buduje system S46 (system teleinformatyczny opisany w Ustawie w art. 46). Będzie to system kluczowy dla działania krajowego systemu cyberbezpieczeństwa, a NASK PIB przygotowuje się do jego utrzymania i rozwoju, co wymaga odpowiedniego finansowania. NASK PIB pracuje także nad uruchomieniem Centrum Certyfikacji.	

TABELA ZGODNOŚCI				
TYTUŁ PROJEKTU	Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw			
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)			
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU	Termin wejścia w życie uwzględnia konieczność podjęcia niezbędnych działań przez krajowy organ certyfikacji cyberbezpieczeństwa oraz konieczność jak najszybszego wprowadzenia w życie tych przepisów.			
l.p.	**jednostka redakcyjna aktu o cyberbezpieczeństwie**	**treść przepisu UE**	**jednostka redakcyjna ustawy**	**treść przepisu/przepisów projektu ustawy**
1.	Art. 2 pkt 1	1) „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;	Art. 2 pkt 11	11) cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami;
2.	Art. 2 pkt 8	8)„cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;	Art. 2 pkt 12	„12) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz na inne podmioty;”

3.	Art. 2 pkt 12- 15	12) „produkt ICT” oznacza element lub grupę elementów sieci lub systemów informatycznych; 13) „usługa ICT” oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych; 14) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT; 15) „akredytacja” oznacza akredytację zgodnie z definicją w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008;	Art. 2 pkt 1,33 i 34 oraz 45	1) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30), zwanym dalej „rozporządzeniem 765/2008”; 33) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT; 34) produkt ICT – element lub grupę elementów systemu informacyjnego; 45) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;
4.	Art. 2 pkt 17-18	17)„ocena zgodności” oznacza ocenę zgodności zgodnie z definicją w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008; 18) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność zgodnie z definicją w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;	Art. 2 pkt 23 i 30	23) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia 765/2008; 30) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;
5.	Art. 46	1. Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienia zharmonizowanego podej-ścia na poziomie unijnym do europejskich programów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego	Art. 1 ust. 1 pkt 1a	„1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz.

		rynku cyfrowego w zakresie produktów ICT, usług ICT i procesów ICT. 2. Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa i potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenia dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia.		UE L 151 z 07.06.2019, str. 15), zwanego dalej, „rozporządzeniem 2019/881”;
6.	Art. 53	1. Europejski program certyfikacji cyberbezpieczeństwa może zezwalać na ocenę zgodności przez stronę pierwszą przeprowadzaną na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT. Na ocenę zgodności przez stronę pierwszą zezwala się jedynie w przypadku produktów ICT, usług ICT lub procesów ICT, które stwarzają niewielkie ryzyko odpowiadające poziomowi uzasadnienia zaufania „podstawowy”. 2. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT może wydać unijną deklarację zgodności stwierdzającą, że wykazano spełnienie wymogów określonych w programie. Wydając taką deklarację, wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT przyjmuje na siebie odpowiedzialność za	Art. 59k ust. 1 pkt 1	Art. 59k. 1. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem: 1) deklaracji zgodności - badaniom przez dostawcę sprzętu lub oprogramowania, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy;

		zgodność produktu ICT, usługi ICT lub procesu ICT z wymogami określonymi w tym programie. 3. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT udostępnia – przez okres przewidziany w odpowiednim europejskim programie certyfikacji cyberbezpieczeństwa – krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 ust. 1, unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT lub usług ICT z programem. Kopię unijnej deklaracji zgodności przedkłada się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA. 4. Wydanie unijnej deklaracji zgodności jest dobrowolne, o ile prawo Unii lub prawo państw członkowskich nie stanowi inaczej. 5. Unijne deklaracje zgodności są uznawane we wszystkich państwach członkowskich.		
7.	Art. 56 ust. 6	W przypadku gdy europejski program certyfikacji cyberbezpieczeństwa przyjęty na podstawie art. 49 wymaga poziomu uzasadnienia zaufania „wysoki”, europejski certyfikat cyberbezpieczeństwa wydawany w ramach tego programu może być wydany wyłącznie przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – w następujących przypadkach – przez jednostkę oceniającą zgodność: a) po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa każdego europejskiego certyfikatu cyberbezpieczeństwa wydanego przez daną jednostkę oceniającą zgodność; lub	Art. 59n	Art. 59n. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji niezwłocznie przesyła, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285) do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego: 1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania wysoki; 2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania wysoki.

		b) na podstawie ogólnego powierzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność.		2. Minister właściwy do spraw informatyzacji: 1) zatwierdza certyfikat, o którym mowa w ust. 1; 2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą, rozporządzeniem 2019/881 lub programami, o których mowa w ust. 1. 3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się, jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja. 4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg oceny zgodności. 5. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy może zasięgnąć opinii instytutu badawczego nadzorowanego przez tego ministra w zakresie zgodności certyfikacji z krajowym lub europejskim programem certyfikacji cyberbezpieczeństwa. Instytut badawczy przekazuje opinię w terminie 1 miesiąca od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 6. Minister właściwy do spraw informatyzacji cofa certyfikat, jeżeli jest on niezgodny z ustawą, rozporządzeniem 2019/881, europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa. 7. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

8.	Art. 58 ust. 1-6	1. Każde państwo członkowskie wyznacza na swoim terytorium przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – za zgodą innego państwa członkowskiego – wyznacza przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa ustanowiony na terytorium tego innego państwa członkowskiego jako organ odpowiedzialny za zadania związane z nadzorem w wyznaczającym państwie członkowskim. 2. Każde państwo członkowskie informuje Komisję o wyznaczonych krajowych organach ds. certyfikacji cyberbezpieczeństwa, a w przypadku gdy państwo członkowskie wyznacza więcej niż jeden organ, informuje ono również Komisję o zadaniach powierzonych każdemu z tych organów. 3. Bez uszczerbku dla art. 56 ust. 5 lit. a) i art. 56 ust. 6 każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa pozostaje niezależny od jednostek, nad którymi sprawuje nadzór, w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji. 4. Państwa członkowskie zapewniają, by działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, była ściśle oddzielona od ich działalności związanej z nadzorem określonej w niniejszym artykule i by oba rodzaje tej działalności były wykonywane niezależnie od siebie. 5. Państwa członkowskie zapewniają, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa posiadały	Art. 59b	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa; 2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, stosowania przepisów rozporządzenia 2019/881 oraz postanowień krajowych lub europejskich programów certyfikacji cyberbezpieczeństwa; 3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59a ust. 1 pkt 3 i 4; 4) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881; 5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy; 6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania wysoki; 7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania wysoki; 8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa; 9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa innych państw członkowskich lub innymi

		odpowiednie zasoby na potrzeby wykonywania swoich uprawnień i wywiązywania się ze swoich zadań w skuteczny i wydajny sposób. 6. W celu skutecznego wdrożenia niniejszego rozporządzenia zasadnym jest, aby organy te uczestniczyły w pracach ECCG w aktywny, skuteczny, wydajny i bezpieczny sposób.		organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymaganiami rozporządzenia 2019/881 lub z wymaganiami określonymi europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa; 10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa; 11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i; 12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG", corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b–d oraz ust. 8 rozporządzenia 2019/881; 13) uczestniczenie w pracach ECCG; 14) prowadzenie postępowań w zakresie cofnięcia certyfikatu; 15) nadzorowanie i egzekwowanie zawartych w europejskim programie certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymaganiami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku; 16) przeprowadzanie badań certyfikowanych produktów ICT, usług ICT lub procesów ICT.
9.	Art. 58 ust. 7 lit. a-d	7. Krajowe organy ds. certyfikacji cyberbezpieczeństwa: a) nadzorują i egzekwują stosowanie zawartych w europejskich programach certyfikacji bezpieczeństwa na podstawie art. 54 ust. 1 lit. j) zasad monitorowania	Art. 59b pkt 1,2, 5, 15	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

		zgodności produktów ICT, usług ICT i procesów ICT z wymogami europejskich certyfikatów cyberbezpieczeństwa wydanych na ich terytoriach, we współpracy z innymi odpowiednimi organami nadzoru rynku; b)monitorują wykonywanie obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT, którzy mają siedzibę na ich terytorium i którzy przeprowadzają ocenę zgodności przez stronę pierwszą, oraz egzekwują takie obowiązki, w szczególności monitorują wykonywanie obowiązków takich wytwórców lub dostawców, które określono w art. 53 ust. 2 i 3 i w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa, oraz egzekwują takie obwiązki; c) bez uszczerbku dla art. 60 ust. 3 aktywnie wspomagają i wspierają krajowe jednostki akredytujące w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia; d) monitorują i nadzorują działalność podmiotów publicznych, o których mowa w art. 56 ust. 5; 34	Art. 59h ust. 4, 7 i 8, Art. 59m, art. 59q, Art. 59u, Art. 59w	1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa; 2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, stosowania przepisów rozporządzenia 2019/881 oraz postanowień krajowych lub europejskich programów certyfikacji cyberbezpieczeństwa;; 5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy; 15) nadzorowanie i egzekwowanie zawartych w europejskim programie certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymaganiami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;; Art. 59h 4. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych i europejskich programów certyfikacji cyberbezpieczeństwa. 7. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu akredytacji jednostce oceniającej zgodność.8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera: 1) oznaczenie podmiotu, któremu cofnięto akredytację;

				2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji; 3) datę cofnięcia akredytacji. Art. 59m. Jednostka oceniająca zgodność niezwłocznie przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, dane podmiotu, któremu cofnięto certyfikat wraz ze wskazaniem przyczyny jego cofnięcia albo dane podmiotu, któremu odmówiono wydania certyfikatu wraz ze wskazaniem przyczyn odmowy. Art. 59q. 1. W okresie, na jaki został wydany certyfikat produkt ICT, usługa ICT lub proces ICT dla którego go wydano, ma spełniać kryteria obowiązujące na dzień jego wydania. 2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że produkt ICT, usługa ICT lub proces ICT, dla którego wydano certyfikat , nie spełnia lub przestał spełniać kryteria certyfikacji. 3. Jednostka oceniająca zgodność informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych. Art. 59u. Po wydaniu deklaracji zgodności dostawca niezwłocznie przesyła jej kopię ministrowi właściwemu do spraw informatyzacji na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych. Art. 59w. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa produktów ICT, usług ICT lub procesów ICT lub dla których została

				wydana krajowa deklaracja zgodności, udostępnia publicznie informacje zawierające: 1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT; 2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem; 3) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa; 4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatnościach związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa. 2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności.
10.	Art. 58 ust. 7 lit. e	e) w stosownych przypadkach zezwalają na działalność jednostek oceniających zgodność, zgodnie z art. 60 ust. 3, oraz ograniczają, zawieszają lub cofają istniejące zezwolenia, jeżeli jednostki oceniające zgodność naruszają wymogi niniejszego rozporządzenia;	Art. 59b pkt 11 oraz art. 59i	Art. 59b Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i; Art. 59i. 1. W przypadku, gdy europejski program certyfikacji cyberbezpieczeństwa określa szczegółowe lub dodatkowe wymagania, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, czynności

				w ramach oceny zgodności dokonywanej na jego podstawie wykonuje tylko jednostka oceniająca zgodność posiadająca zezwolenie ministra właściwego do spraw informatyzacji. 2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie przez jednostkę oceniającą zgodność zadań w ramach programów certyfikacji cyberbezpieczeństwa, o których mowa w ust. 1, na wniosek jednostki oceniającej zgodność, która spełniła wymagania określone w tych programach. 3. Minister właściwy do spraw informatyzacji może z urzędu cofnąć albo zawiesić zezwolenie, o którym mowa w ust. 2, jeżeli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa. Cofnięcie albo zawieszenie zezwolenia następuje w drodze decyzji. 4. Decyzję o zawieszeniu zezwolenia wydaje się na czas określony, nie dłuższy niż 2 lat. 5. W przypadku przywrócenia zgodności z postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu zezwolenia. 6. Minister właściwy do spraw informatyzacji cofa zezwolenie, jeżeli upłynął okres, na który wydano decyzję, o której mowa w ust. 4, a naruszenie postanowień ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa, nie ustało. 7. Do postępowań, o których mowa w ust. 3, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
11.	Art. 58 ust. 7 lit. f	f) rozpatrują skargi osób fizycznych lub prawnych dotyczące europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa, europejskich	Art. 59zd	Art. 59zd. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na: 1) podmiot, który wydał unijną lub krajową deklarację zgodności, jeżeli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja

		certyfikatów cyberbezpieczeństwa wydanych przez jednostki oceniające zgodność zgodnie z art. 56 ust. 6 lub unijnych deklaracji zgodności wydanych na podstawie art. 53 oraz badają w odpowiednim zakresie przedmiot takich skarg i informują skarżącego w rozsądnym terminie o postępach i wynikach badania;		dotyczy nie spełnia wymagań określonych w programie certyfikacji cyberbezpieczeństwa; 2) jednostkę oceniającą zgodność. 2. Minister rozpatruje skargi, o których mowa w ust. 1, w sposób i na zasadach określonych w programie certyfikacji cyberbezpieczeństwa, a w przypadku jeżeli program nie określa sposobu i zasad rozpatrywania skarg stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.”;
12.	Art. 58 ust. 7 lit. g	g) przedkładają ENISA i ECCG roczne sprawozdanie z działań przeprowadzonych na podstawie lit. b), c) i d) niniejszego ustępu lub na podstawie ust. 8;	Art. 59b pkt 12	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b-d oraz ust. 8 rozporządzenia 2019/881;
13.	Art. 58 ust. 7 lit. h	h) współpracują z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT i procesów ICT, z wymogami niniejszego rozporządzenia lub z wymogami określonych europejskich programów certyfikacji cyberbezpieczeństwa;	Art. 59b pkt 9	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa innych państw członkowskich lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymaganiami rozporządzenia 2019/881 lub z wymaganiami określonymi europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa;
14.	Art. 58 ust. 7 lit. i	i) monitorują odpowiednie zmiany w dziedzinie certyfikacji cyberbezpieczeństwa.	Art. 59b pkt 8	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

				8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;
15.	Art. 58 ust. 8 lit. a	8. Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa ma co najmniej następujące uprawnienia do: a) żądania od jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz podmiotów, które wydały unijne deklaracje zgodności przekazania wszelkich informacji, których organ ten potrzebuje do wykonywania swoich zadań;	Art. 59x	Art. 59x. Na wniosek ministra właściwego do spraw informatyzacji podmiot, o którym mowa w art. 59a ust. 1 pkt 3 i 4, , przedstawia informacje dotyczące: 1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności; 2) funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa; 3) liczby wydanych certyfikatów, w tym programów, w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały; 4) liczby wydanych deklaracji zgodności, w tym programów, w ramach których zostały wydane;
16.	Art. 58 ust. 8 lit. b – d	b) prowadzenia postępowań, w formie audytów, w stosunku do jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i podmiotów, które wydały unijne deklaracje zgodności, w celu weryfikacji przestrzegania przez nie niniejszego tytułu; c) stosowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia, by jednostki oceniające zgodność, posiadacze europejskich certyfikatów cyberbezpieczeństwa i podmioty, które wydały unijne deklaracje zgodności przestrzegali niniejszego rozporządzenia lub zachowywali zgodność z danym europejskim programem certyfikacji cyberbezpieczeństwa; d) uzyskania dostępu do pomieszczeń jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa do celów prowadzenia	Art. 59y – zd	Art. 59y. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59a ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT. 2. Do kontroli, o której mowa w ust. 1, przeprowadzonej wobec podmiotów: 1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców; 2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli. Art. 59z. Do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa stosuje się przepisy art. 55–59.

		postępowań zgodnie z prawem procesowym Unii lub państwa członkowskiego;		Art. 59za. Minister właściwy do spraw informatyzacji w ramach przeprowadzanej kontroli może poddać produkt ICT, usługę ICT lub proces ICT, dla których został wydany certyfikat lub deklaracja zgodności, badaniom lub zlecić ich przeprowadzenie, w celu ustalenia, czy spełniają one wymagania określone w ustawie, rozporządzeniu 2019/881, krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa. Art. 59zb. 1. Badanie, o którym mowa w art. 59za, może zostać przeprowadzone na próbkach produktu ICT. 2. Podmiot kontrolowany jest obowiązany do przekazania osobom prowadzącym czynności kontrolne wskazanej przez nie próbki produktu ICT. Z przekazania próbki sporządza się protokół. 3. Protokół zawiera nazwę produktu ICT, oznaczenie certyfikatu wydanego dla tego produktu ICT lub deklaracji zgodności wydanej dla tego produktu ICT , wielkość próbki przekazanej do badania, dane identyfikujące produkt ICT, takie jak numer seryjny przekazanego jako próbka egzemplarza produktu ICT oraz datę przekazania próbki. 4. Jeżeli przeprowadzone badania wykazały, że produkt ICT nie spełnia wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości informację o niespełnianiu przez produkt ICT wymagań określonych w programie certyfikacji. 5. W przypadku certyfikatów zatwierdzanych przez ministra właściwego do spraw informatyzacji, minister właściwy do spraw informatyzacji uchyla decyzję o zatwierdzeniu certyfikatu. 6. Koszty badań, o których mowa w art. 59za, ponosi podmiot kontrolowany. 7. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, wzór protokołu, o którym mowa w us3, kierując się

				potrzebą zapewnienia możliwości identyfikacji próbki produktu ICT oraz jednolitości i przejrzystości protokołów. Art. 59zc. 1. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że produkt ICT nie spełnia wymagań określonych w ustawie, rozporządzeniu 2019/881, europejskim programie certyfikacji cyberbezpieczeństwa lub krajowym programie certyfikacji cyberbezpieczeństwa informuje o tym podmiot, który wydał dany certyfikat. 2. Minister właściwy do spraw informatyzacji może cofnąć certyfikat w przypadku stwierdzenia, że produkt ICT, dla którego wydany został certyfikat odwołujący się do poziomu zaufania wysoki określony w europejskim programie certyfikacji cyberbezpieczeństwa lub krajowym programie certyfikacji cyberbezpieczeństwa. Art. 59zd. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na: 1) podmiot, który wydał unijną lub krajową deklarację zgodności, jeżeli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja dotyczy nie spełnia wymagań określonych w programie certyfikacji cyberbezpieczeństwa; 2) jednostkę oceniającą zgodność. 2. Minister rozpatruje skargi, o których mowa w ust. 1, w sposób i na zasadach określonych w programie certyfikacji cyberbezpieczeństwa, a w przypadku jeżeli program nie określa sposobu i zasad rozpatrywania skarg stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.”;

17.	Art. 58 ust. 8 lit. e	e) cofnięcia, zgodnie z prawem krajowym, europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa wydanych przez jednostki oceniające zgodność zgodnie z art. 56 ust. 6, jeżeli certyfikaty te nie są zgodne z niniejszym rozporządzeniem lub z europejskim programem certyfikacji cyberbezpieczeństwa;	Art. 59b pkt 14 Art. 59n	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 14) prowadzenie postępowań w zakresie cofnięcia certyfikatu; Art. 59n. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji niezwłocznie przesyła, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285) do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego: 1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania wysoki; 2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania wysoki. 2. Minister właściwy do spraw informatyzacji: 1) zatwierdza certyfikat, o którym mowa w ust. 1; 2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą, rozporządzeniem 2019/881 lub programami, o których mowa w ust. 1. 3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się, jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.

				4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg oceny zgodności. 5. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy może zasięgnąć opinii instytutu badawczego nadzorowanego przez tego ministra w zakresie zgodności certyfikacji z krajowym lub europejskim programem certyfikacji cyberbezpieczeństwa. Instytut badawczy przekazuje opinię w terminie 1 miesiąca od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 6. Minister właściwy do spraw informatyzacji cofa certyfikat, jeżeli jest on niezgodny z ustawą, rozporządzeniem 2019/881, europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa. 7. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.
18.	Art. 58 ust. 8 lit. f	f) nakładania kar zgodnie z prawem krajowym, jak przewidziano w art. 65, oraz żądania natychmiastowego zaprzestania naruszeń obowiązków określonych w niniejszym rozporządzeniu.	Art. 59b pkt 2 oraz Art. 73 ust. 1a-1c	Art. 59b Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, stosowania przepisów rozporządzenia 2019/881 oraz postanowień krajowych lub europejskich programów certyfikacji cyberbezpieczeństwa; Art. 73 . „1a. Jednostka oceniająca zgodność, która nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne, podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok

				poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”. 1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających, w chwili jego wydania, wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia. 1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: 1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, 2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, 3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, 4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji, 5) nie wykonuje obowiązku określonego w art. 59u – podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.”,
19.	Art. 58 ust. 9	9. Krajowe organy ds. certyfikacji cyberbezpieczeństwa współpracują ze sobą i z Komisją, w szczególności wymieniając informacje, doświadczenie i dobre praktyki odnoszące się do certyfikacji cyberbezpieczeństwa i	Art. 59b pkt 9	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

		kwestii technicznych dotyczących cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT.		9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa innych państw członkowskich lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymaganiami rozporządzenia 2019/881 lub z wymaganiami określonymi europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa;
20.	Art. 59	1. W celu uzyskania równoważnych norm w całej Unii w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności krajowe organy ds. certyfikacji cyberbezpieczeństwa podlegają wzajemnemu przeglądowi. 2. Wzajemny przegląd przeprowadza się w oparciu o rzetelne i przejrzyste kryteria i procedury oceny, w szczególności w odniesieniu do wymagań dotyczących struktury, zasobów ludzkich i procedur, poufności i skarg. 3. W ramach wzajemnego przeglądu ocenia się: a) w stosownych przypadkach – czy działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, jest ściśle oddzielona od działalności związanej z nadzorem określonej w art. 58 i czy te działalności są wykonywane niezależnie od siebie; b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z europejskimi certyfikatami cyberbezpieczeństwa na podstawie art. 58 ust. 7 lit. a);	Art. 59b pkt 4	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 4) przeprowadzanie wzajemnego przeglądu o którym mowa w art. 59 rozporządzenia 2019/881;

		c) procedury nadzorowania i egzekwowania obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT na podstawie art. 58 ust. 7 lit. b); d) procedury monitorowania, wydawania zezwoleń na działalność i nadzorowania działalności jednostek oceniających zgodność; e) w stosownych przypadkach – czy członkowie personelu organów i jednostek wydających certyfikaty o poziomie uzasadnienia zaufania „wysoki” zgodnie z art. 56 ust. 6 mają odpowiednią wiedzę fachową. 4. Wzajemny przegląd musi być przeprowadzany przez co najmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisję i musi być przeprowadzany co najmniej raz na pięć lat. ENISA może uczestniczyć we wzajemnym przeglądzie. 5. Komisja może przyjmować akty wykonawcze ustanawiające plan wzajemnego przeglądu obejmujący okres co najmniej pięciu lat, ustanawiające kryteria dotyczące składu zespołu ds. wzajemnego przeglądu, metodykę wykorzystywaną do wzajemnego przeglądu, harmonogram, częstotliwość oraz inne zadania związane z wzajemnym przeglądem. Przyjmując te akty wykonawcze, Komisja należycie uwzględnia stanowisko ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2. 6. Wyniki wzajemnych przeglądów analizuje ECCG, która sporządza podsumowania, które można podawać do wiadomości publicznej, i która, w razie potrzeby, wydaje		

		wytyczne lub zalecenia dotyczące działań lub środków, jakie mają podjąć zainteresowane podmioty.		
21.	Art. 60 ust. 1-2	1. Jednostki oceniające zgodność są akredytowane przez krajowe jednostki akredytujące wyznaczone na podstawie rozporządzenia (WE) nr 765/2008. Akredytacji takiej udziela się jedynie wtedy, gdy jednostki oceniające zgodność spełniają wymagania określone w załączniku do niniejszego rozporządzenia. 2. W przypadku gdy europejski certyfikat cyberbezpieczeństwa wydawany jest przez krajowy organ ds. certyfikacji cyberbezpieczeństwa na podstawie art. 56 ust. 5 lit. a) i art. 56 ust. 6, jednostkę certyfikującą krajowego organu ds. certyfikacji cyberbezpieczeństwa akredytuje się jako jednostkę oceniającą zgodność na podstawie ust. 1 niniejszego artykułu. .	Art. 59h	Art. 59h. . 1. Oceny zgodności w obszarze cyberbezpieczeństwa dokonuje jednostka oceniająca zgodność akredytowana z uwzględnieniem wymagań określonych w art. 59c posiadająca akredytację obejmującą ocenę zgodności produktu ICT, usługi ICT lub procesu ICT, w obszarze cyberbezpieczeństwa. 2. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji. 3. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. 4. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych programów certyfikacji cyberbezpieczeństwa i europejskich programów certyfikacji cyberbezpieczeństwa. 5. Informacja o udzielonej akredytacji, o której mowa w ust. 2, zawiera: 1) oznaczenie podmiotu, któremu udzielono akredytacji; 2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji. 6. Akredytacji udziela się na okres nie dłuższy niż 5 lat. 7. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu akredytacji jednostce oceniającej zgodność. 8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera: 1) oznaczenie podmiotu, któremu cofnięto akredytację;

				2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji; 3) datę cofnięcia akredytacji.
22.	Art. 60 ust. 3	3. W przypadku gdy europejskie programy certyfikacji cyberbezpieczeństwa określają szczególne lub dodatkowe wymogi zgodnie z art. 54 ust. 1 lit. f), krajowy organ ds. certyfikacji cyberbezpieczeństwa może zezwolić na wykonywanie zadań w ramach takich programów wyłącznie takim jednostkom oceniającym zgodność, które spełniają te wymogi.	Art. 59i	Art. 59i. 1. W przypadku, gdy europejski program certyfikacji cyberbezpieczeństwa określa szczegółowe lub dodatkowe wymagania, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, czynności w ramach oceny zgodności dokonywanej na jego podstawie wykonuje tylko jednostka oceniająca zgodność posiadająca zezwolenie ministra właściwego do spraw informatyzacji. 2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie przez jednostkę oceniającą zgodność zadań w ramach programów certyfikacji cyberbezpieczeństwa, o których mowa w ust. 1, na wniosek jednostki oceniającej zgodność, która spełniła wymagania określone w tych programach. 3. Minister właściwy do spraw informatyzacji może z urzędu cofnąć albo zawiesić zezwolenie, o którym mowa w ust. 2, jeżeli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa. Cofnięcie albo zawieszenie zezwolenia następuje w drodze decyzji. 4. Decyzję o zawieszeniu zezwolenia wydaje się na czas określony, nie dłuższy niż 2 lat. 5. W przypadku przywrócenia zgodności z postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu zezwolenia. 6. Minister właściwy do spraw informatyzacji cofa zezwolenie, jeżeli upłynął okres, na który wydano decyzję, o której mowa w ust. 4, a naruszenie postanowień ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa, nie ustało.

				7. Do postępowań, o których mowa w ust. 3, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
23.	Art. 60 ust. 4	4. Akredytacji, o której mowa w ust. 1, udziela się jednostkom oceniającym zgodność na maksymalnie pięć lat i można ją odnowić na tych samych warunkach, o ile jednostka oceniająca zgodność nadal spełnia wymogi określone w niniejszym artykule. Krajowe jednostki akredytujące podejmują, w odpowiednich ramach czasowych, wszelkie stosowne środki w celu ograniczenia, zawieszenia lub cofnięcia akredytacji jednostki oceniającej zgodność udzielonej na podstawie ust. 1, w przypadku gdy warunki udzielenia akredytacji nie zostały spełnione, przestały być spełnione lub gdy jednostka oceniająca zgodność narusza niniejsze rozporządzenie.	Art. 59c oraz art. 59h	Art. 59c. Polskie Centrum Akredytacji sprawuje nadzór w zakresie udzielonej akredytacji nad akredytowanymi jednostkami prowadzącymi ocenę zgodności produktów ICT, usług ICT lub procesów ICT w obszarze cyberbezpieczeństwa, przy uwzględnieniu wymagań, o których mowa w art. 22 ust. 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) oraz wymagań określonych w: 1) załączniku do rozporządzenia 2019/881; 2) poszczególnych europejskich programach certyfikacji cyberbezpieczeństwa lub krajowych programach certyfikacji cyberbezpieczeństwa. Art. 59h. 1. Oceny zgodności w obszarze cyberbezpieczeństwa dokonuje jednostka oceniająca zgodność akredytowana z uwzględnieniem wymagań określonych w art. 59c posiadająca akredytację obejmującą ocenę zgodności produktu ICT, usługi ICT lub procesu ICT, w obszarze cyberbezpieczeństwa. 2. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji. 3. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. 4. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych programów certyfikacji cyberbezpieczeństwa i europejskich programów certyfikacji cyberbezpieczeństwa. 5. Informacja o udzielonej akredytacji, o której mowa w ust. 2, zawiera:

				1) oznaczenie podmiotu, któremu udzielono akredytacji; 2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji. 6. Akredytacji udziela się na okres nie dłuższy niż 5 lat. 7. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu akredytacji jednostce oceniającej zgodność. 8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera: 1) oznaczenie podmiotu, któremu cofnięto akredytację; 2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji; 3) datę cofnięcia akredytacji.
24.	Art. 62	1. Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („ECCG”). 2. W skład ECCG wchodzą przedstawiciele krajowych organów ds. certyfikacji cyberbezpieczeństwa lub przedstawiciele innych odpowiednich organów krajowych. Członek ECCG nie może reprezentować więcej niż dwóch państw członkowskich. 3. Interesariusze i odpowiednie strony trzecie mogą być zapraszani na posiedzenia ECCG i do udziału w jej pracach. 4. ECCG ma następujące zadania: a) doradzanie i pomaganie Komisji przy pracach nad zapewnieniem spójnego wprowadzania i stosowania niniejszego tytułu, w szczególności w odniesieniu do unijnego kroczącego programu prac, kwestii związanych z	Art. 59b pkt 13	Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy: 13) uczestniczenie w pracach ECCG;

		polityką certyfikacji cyberbezpieczeństwa, koordynacji koncepcji politycznych oraz przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa; b) pomaganie, doradzanie i współpracowanie z ENISA w związku z przygotowywaniem propozycji programu na podstawie art. 49; c) wydawanie opinii na temat propozycji programu przygotowanej przez ENISA na podstawie art. 49 niniejszego rozporządzenia; d) zwracanie się do ENISA z wnioskiem o przygotowanie propozycji programu na podstawie art. 48 ust. 2; e) wydawanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa; f) monitorowanie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk odnoszących się do programów certyfikacji cyberbezpieczeństwa; g) ułatwianie współpracy pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa w ramach niniejszego tytułu poprzez budowanie zdolności, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa; h) wspieranie w zakresie wdrażania mechanizmów wzajemnej oceny zgodnie z zasadami ustanowionymi w		

		danym europejskim programie certyfikacji cyberbezpieczeństwa na podstawie art. 54 ust. 1 lit. u); i) ułatwianie dostosowywania europejskich programów cyberbezpieczeństwa do międzynarodowo uznanych norm, w tym przez dokonywanie przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa i, w stosownych przypadkach, wydawanie skierowanych do ENISA zaleceń dotyczących podjęcia współpracy z odpowiednimi międzynarodowymi organizacjami normalizacyjnymi w celu wyeliminowania braków lub luk w istniejących międzynarodowo uznanych normach. 5. Komisja, z pomocą ENISA, przewodniczy ECCG i zapewnia ECCG obsługę sekretariatu, zgodnie z art. 8 ust. 1 lit. e).		
25.	Art. 65	Państwa członkowskie ustanawiają przepisy o karach nakładanych w przypadku naruszenia niniejszego tytułu i naruszenia europejskich programów certyfikacji cyberbezpieczeństwa oraz stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie niezwłocznie powiadamiają Komisję o tych przepisach i środkach, a następnie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.	Art. 73 ust. 1a-1c	Art. 73 1a. Jednostka oceniająca zgodność, która nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne, podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”. 1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających, w chwili jego wydania, wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w

				wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia. 1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: 1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, 2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, 3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, 4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji, 5) nie wykonuje obowiązku określonego w art. 59u – podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.”,”,

TABELA ZGODNOŚCI	
TYTUŁ PROJEKTU	Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE. L 2018 Nr 321, str. 36)
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU	Termin wejścia w życie uwzględnia konieczność jak najszybszego wprowadzenia w życie tych przepisów.

l.p.	jednostka redakcyjna Europejskiego Kodeksu Łączności Elektronicznej	treść przepisu UE	jednostka redakcyjna ustawy	treść przepisu/przepisów projektu ustawy
1.	Art. 2 pkt 21	„bezpieczeństwo sieci i usług” oznacza zdolność sieci i usług łączności elektronicznej do odpierania, na danym poziomie pewności, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność tych sieci i usług, przechowywanych, przekazywanych lub przetwarzanych danych lub związanych z nimi usług oferowanych przez te sieci lub usługi łączności elektronicznej lub dostępnych za ich pośrednictwem;	Art. 2 pkt 2	2) bezpieczeństwo sieci lub usług komunikacji elektronicznej – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność: a) tych sieci lub usług, b) przetwarzanych informacji objętych tajemnicą komunikacji elektronicznej, c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;
2.	Art. 2 pkt 42	42)„incydent związany z bezpieczeństwem” oznacza zdarzenie, które ma rzeczywisty niekorzystny skutek dla bezpieczeństwa sieci lub usługi łączności elektronicznej.	Art. 2 pkt 20	incydent telekomunikacyjny – każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci lub usług komunikacji elektronicznej;
3.	Art. 29	Art. 29 1. Państwa członkowskie ustanawiają przepisy dotyczące sankcji, w tym, w razie potrzeby, grzywien i innych niż karne określonych z góry lub okresowych sankcji, mających zastosowanie do naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy lub	Art. 76a-76b	Art. 76a. 1. Karze pieniężnej podlega przedsiębiorca komunikacji elektronicznej, który: 1) nie wypełnia obowiązku systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia, o którym mowa w art. 20a ust. 2;

		dowolnej wiążącej decyzji przyjętej przez Komisję, krajowy organ regulacyjny lub inny właściwy organ na podstawie niniejszej dyrektywy oraz wprowadzają wszelkie środki niezbędne, by zapewnić ich wykonanie. W granicach określonych przepisami krajowego prawa krajowe organy regulacyjne lub inne właściwe organy mają prawo nakładać takie sankcje. Przewidziane sankcje muszą być odpowiednie, skuteczne, proporcjonalne i odstraszające. 2. Państwa członkowskie przewidują sankcje w kontekście procedury, o której mowa w art. 22 ust. 3, jedynie w przypadku gdy przedsiębiorstwo lub organ publiczny świadomie lub w sposób rażąco niedbały przekazują mylące, błędne lub niepełne informacje. Przy określaniu kwoty grzywien lub okresowych sankcji nakładanych na przedsiębiorstwo lub organ publiczny za świadome lub rażąco niedbałe przekazanie mylących, błędnych lub niepełnych informacji w kontekście procedury, o której mowa w art. 22 ust. 3, uwzględnia się, między innymi, czy postępowanie przedsiębiorstwa lub organu publicznego miało negatywny wpływ na konkurencję i, w szczególności, czy wbrew pierwotnie przekazanym informacjom lub wszelkiej ich aktualizacji przedsiębiorstwo lub organ publiczny wdrożył, rozbudował albo zmodernizował sieć lub nie wdrożył sieci lub nie dostarczył obiektywnego uzasadnienia tej zmiany planu.		2) nie podejmuje środków, o których mowa w art 20a ust. 2 pkt 2; 3) nie dokumentuje czynności, o których mowa w art. 20a ust. 2 pkt 1 i 2; 4) nie przekazuje informacji, o których mowa w art. 20b ust. 2, w terminie wskazanym w żądaniu Prezesa UKE; 5) nie wykonuje obowiązku, o którym mowa w art. 20b ust. 4, w terminie wskazanym w decyzji Prezesa UKE; 6) nie obsługuje incydentu telekomunikacyjnego, o którym mowa w art. 20c pkt 1; 7) nie zgłasza poważnego incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2; 8) nie współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco lub z właściwym CSIRTMON, CSIRT NASK, CSIRT GOV i tym samym nie wykonuje obowiązku, o którym mowa w art. 20d ust. 1 pkt 3; 9) nie usuwa w wyznaczonym przez Prezesa UKE terminie podatności, która doprowadziła lub mogła doprowadzić do incydentu telekomunikacyjnego lub krytycznego, o której mowa w art. 54a; 10) nie wykonuje zaleceń pokontrolnych Prezesa UKE, o których mowa w art. 59. 2. Prezes UKE, jeżeli przemawia za tym charakter lub zakres naruszenia, może nałożyć karę pieniężną na przedsiębiorcę komunikacji elektronicznej, który: 1) nie wyznacza dwóch osób, o których mowa w art. 20a ust. 4; 2) nie zapewnia dostępu do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań;

				3) nie wykonuje obowiązku, o którym mowa w art. 20f ust. 1 i 2; 4) nie wykonuje obowiązku, o którym mowa w art. 20h ust. 5. 3. Kara, o której mowa w ust. 1 i 2, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia. 4. Karę, o której mowa w ust. 1: 1) pkt 6 – nakłada się za każdy stwierdzony przypadek zaniechania obsługi incydentu telekomunikacyjnego; 2) pkt 7 – nakłada się za każdy stwierdzony przypadek niezgłoszenia poważnego incydentu telekomunikacyjnego. 5. Niezależnie od kar pieniężnych, o których mowa w ust. 1 i 2, Prezes UKE może nałożyć na osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy. Art. 76b. 1. Kary pieniężne, o których mowa w art. 76a ust. 1 i 2, nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności. 2. W przypadku, gdy podmiot w roku kalendarzowym poprzedzającym rok nałożenia kary pieniężnej nie osiągnął przychodu lub osiągnął przychód w wysokości nieprzekraczającej 500 000 zł, Prezes UKE nakładając karę pieniężną uwzględnia średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej.

				3. W przypadku, gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, lub gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł. 4. W przypadku, gdy przed wydaniem decyzji o nałożeniu kary pieniężnej podmiot nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary pieniężnej, Prezes UKE nakładając karę pieniężną, uwzględnia: 1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok; 2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających ten rok. Przepis ust. 3 stosuje się odpowiednio. 5. W przypadku, gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, o którym mowa w ust. 1, Prezes UKE uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary. Przepisy ust. 2–4 stosuje się odpowiednio. 6. Ustalając wysokość kary pieniężnej Prezes UKE uwzględnia charakter i zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe. 7. Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 1 miesiąca od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej

				w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 złotych.
4.	Art. 40 ust. 1	1. Państwa członkowskie zapewniają, aby dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowały właściwe i proporcjonalne środki techniczne i organizacyjne w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Środki te muszą zapewniać poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka z uwzględnieniem aktualnego stanu wiedzy i technologii. W szczególności wprowadza się środki, obejmujące, w stosowanych przypadkach, szyfrowanie, zapobiegające wpływowi i minimalizujące wpływ, jaki na użytkowników i na inne sieci i usługi mogą mieć przypadki stwarzające zagrożenie bezpieczeństwa. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) ułatwia zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 526/2013 (45) koordynację państw członkowskich, aby uniknąć powstawania rozbieżnych krajowych wymogów, które mogą tworzyć ryzyko dla bezpieczeństwa i bariery dla rynku wewnętrznego.	Art. 1 ust. 2, Art. 20a ust. 1-3 i 7 Art. 20c Art. 20g	Art. 1 - w ust. 2: – uchyla się pkt 1; Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia. 2. Przedsiębiorca komunikacji elektronicznej: 1) przeprowadza systematyczne szacowanie ryzyka wystąpienia sytuacji szczególnego zagrożenia co najmniej raz w roku; 2) podejmuje środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów: a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia, c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,

				d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej – przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków; 3) dokumentuje czynności, o których mowa w pkt 1 i 2. 3. Przedsiębiorca komunikacji elektronicznej sporządzający plan działań w sytuacji szczególnego zagrożenia dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2. 7. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA", skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej. Art. 20c. Przedsiębiorca komunikacji elektronicznej: 1) zapewnia obsługę incydentu telekomunikacyjnego; 2) może przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco informacje: a) o cyberzagrożeniach, podatnościach i incydentach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci lub usług komunikacji elektronicznej, b) o wykorzystywanych technologiach;

				3) zapewnia dostęp do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań. Art. 20g. W przypadku stwierdzenia przesyłania komunikatów elektronicznych zagrażających bezpieczeństwu sieci lub usług komunikacji elektronicznej, przedsiębiorca komunikacji elektronicznej, może zastosować środki polegające na: 1) zablokowaniu przesłania takiego komunikatu, 2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej – w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.
5.	Art. 40 ust. 2	2. Państwa członkowskie zapewniają, aby podmioty udostępniające publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały bez zbędnej zwłoki właściwy organ o incydentach związanych z bezpieczeństwem, które miały znaczący wpływ na funkcjonowanie sieci lub usług. Aby określić istotność wpływu danego incydentu związanego z bezpieczeństwem, uwzględnia się w szczególności następujące parametry, gdy są dostępne:	Art. 20d i art. 20e	Art. 20d. 1. Przedsiębiorca komunikacji elektronicznej: 1) uznaje incydent telekomunikacyjny za poważny incydent telekomunikacyjny; 2) zgłasza poważny incydent telekomunikacyjny, niezwłocznie, nie później niż w ciągu 8 godzin od momentu jego wykrycia, do CSIRT Telco; 3) współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco oraz z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe. 2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania go

		a) liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem; b) czas trwania incydentu związanego z bezpieczeństwem; c) geograficzny zasięg obszaru dotkniętego incydentem związanym z bezpieczeństwem; d) zakres wpływu na funkcjonowanie sieci lub usługi; e) zakres wpływu na działalność ekonomiczną i społeczną.		w postaci elektronicznej przy użyciu innych dostępnych środków komunikacji. 3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, biorąc pod uwagę rekomendacje ENISA, progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny, uwzględniając: 1) liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ; 2) czas trwania skutków incydentu telekomunikacyjnego; 3) obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego; 4) zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług; 5) wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej; 6) wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 7) wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych; 8) wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Art. 20e. 1. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, zawiera: 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy oraz numer we właściwym rejestrze, jeżeli został nadany;

				2) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia; 3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; 4) opis wpływu incydentu telekomunikacyjnego na sieci i usługi, w tym: a) sieci telekomunikacyjne, na które poważny incydent telekomunikacyjny miał wpływ, b) usługi komunikacji elektronicznej zgłaszającego, na które poważny incydent telekomunikacyjny miał wpływ, c) liczbę użytkowników usługi komunikacji elektronicznej, na których poważny incydent telekomunikacyjny miał wpływ, d) moment wystąpienia i wykrycia poważnego incydentu telekomunikacyjnego oraz czas jego trwania, e) zasięg geograficzny obszaru, którego dotyczy poważny incydent telekomunikacyjny, f) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi kluczowej przez operatorów usług kluczowych, jeżeli jest znany, g) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi cyfrowej przez dostawców usług cyfrowych, jeżeli jest znany, h) przyczynę zaistnienia poważnego incydentu telekomunikacyjnego i sposób jego przebiegu oraz skutki jego oddziaływania na sieci telekomunikacyjne lub świadczone usługi komunikacji elektronicznej,

				i) wpływ poważnego incydentu telekomunikacyjnego na połączenia z numerami alarmowymi, j) wpływ poważnego incydentu telekomunikacyjnego na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego; 5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej; 6) informacje o podjętych działaniach zapobiegawczych; 7) informacje o podjętych działaniach naprawczych. 2. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, może zawierać inne istotne informacje. 3. Przedsiębiorca komunikacji elektronicznej przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu telekomunikacyjnego. 4. Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20d ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu telekomunikacyjnego przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco. 5. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco może zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

				6. W zgłoszeniu przedsiębiorca komunikacji elektronicznej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
6.	Art. 40 ust. 2	W stosownych przypadkach dany właściwy organ informuje właściwe organy innych państw członkowskich oraz ENISA. W przypadku gdy właściwy organ uzna, że ujawnienie incydentu związanego z bezpieczeństwem leży w interesie publicznym, może podać tę informację do wiadomości publicznej lub nałożyć taki obowiązek na podmioty. Raz w roku właściwy organ przekazuje Komisji i ENISA sprawozdanie podsumowujące otrzymane zgłoszenia i działania podjęte zgodnie z niniejszym ustępem.	Art. 20h	Art. 20h. 1. Prezes UKE kierując się rekomendacjami ENISA dotyczącymi raportowania incydentów telekomunikacyjnych: 1) informuje o wystąpieniu poważnego incydentu telekomunikacyjnego organy regulacyjne innych państw członkowskich oraz ENISA, jeżeli uzna charakter tego incydentu za istotny; 2) przekazuje Komisji Europejskiej oraz ENISA sprawozdanie za rok poprzedni zawierające informacje o poważnych incydentach telekomunikacyjnych. 2. Prezes UKE może publikować na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej, w przypadkach uzasadnionych interesem publicznym, informację o wystąpieniu poważnego incydentu telekomunikacyjnego. 3. Prezes UKE informuje niezwłocznie, w terminie nie dłuższym niż 3 dni, przedsiębiorcę komunikacji elektronicznej, u którego wystąpił poważny incydent telekomunikacyjny, o opublikowaniu informacji, o której mowa w ust. 2, wraz ze wskazaniem adresu elektronicznego, pod którym udostępniona jest ta informacja. 4. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 3, jest obowiązany opublikować na swojej stronie internetowej informację o wystąpieniu poważnego incydentu telekomunikacyjnego oraz umieścić adres elektroniczny, o którym mowa w ust. 3, niezwłocznie, nie później niż w terminie 3 dni od otrzymania informacji, o której mowa w ust. 3. 5. Prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej, o którym mowa w ust. 3, obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób jej publikacji, jeżeli

				sposoby opublikowania informacji, o których mowa w ust. 2 i 3, w niewystarczającym stopniu służą ochronie interesu publicznego.”;
7.	Art. 40 ust. 3	3. Państwa członkowskie zapewniają, aby w przypadku szczególnego i znacznego zagrożenia wystąpieniem incydentu związanego z bezpieczeństwem w publicznych sieciach łączności elektronicznej lub w ramach dostępnych publicznie usług łączności elektronicznej podmioty udostępniające takie sieci lub świadczące takie usługi informowały swoich użytkowników, na których takie zagrożenie może mieć wpływ, o wszelkich możliwych środkach ochronnych lub naprawczych, które użytkownicy mogą podjąć. W stosownych przypadkach podmioty powinny informować swoich użytkowników również o samym zagrożeniu.	Art. 20f	Art. 20f. 1. Przedsiębiorca komunikacji elektronicznej publikuje na swojej stronie internetowej informacje o: 1) potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej; 2) rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym; 3) przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych. 2. Przedsiębiorca komunikacji elektronicznej, w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego, informuje swoich użytkowników, na których takie zagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach. Przedsiębiorca komunikacji elektronicznej informuje tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. 3. Przedsiębiorca komunikacji elektronicznej, informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.
8.	Art. 40 ust. 4	4. Przepisy niniejszego artykułu nie naruszają przepisów rozporządzenia (UE) 2016/679 oraz dyrektywy 2002/58/WE.	Nd.	Proponowane zmiany w art. 39 ustawy o krajowym systemie cyberbezpieczeństwa dot. przetwarzania danych osobowych pozyskanych w związku ze zgłoszeniem incydentu telekomunikacyjnego

				przez CSIRT Telco mieszczą się w ramach przepisów rozporządzenia (UE) 2016/679.
9.	Art. 40 ust. 5	5. Komisja, w jak największym stopniu uwzględniając opinię ENISA, może przyjąć akty wykonawcze określające szczegółowo techniczne i organizacyjne środki, o których mowa w ust. 1, a także okoliczności, format i procedury stosowane w odniesieniu do wymogów dotyczących zgłoszenia na podstawie ust. 2. Opierają się one w jak najszerszym zakresie na normach europejskich i międzynarodowych i nie uniemożliwiają państwom członkowskim przyjmowania dodatkowych wymogów służących osiągnięciu celów określonych w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 118 ust. 4.	Nd.	Przepis skierowany do Komisji.
10.	Art. 41 ust. 1	1. Państwa członkowskie zapewniają, aby w celu wdrożenia art. 40 właściwe organy były uprawnione do wydawania wiążących instrukcji – w tym instrukcji dotyczących środków wymaganych, aby zaradzić incydentowi związanemu z bezpieczeństwem lub aby zapobiec wystąpieniu takiego incydentu, gdy zidentyfikowano znaczne zagrożenie, oraz terminów wdrożenia – podmiotom udostępniającym publiczne sieci łączności elektronicznej lub świadczącym publicznie dostępne usługi łączności elektronicznej.	Art. 20b ust. 4-5 i art. 20d ust. 1 pkt 3 oraz art. 44a	Art. 20b ust. 4. Prezes UKE może, w drodze decyzji, w przypadku powstania w wyniku dokonanej oceny, o której mowa w ust. 1, uzasadnionych wątpliwości co do stosowania właściwych środków technicznych i organizacyjnych, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek: 1) właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych lub 2) poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę komunikacji elektronicznej, niezależny podmiot i udostępnienia Prezesowi UKE wyników tego audytu. 5. W decyzji nakładającej obowiązek, o którym mowa w ust. 4: 1) w pkt 1 – Prezes UKE wskazuje termin właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych;

				2) w pkt 2 – Prezes UKE określa termin udostępnienia wyników audytu bezpieczeństwa. Art. 20d. 3) współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco oraz z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe. „Art. 44a. . 3. Do zadań CSIRT Telco w ramach wspierania przedsiębiorców komunikacji elektronicznej należy: 1) przyjmowanie zgłoszeń o incydentach telekomunikacyjnych; 2) reagowanie na incydenty telekomunikacyjne; 6. CSIRT Telco może zwrócić się do Prezesa UKE o wezwanie przedsiębiorcy komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego. Art. 53 ust. 1 pkt 3 oraz ust. 2 pkt 3 „1. Nadzór w zakresie stosowania przepisów ustawy sprawują: 3) Prezes UKE w zakresie wypełniania przez przedsiębiorców komunikacji elektronicznej obowiązków określonych w art. 20a ust. 2 i 3, art. 20b ust. 2 i 4, art. 20d ust. 1 i art. 20f oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b.”, „2. W ramach nadzoru, o którym mowa w ust. 1:

				3) Prezes UKE prowadzi kontrole w zakresie, o którym mowa w ust. 1 w pkt 3, oraz nakłada kary pieniężne na przedsiębiorców komunikacji elektronicznej."; Art. 54a. Prezes UKE może, po otrzymaniu wniosku od CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego.
11.	Art. 41 ust. 2	2. Państwa członkowskie zapewniają, aby właściwe organy były uprawnione do wymagania od podmiotów udostępniających publiczne sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej: a) dostarczania informacji potrzebnych do oceny bezpieczeństwa ich sieci i usług, w tym do oceny udokumentowanych polityk bezpieczeństwa; oraz b) poddania się audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany niezależny podmiot lub właściwy organ i udostępnienia właściwemu organowi wyników takiego audytu. Koszty wspomnianego audytu ponosi dostawca.	Art. 20b ust. 2-6	Art. 20b.. 2. Przedsiębiorca komunikacji elektronicznej jest obowiązany do przekazania Prezesowi UKE, na jego żądanie, informacji niezbędnych do dokonania oceny. 3. Żądanie, o którym mowa w ust. 2, zawiera: 1) wskazanie podmiotu obowiązanego do przekazania informacji; 2) datę; 3) wskazanie zakresu żądanych informacji oraz okresu, którego dotyczą; 4) wskazanie celu, jakiemu informacje mają służyć; 5) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni; 6) pouczenie o zagrożeniu karą, o której mowa w art. 76a ust. 1 pkt 4.

				4. Prezes UKE może, w drodze decyzji, w przypadku powstania w wyniku dokonanej oceny, o której mowa w ust. 1, uzasadnionych wątpliwości co do stosowania właściwych środków technicznych i organizacyjnych, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek: 1) właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych lub 2) poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę komunikacji elektronicznej, niezależny podmiot i udostępnienia Prezesowi UKE wyników tego audytu. 5. W decyzji nakładającej obowiązek, o którym mowa w ust. 4: 1) w pkt 1 – Prezes UKE wskazuje termin właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych; 2) w pkt 2 – Prezes UKE określa termin udostępnienia wyników audytu bezpieczeństwa. 6. Do audytu bezpieczeństwa, o którym mowa w ust. 5 pkt 2, stosuje się odpowiednio art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5. Audytorzy, o których mowa w art. 15 ust. 2 pkt 2, wykonujący audyt bezpieczeństwa muszą być niezależni od przedsiębiorcy komunikacji elektronicznej, u którego prowadzony jest audyt bezpieczeństwa.

12.	Art. 41 ust. 3	3. Państwa członkowskie zapewniają, aby właściwe organy posiadały wszelkie uprawnienia niezbędne do badania przypadków nieprzestrzegania wymogów oraz ich wpływu na bezpieczeństwo sieci i usług.	Art. 20b ust. 1 Art. 53 ust. 1 pkt 3 oraz ust. 2 pkt 3	Art. 20b. 1. Prezes UKE może dokonywać oceny zastosowanych przez przedsiębiorcę komunikacji elektronicznej środków technicznych i organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2, kierując się rekomendacjami ENISA. Art. 53 ust. 1 pkt 3 oraz ust. 2 pkt 3 „3) Prezes UKE w zakresie wypełniania przez przedsiębiorców komunikacji elektronicznej obowiązków określonych w art. 20a ust. 2 i 3, art. 20b ust. 2 i 4, art. 20d ust. 1 i art. 20f oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b.”, „3) Prezes UKE prowadzi kontrole w zakresie, o którym mowa w ust. 1 w pkt 3, oraz nakłada kary pieniężne na przedsiębiorców komunikacji elektronicznej.”;
13.	Art. 41 ust. 4	4. Państwa członkowskie zapewniają, aby – w celu wdrożenia przepisów art. 40 – właściwe organy dysponowały uprawnieniami pozwalającymi im zwracać się o pomoc do Zespołu Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym (CSIRT) wyznaczonego na podstawie art. 9 dyrektywy (UE) 2016/1148 w związku z problemami wchodzącymi w zakres zadań CSIRT zgodnie z pkt 2 załącznika I do tej dyrektywy.	Art. 44a ust. 3 pkt 5	Art. 44a 3. Do zadań CSIRT Telco w ramach wspierania przedsiębiorców komunikacji elektronicznej należy: 5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymiany informacji o cyberzagrożeniach.
14.	Art. 41 ust. 5	5. Właściwe organy, w stosownych przypadkach oraz zgodnie z prawem krajowym, konsultują się i współpracują z odpowiednimi krajowymi organami ścigania, właściwymi organami w rozumieniu art. 8 ust. 1 dyrektywy (UE) 2016/1148 oraz krajowymi organami ds. ochrony danych.	art. 34 ust.1 art. 44a ust. 3 pkt 7	art. 34 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy, CSIRT Telco oraz SOC zewnętrzne współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. art. 44a ust. 3 Do zadań CSIRT Telco w ramach wspierania przedsiębiorców komunikacji elektronicznej należy:

				7) współpraca z organem właściwym do spraw ochrony danych osobowych podczas reagowania na incydent telekomunikacyjny, który doprowadził do naruszenia ochrony danych osobowych.

ODWRÓCONA TABELA ZGODNOŚCI			
projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw			
l.p.	**jednostka redakcyjna projektu**	**treść przepisu**	**uzasadnienie wprowadzenia przepisu**
1.	Art. 1	po pkt 1 dodaje się pkt 1a w brzmieniu: „1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno–komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanego dalej „rozporządzeniem 2019/881;”, – w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4–6 w brzmieniu: „4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów; 5) zasady wyznaczania Operatora strategicznej sieci bezpieczeństwa oraz jego zadania; 6) zasady przyznania zasobów częstotliwości z zakresu 703 – 7133 MHz oraz 758 – 7688 MHz; b) w ust. 2: – pkt 2 otrzymuje brzmienie: „2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73), z wyjątkiem art. 67a i 67b oraz art. 73 i 74;	Niniejsza ustawa oprócz implementacji przepisów Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15) (dalej akt o cyberbezpieczeństwie) wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.

2.	Art. 2 ust. 1 pkt 3	3) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;	Projekt ustawy dostosowuje katalog definicji w ustawie o KSC do zmian jakie zostały wprowadzone w akcie o cyberbezpieczeństwie. W szczególności oznacza to konieczność przyjęcia nowej definicji cyberbezpieczeństwa, która została wprowadzona w ww. akcie prawnym. Tam gdzie jest to konieczne, zachowano poprzednie znaczenia terminu: „cyberbezpieczeństwo" i wprowadzone zostało pojęcie „bezpieczeństwa systemów informacyjnych" (art. 2 pkt 4a), którego zakres jest identyczny z poprzednią definicją cyberbezpieczeństwa. Nie spowoduje to jednak zmian w zakresie konkretnych obowiązków, jakie obecnie nakłada ustawa na podmioty krajowego systemu cyberbezpieczeństwa . W celu zachowania spójności z dyrektywą NIS pojęcie „sieci i systemów informatycznych" zastąpione zostało pojęciem „systemy informacyjne" zgodnie ze sposobem, w jakim to pojęcie zostało implementowane do polskiego porządku prawnego w 2018 roku. Pojęcie to zastąpiło więc pojęcie „cyberbezpieczeństwa" w przepisach, które były bezpośrednią implementacją przepisów dyrektywy NIS. Dzięki temu treść tych przepisów nie ulega w praktyce zmianie.
3.	Art. 2 pkt 4-9	4) certyfikat – europejski certyfikat cyberbezpieczeństwa lub krajowy certyfikat cyberbezpieczeństwa; 5) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		6) CSIRT MON – CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej; 7) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy; 8) CSIRT INT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Wywiadu na rzecz jednostek organizacyjnie podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych oraz Agencji Wywiadu; 9) CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;	Nowe definicje związane są z wprowadzeniem nowych elementów mających na celu usprawnienie działania krajowego systemu cyberbezpieczeństwa.
4.	Art. 2 ust. 1 pkt 15	15) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w art. 2 pkt 3–6 rozporządzenia 765/2008;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Nowe definicje związane są z wprowadzeniem nowych elementów mających na celu usprawnienie działania krajowego systemu cyberbezpieczeństwa.
5.	Art. 2 ust. 1 pkt 16	16) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;”,	Niniejsza zmiana jest wprost wynikiem zmiany definicji cyberbezpieczeństwa i w praktyce sprawia, że treść definicji incydentu nie ulega zmianie.
6.	Art. 2 ust. 1 pkt 22	22) ISAC – centrum wymiany i analizy informacji na temat podatności cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

			Nowe definicje związane są z wprowadzeniem nowych elementów mających na celu usprawnienie działania krajowego systemu cyberbezpieczeństwa.
7.	Art. 2 ust. 1 pkt 26 – 28	26) krajowa deklaracja zgodności – deklaracja zgodności wydana w ramach krajowego programu certyfikacji cyberbezpieczeństwa; 27) krajowy program certyfikacji cyberbezpieczeństwa – kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych przez Radę Ministrów i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT i procesów ICT; 28) krajowy poziom uzasadnienia zaufania – potwierdzenie, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi wskazanego poziomu bezpieczeństwa określonego w krajowym programie certyfikacji cyberbezpieczeństwa; .	Wprowadzone w punktach 26-86 definicje związane są z przepisami wprowadzającymi krajowe programy certyfikacji cyberbezpieczeństwa. Wiele kwestii związanych z deklaracjami zgodności i certyfikatami odnoszącymi się do europejskich programów certyfikacyjnych zostało rozwiązanych w bezpośrednio stosowanych przepisach aktu o cyberbezpieczeństwie. Celem jest, by przepisy dotyczące krajowe certyfikaty i deklaracje zgodności zawierały analogiczne rozwiązania. Krajowy poziom uzasadnienia zaufania został wprowadzony, gdyż definicja poziomu uzasadnienia zaufania z aktu o cyberbezpieczeństwie odnosi się tylko do europejskich programów certyfikacyjnych. W związku z tym, chcąc zastosować podobne rozwiązania co w europejskich programach certyfikacyjnych, wprowadzona została definicja krajowego poziomu uzasadnienia zaufania. Treściowo jest ona analogiczna do tej wprowadzonej w akcie o cyberbezpieczeństwie.
8.	Art. 2 ust. 1 pkt 31	31) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;”,	Niniejsza zmiana jest wprost wynikiem zmiany definicji cyberbezpieczeństwa i w praktyce sprawia, że treść definicji podatności nie ulega zmianie.
9.	Art. 2 ust. 1 pkt 38 i 39	38) SOC wewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa utworzony w ramach struktury operatora usługi kluczowej; 39) SOC zewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa świadczący usługi na rzecz operatora usługi kluczowej;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu

			cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Nowe definicje związane są z wprowadzeniem nowych elementów mających na celu usprawnienie działania krajowego systemu cyberbezpieczeństwa.
10.	Art. 3a	„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu: 1) identyfikacji źródła i analizy ruchu sieciowego powodującego wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usługi kluczowej, usługi cyfrowej lub realizację zadań publicznych, 2) czasowego ograniczenia ruchu sieciowego z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu.”;	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.
11.	art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 11 w ust. 3 we wprowadzeniu do wyliczenia, w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 14 ust. 3, w art. 15 w ust. 2 w pkt 3, w	6) użyte w art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 11 w ust. 3 we wprowadzeniu do wyliczenia, w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 14 ust. 3, w art. 15 w ust. 2 w pkt 3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5 dwukrotnie, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 48 w pkt 1, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa”, zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „CSIRT sektorowy”;	Pojęcie „sektorowy zespół cyberbezpieczeństwa” zostało zastąpione pojęciem „CSIRT sektorowy. Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.

	art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5 dwukrotnie, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 48 w pkt 1, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4		
12.	Art. 4	Art. 4 a) po pkt 2 dodaje się pkt 2a w brzmieniu: „2a) przedsiębiorców komunikacji elektronicznej;”, b) po pkt 5 dodaje się pkt 5a w brzmieniu: „5a) CSIRT Telco;”, c) po pkt 6 dodaje się pkt 6a i 6b w brzmieniu: „6a) CSIRT INT; 6b) ISAC, o którym mowa w art. 25a;”, d) w pkt 7 wyrazy „w art. 9 pkt 1–6, 8, 9, 11 i 12” zastępuje się wyrazami „w art. 9 pkt 1–6, 8–10”,	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres podmiotowy w celu wzmocnienia cyberbezpieczeństwa wskazanych podmiotów. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		e) po pkt 7 dodaje się pkt 7a w brzmieniu: „7a) Urząd Komisji Nadzoru Finansowego;”, f) pkt 8 otrzymuje brzmienie: „8) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r. poz. 574 i 583;”, g) po pkt 14 dodaje się pkt 14a i14b w brzmieniu: „14a) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2021 r. poz. 2233, 2368, oraz z 2022 r. poz. 88 i 258); 14b) Polski Fundusz Rozwoju oraz inne instytucje rozwoju, o których mowa w ustawie z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2021 r. poz. 1010, 2219 i 2349);”, h) pkt 16 otrzymuje brzmienie: „16) SOC zewnętrzne; i) po pkt 17 dodaje się punkt 17a w brzmieniu: „17a) Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE”;	
13.	Art. 7	w art. 7: a) po ust 3 dodaje się ust. 3a w brzmieniu: „3a. W przypadku podmiotów, dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, wpisanie do wykazu operatorów usług kluczowych albo zmiana danych tych podmiotów dokonuje się z urzędu.”, b) w ust. 4 wyrazy „nie później niż w terminie 6 miesięcy” zastępuje się wyrazami „niezwłocznie, nie później niż w terminie 1 miesiąca”, c) ust. 5 otrzymuje brzmienie: „5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejsza zmiana ma uporządkować kwestie związane z podpisywaniem wniosków o wpis o do wykazu operatorów usług kluczowych. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

14.	art. 8 pkt 3, pkt 5 lit. d, art. 9 ust. 1 pkt 2, art. 13 ust. 1 pkt 2, art. 22 ust. 1 pkt 4, art. 26 ust. 1, 3 pkt 1, 2, 4, 10, 14 lit. b i c i w ust. 6 pkt 2 , art. 33 ust. 4a, art. 35 ust. 4-5, art. 37 ust. 1, art. 39 ust. 1, 3 i 4 , art. 46 ust. 1 pkt 5, art. 51 pkt 2, 7 i 8, art. 52 pkt 2 i 4, art. 53 ust. 1 pkt 2 lit. a, art. 62 ust. 2 pkt 3, art. 65 ust. 1 pkt 1 i ust. 2, art. 73 ust. 5 pkt 1, art. 83	użyte w art. 8 w pkt 3, w pkt 5 w lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, w ust. 3 w pkt 1, 2, 4 i 10, w pkt 14 w lit. b i c i w ust. 6 w pkt 2 , w art. 33 w ust. 4a, w art. 35 w ust. 4 i 5, w art. 37 w ust. 1, w art. 39 w ust. 1, 3 i 4 , w art. 46 w ust. 1 w pkt 5, w art. 51 w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i 2, w art. 73 w ust. 5 w pkt 1, w art. 83, w różnej liczbie i różnym przypadku, wyrazy „ zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i przypadku wyrazem „ cyberzagrożenie”;	Pojęcie „zagrożenie cyberbezpieczeństwa” zostało zastąpione pojęciem cyberzagrożenia (art. 2 pkt 17). Definicja cyberzagrożenia została wprowadzona w akcie o cyberbezpieczeństwie i jest ona bardzo zbliżona do funkcjonującej w naszym systemie prawnym definicji „zagrożenia cyberbezpieczeństwa”. Nie jest zasadne utrzymywanie w systemie prawnym obu tych pojęć i dlatego pozostawiono jedynie sformułowanie „cyberzagrożenie”. Nowe pojęcie jest zgodne z najnowszą terminologią w dziedzinie cyberbezpieczeństwa stosowaną w państwach członkowskich Unii Europejskiej.

15.	Art. 8 pkt 5 lit. b	w art. 8 w pkt 5 lit. b otrzymuje brzmienie: „b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji,”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
16.	Art. 9 ust. 1 i 2	7) w art. 9: a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”, b) ust. 2 otrzymuje brzmienie: „2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego dane osób, o których mowa w ust. 1 pkt 1, zawierające imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych - w terminie 14 dni od dnia ich zmiany.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten doprecyzowuje kwestie związane ze zgłaszaniem osób kontaktowych do krajowego systemu cyberbezpieczeństwa.
17.	Art. 9	w art. 9: a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”, b) ust. 2 otrzymuje brzmienie: „2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa dane osób, o których mowa w ust. 1 pkt 1, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych – w terminie 14 dni od dnia ich zmiany. Organ właściwy do spraw cyberbezpieczeństwa przekazuje te dane do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten doprecyzowuje kwestie związane ze zgłaszaniem osób kontaktowych do krajowego systemu cyberbezpieczeństwa.
18.	Art. 10	12) w art. 10: a) w ust. 1, ust. 2 we wprowadzeniu do wyliczenia oraz w ust. 3 i 4 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”, b) w ust. 2 pkt 2 otrzymuje brzmienie:	Niniejsza zmiana jest związana z wprowadzaniem w akcie o cyberbezpieczeństwie definicji cyberbezpieczeństwa. W związku z tym, iż automatycznie zastąpiła ona dotychczas funkcjonującą krajową definicję cyberbezpieczeństwa. W związku z tym konieczne

		„2) ochronę dokumentów przed przypadkowym uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”, c) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazami „bezpieczeństwa systemów informacyjnych”;	było dostosowanie przepisów posługujących się tym pojęciem. Tam gdzie konieczne było zachowanie wcześniejszego rozumienia cyberbezpieczeństwa słowo to zostało zastąpione sformułowaniem „bezpieczeństwo systemów informacyjnych”.
19.	Art. 11	w art. 11: a) w ust. 1 w pkt 4 wyrazy „ CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”; b) w ust. 2 po wyrazach „przekazywane jest w postaci elektronicznej” dodaje się wyrazy „za pomocą systemu, o którym mowa w art. 46 ust. 1”; c) w ust. 3: – pkt 1 i 2 otrzymują brzmienie: „1) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, koordynowanej przez CSIRT GOV, CSIRT MON lub CSIRT NASK, przekazując niezbędne dane, w tym dane osobowe; 2) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach.”; – uchyla się pkt 3; d) po ust. 3 dodaje się ust. 3a – 3b w brzmieniu: „3a. W przypadku gdy: 1) operator usługi kluczowej jest przedsiębiorcą komunikacji elektronicznej oraz 2) zgłasza incydent poważny, będący również poważnym incydentem telekomunikacyjnym zgłoszenie jest przekazywane tylko do CSIRT sektorowego. Zgłoszenie zawiera elementy wskazane w art. 12 i art. 20e. 3b. Operator usługi kluczowej współdziała również z CSIRT Telco w sytuacji, o której mowa w ust. 3a.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten doprecyzowuje kwestie związane z działaniem CSIRT-ów sektorowych wobec operatorów usług kluczowych.
20.	Art. 13	w art. 13: a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”; b) uchyla się ust. 3;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu

		c) dodaje się ust. 5 w brzmieniu: „5. W uzasadnionym przypadku, CSIRT sektorowy przekazuje do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK informacje o których mowa w ust. 1, niezwłocznie po stwierdzeniu zasadności przekazania danej informacji, nie później jednak niż w ciągu 8 godzin od takiego stwierdzenia. ”;	cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
21.	Art. 14	art. 14 otrzymuje brzmienie: „Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13 w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach. 2. Operator usługi kluczowej powołuje SOC wewnętrzny lub zawiera umowę o prowadzenie SOC zewnętrznego, zwaną dalej „umową o świadczenie usług SOC”. 3. Organ tworzący lub nadzorujący operatora usługi kluczowej może utworzyć na rzecz tego operatora SOC zewnętrzny. 4. SOC wewnętrzny może realizować zadania, o których mowa w ust. 1, także na rzecz innych podmiotów. 5. SOC wewnętrzny lub SOC zewnętrzny, na podstawie przeprowadzonego szacowania ryzyka, prowadzi działania zapewniające cyberbezpieczeństwo, w szczególności wprowadza zabezpieczenia, zapewniające poufność integralność, dostępność i autentyczność przetwarzanych danych, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów, a także eksploatacji i architektury systemów, w celu: 1) monitorowania i wykrywania incydentów; 2) reagowania na incydenty; 3) zapobiegania incydentom; 4) zarządzania jakością zabezpieczeń systemów, informacji i aktywów; 5) aktualizowania analizy ryzyka w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na działania, o których mowa w pkt 1–3. 6. Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o sposobie realizacji obowiązku, o którym mowa w ust. 2, polegającego na powołaniu SOC wewnętrzny lub zawarciu umowy o świadczenie usług SOC, albo realizowaniu zadania poprzez SOC zewnętrzny	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie operacyjnych centrów bezpieczeństwa, zwane dalej: ,,SOC”. Pojęcie to zastąpi struktury odpowiedzialne za cyberbezpieczeństwo u operatorów usług kluczowych. SOC posiadają ugruntowaną na rynku pozycję struktur realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek. Operatorzy usług kluczowych będą dysponowały strukturami SOC wewnątrz organizacji lub zawierali umowę z zewnętrznym podmiotem świadczącym usługi SOC. SOC m.in. będzie prowadził szacowanie ryzyka, wykrywał oraz reagował na incydenty. Minister właściwy do spraw informatyzacji będzie prowadził wykaz operacyjnych centrów bezpieczeństwa. Dotychczasowe wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo oraz podmioty zewnętrze, świadczące usługi cyberbezpieczeństwa dla

		utworzony na jego rzecz przez organ tworzący lub nadzorujący, lub o zmianie sposobu realizacji tego obowiązku. 7. W przypadku zawarcia umowy o prowadzenie SOC operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o: 1) zawarciu takiej umowy oraz dacie jej zawarcia, 2) danych kontaktowych, o których mowa w ust. 10 pkt 4, podmiotu, z którym zawarta została umowa, 3) zakresie świadczonej usługi, 4) terminie obowiązywania umowy, 5) rozwiązaniu umowy – w terminie 14 dni od dnia zawarcia lub rozwiązania umowy. 8. W przypadku, gdy jest to niezbędne dla zapewnienia bezpieczeństwa systemów informacyjnych, podmiot prowadzący SOC zapewnia bezpieczny i zdalny dostęp do swoich systemów obsługiwanemu operatorowi usługi kluczowej przez co najmniej: 1) ustalenie zasad dostępu do systemu; 2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację; 3) minimalizację zakresu danych przechowywanych poza bezpiecznym środowiskiem. 9.Przy zawieraniu umowy o prowadzenie SOC zawiera się zastrzeżenie, że świadczenie tych usług podlega prawu polskiemu. 10. SOC zewnętrzny, udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności: 1) nazwa SOC zewnętrznego; 2) zakres obszaru działania, w tym: a) oferowany rodzaj wsparcia, b) zasady współpracy i wymiany informacji, c) politykę komunikacji i uwierzytelniania informacji; 3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów; 4) dane kontaktowe, w tym: a) adres ze wskazaniem strefy czasowej,	operatorów usług kluczowych, staną się automatycznie SOC w rozumieniu ustawy o KSC.

		b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC, c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC zewnętrznym, d) sposoby kontaktu z SOC zewnętrznym, w tym sposób zgłaszania incydentów SOC.	
22.	Art. 14a	po art. 14 dodaje się art. 14a w brzmieniu: „14a. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz SOC wewnętrznych i SOC zewnętrznych, zwany dalej wykazem SOC. 2. Wykaz SOC zawiera: 1) nazwę (firmę) podmiotu prowadzącego SOC wewnętrzny lub SOC zewnętrzny; 2) nazwę (firmę) podmiotów, na rzecz których SOC wewnętrzny lub SOC zewnętrzny jest prowadzony; 3) siedzibę i adres SOC wewnętrzny lub SOC zewnętrzny; 4) numer identyfikacji podatkowej (NIP), jeżeli został nadany; 5) numer we właściwym rejestrze, jeżeli został nadany; 6) datę wpisania do wykazu SOC; 7) datę wykreślenia z wykazu SOC. 3. Wpisanie do wykazu SOC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie, nie później niż w terminie 14 dni, po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1–5. 4. W przypadku podmiotów dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji wpisanie do wykazu SOC dokonuje się z urzędu po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6. 5. Zmiana danych w wykazie SOC następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Ust. 4 stosuje się odpowiednio.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. To kolejny przepis związany z powoływaniem struktur SOC.

		6. Wnioski, o których mowa w ust. 3 i 5, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. 7. Wpisanie do wykazu SOC i wykreślenie z tego wykazu oraz zmiana danych w wykazie SOC są czynnościami materialno–technicznymi. 8. Minister właściwy do spraw informatyzacji może, z urzędu, wpisać do wykazu, o którym mowa w ust. 1, inny podmiot niż SOC wewnętrzny lub SOC zewnętrzny, jeżeli co najmniej: 1) świadczy usługi z zakresu cyberbezpieczeństwa, w szczególności związane z: a) monitorowaniem, wykrywaniem, reagowaniem i zapobieganiem incydentów, b) zarządzaniem jakością zabezpieczeń systemów, informacji i powierzonych aktywów, c) aktualizowaniem ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent; 2) przedstawi dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742), 3) zawrze z ministrem właściwym do spraw informatyzacji porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46 ust. 1. 9. Minister właściwy do spraw informatyzacji wykreśla z wykazu wpisany z urzędu podmiot, który przestał spełniać warunki, o których mowa w ust. 8. 10. Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia CSIRT GOV, CSIRT MON, CSIRT NASK i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym. 11. Minister właściwy do spraw informatyzacji udostępnia dane z wykazu SOC, na wniosek, następującym podmiotom: 1) organowi właściwemu do spraw cyberbezpieczeństwa, 2) Policji,	

		3) Żandarmerii Wojskowej, 4) Straży Granicznej, 5) Centralnemu Biuru Antykorupcyjnemu, 6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, 7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, 8) sądom, 9) prokuraturze, 10) organom Krajowej Administracji Skarbowej, 11) dyrektorowi Rządowego Centrum Bezpieczeństwa, 12) Służbie Ochrony Państwa – w zakresie niezbędnym do realizacji ich ustawowych zadań.”;	
23.	Art. 17 ust. 2, art. 69 ust. 1 i 2	17) użyty w art. 17 w ust. 2, art. 69 w ust. 1, w ust. 2 w pkt 1, 6 i 7, w różnej liczbie i przypadku, wyraz „cyberbezpieczeństwo” zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „bezpieczeństwo systemów informacyjnych”; 18) w art. 17 w ust. 2 pkt 1 skreśla się wyrazy „systemów informacyjnych i”;	Niniejsza zmiana jest związana z wprowadzaniem w akcie o cyberbezpieczeństwie definicji cyberbezpieczeństwa. W związku z tym, iż automatycznie zastąpiła ona dotychczas funkcjonującą krajową definicję cyberbezpieczeństwa. W związku z tym konieczne było dostosowanie przepisów posługujących się tym pojęciem. Tam gdzie konieczne było zachowanie wcześniejszego rozumienia cyberbezpieczeństwa słowo to zostało zastąpione sformułowaniem „bezpieczeństwo systemów informacyjnych”.
24.	Art. 21	w art. 21 a) w ust. 1 wyrazy „osoby odpowiedzialnej” zastępuje się wyrazami „dwóch osób odpowiedzialnych”, b) w ust. 2 i 3 wyrazy „jedną osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa.

25.	Art. 22	w art. 22: a) po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zgłaszają incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT INT."; b) w ust. 2 po wyrazach „w ust. 1 pkt 2" dodaje się wyrazy „oraz ust. 1a"; c) dodaje się ust. 3–7 w brzmieniu: „3. Niezależnie od zadań, określonych w ust. 1, Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, przekazuje jednocześnie CSIRT INT w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, zgłoszenie, o którym mowa w ust. 1 pkt 4; 4. Jednostki, o których mowa w ust. 3: 1) współdziałają z CSIRT INT podczas obsługi incydentu w podmiocie publicznym, przekazując niezbędne dane, w tym dane osobowe; 2) zapewniają CSIRT INT dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań; 3) przekazują do CSIRT INT dane osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa.

		5. CSIRT INT niezwłocznie przekazuje informacje, o których mowa w ust. 6, do CSIRT GOV.”;	
26.	Art. 23 i 24	w art. 23 w ust. 3 i 4 oraz w art. 24 w zdaniu pierwszym wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa.
27.	Art. 25a	„Rozdział 5a Zadania i obowiązki ISAC w ramach krajowego systemu cyberbezpieczeństwa Art. 25a 1. ISAC oraz minister właściwy do spraw informatyzacji mogą zawrzeć porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46, jeżeli ISAC w szczególności: 1) wspiera podmioty krajowego systemu cyberbezpieczeństwa w: a) rozpoznawaniu cyberzagrożeń i obsługi incydentów, b) podnoszeniu świadomości cyfrowej, 2) gromadzi i analizuje informacje o podatnościach, cyberzagrożeniach i incydentach oraz zapewnia podmiotom krajowego systemy cyberbezpieczeństwa dostęp do tych informacji i wyników analiz 2. Jeżeli ISAC jest jednostką organizacyjną nieposiadającą osobowości prawnej, strony tworzące ISAC wyznaczają przedstawiciela w celu zawarcia porozumienia, o którym mowa w ust. 1. 3. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC, które zawarły porozumienie, o którym mowa w ust. 1, zwany dalej „wykazem ISAC”. 4. Wykaz ISAC zawiera: 1) nazwę ISAC; 2) imię i nazwisko osoby reprezentującej ISAC wraz z numerem telefonu oraz adresem poczty elektronicznej;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. ISAC (centrum wymiany i analiz informacji), tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o cyberzagrożeniach i podatnościach oraz wymiana informacji o najlepszych praktykach.

		3) siedzibę i adres ISAC, jeżeli posiada; 4) numer identyfikacji podatkowej (NIP), jeżeli został nadany; 5) numer we właściwym rejestrze, jeżeli został nadany; 6) adres poczty elektronicznej ISAC; 7) adres strony internetowej ISAC, jeżeli posiada; 8) adres do doręczeń elektronicznych ISAC, jeżeli posiada; 9) datę zawarcia porozumienia; 10) datę wpisania do wykazu ISAC; 11) datę wykreślenia z wykazu ISAC. 5. Wpisanie do wykazu ISAC następuje niezwłocznie, najpóźniej w ciągu 7 dni od zawarcia porozumienia, o którym mowa w ust. 1. 6. Wykreślenie ISAC z wykazu ISAC następuje w przypadku: 1)rozwiązania porozumienia, o którym mowa w ust. 1, 2) rozwiązania ISAC. 7. Zmiana danych w wykazie ISAC następuje na wniosek podmiotu prowadzącego ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu. Wniosek sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. 8. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno–technicznymi. 9. Wykaz ISAC jest publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. W publikowanym wykazie nie umieszcza się informacji wskazanych w ust. 4 pkt 2. 10. ISAC wpisany do wykazu ISAC współpracuje z CSIRT GOV, CSIRT MON lub CSIRT NASK, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów. 11. ISAC wpisany do wykazu ISAC przedkłada ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.	

		12. Minister właściwy do spraw informatyzacji, na wniosek organu właściwego albo z urzędu, może przeprowadzić kontrolę: 1) zgodności z prawem działania ISAC wpisanego do wykazu ISAC; 2) przestrzegania przez ISAC wpisany do wykazu ISAC, zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa. 13. Do kontroli, o której mowa w ust. 12, przepis art. 54 ust. 2 stosuje się odpowiednio. 14. W razie stwierdzenia, że działalność ISAC wpisanego do wykazu ISAC jest niezgodna z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa, minister właściwy do spraw informatyzacji, w zależności od rodzaju i stopnia stwierdzonych nieprawidłowości, może: 1) wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości w określonym terminie lub 2) wypowiedzieć porozumienie, o którym mowa w ust. 1.”;	
28.	Art. 26	w art. 26: a) ust. 2 otrzymuje brzmienie: „2. CSIRT GOV, CSIRT MON i CSIRT NASK w uzasadnionych przypadkach na wniosek podmiotów krajowego systemu cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów i incydentów telekomunikacyjnych.”, b) po ust. 2 dodaje się ust. 2a i 2b w brzmieniu: „2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów i incydentów telekomunikacyjnych, o których mowa w ust. 2: a) CSIRT NASK za zgodą ministra właściwego do spraw informatyzacji, b) CSIRT GOV za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego, lub c) CSIRT MON za zgodą Ministra Obrony Narodowej.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana jest związana z usprawnieniami w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. Wskazane tu zostały nowe zadania wykonywane przez zespoły reagowania na incydenty komputerowe.

		2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków porozumiewania się na odległość.”, c) w ust. 3: – w pkt 1 po wyrazie „incydentów” dodaje się wyrazy: „i incydentów telekomunikacyjnych”, – w pkt 2 po wyrazie „incydentami” dodaje się wyrazy: „i incydentami telekomunikacyjnymi”, – w pkt 3 wyrazy „incydentów i ryzyk” zastępuje się wyrazami „incydentów, incydentów telekomunikacyjnych i ryzyk”, – pkt 5 otrzymuje brzmienie: „5) reagowanie oraz koordynacja reagowania na zgłoszone incydenty i incydenty telekomunikacyjne;”, – w pkt 6 wyrazy „w tym incydentów poważnych oraz incydentów istotnych” zastępuje się wyrazami „w tym incydentów poważnych, incydentów istotnych oraz incydentów telekomunikacyjnych”, – w pkt 10 po wyrazie „oraz” dodaje się wyrazy „z CSIRT INT”, – w pkt 12 wyrazy „30 maja” zastępuje się wyrazami „31 stycznia”, – pkt 16 otrzymuje brzmienie: „16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz ENISA;”, – w pkt 16 kropkę zastępuje się średnikiem i dodaje się pkt 17–22 w brzmieniu: „17) gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych; 18) przygotowywanie na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych; 19) przygotowywanie na zlecenie Pełnomocnika analiz skutków incydentów i incydentów telekomunikacyjnych oraz przebiegu obsługi incydentów i incydentów telekomunikacyjnych;	

		20) przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa; 21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, poprzez: a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi do spraw cyberbezpieczeństwa i podmiotem krajowego systemu cyberbezpieczeństwa, u którego wykonywany jest test, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach; 22) udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRT GOV, CSIRT MON lub CSIRT NASK, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.”, d) ust. 4 otrzymuje brzmienie: „4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu lub incydentu telekomunikacyjnego, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określą we współpracy z CSIRT sektorowymi, CSIRT Telco i CSIRT INT sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu lub incydentu telekomunikacyjnego.”, e) w ust. 5 wprowadzenie do wyliczenia otrzymuje brzmienie: „Do zadań CSIRT MON należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”, f) w ust. 6: – w pkt 1: – – lit. a otrzymuje brzmienie: „a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6 i 10 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”, – – lit. c otrzymuje brzmienie: „c) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce,”, – po pkt 1 dodaje się pkt 1a w brzmieniu:	

		„1a) koordynacja obsługi incydentów telekomunikacyjnych zgłaszanych przez przedsiębiorców komunikacji elektronicznej, z wyjątkiem incydentów telekomunikacyjnych zgłaszanych przez podmioty wskazane w ust. 5 i 7, g) w ust. 7 - wprowadzenie do wyliczenia otrzymuje brzmienie: „Do zadań CSIRT GOV należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:"; - po pkt 4 dodaje się pkt 4a– 4c w brzmieniu: „4a) Państwowe Gospodarstwo Wodne Wody Polskie; 4b) Polski Fundusz Rozwoju i inne instytucje rozwoju; 4c) Urząd Komisji Nadzoru Finansowego;", h) w ust. 8 wyrazy „zgłoszenie incydentu" zastępuje się wyrazami „zgłoszenie incydentu lub incydentu telekomunikacyjnego" i) ust. 9 otrzymuje brzmienie: „9. Działalność bieżąca CSIRT NASK jest finansowana w formie dotacji podmiotowej ze środków, których dysponentem jest minister właściwy do spraw informatyzacji.", j) po ust. 9 dodaje się ust. 9a i 9b w brzmieniu: 9a. Rozbudowa i modernizacja infrastruktury teleinformatycznej CSIRT NASK służącej realizacji jego zadań może być dofinansowana w formie dotacji celowej ze środków budżetu państwa, których dysponentem jest minister właściwy do spraw informatyzacji.", k) w ust. 11 wyrazy „Ministra Cyfryzacji" zastępuje się wyrazami „ministra właściwego do spraw informatyzacji", l) dodaje się ust. 12 w brzmieniu: „12. Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy do spraw informatyzacji informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w ust. 10. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej."; 	

29.	Art. 26 i art. 49	użyte w art. 26 w ust. 3 w pkt 16 oraz w art. 49 w ust. 3 w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)" zastępuje się wyrazem „ ENISA";	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Drobna zmiana redakcyjna związana ze zdefiniowaniem ENISY.
30.	Art. 31	w art. 31: a) po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w 20d ust. 1 pkt 2, a także uzgodnią sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji – w przypadku braku możliwości dokonania zgłoszenia albo przekazania tych informacji w postaci elektronicznej." b) ust. 2 otrzymuje brzmienie: 2. Komunikat zawierający informacje, o których mowa w ust. 1 – 1a, CSIRT MON, CSIRT NASK i CSIRT GOV publikuje na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego. Komunikat podlega również publikacji w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejszy przepis nie implementuje wprost dyrektywy ustanawiającej Europejski Kodeks Łączności Elektronicznej.
31.	Art. 32 ust. 4	art. 32 ust. 4 otrzymuje brzmienie: „4. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy lub CSIRT Telco na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotów krajowego systemu cyberbezpieczeństwa mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.";	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

			Przepis stanowi podstawę dla wymiany informacji między CSIRT-ami poziomu krajowego a CSIRT-ami sektorowymi oraz CSIRT TELCO
32.	Art. 33 ust. 1a – 1d	w art. 33: a) dodaje się ust. 1a–1d w brzmieniu: „1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT. 1b. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, jest uprawniony do stosowania technik mających na celu: obserwację i analizę pracy, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez urządzenie informatyczne lub oprogramowanie. 1c. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, badanych urządzeń i oprogramowania, które ograniczyłyby możliwość przeprowadzenia badania. 1d. Badanie, o którym mowa w ust. 1: a) nie narusza autorskich praw osobistych oraz majątkowych, oraz b) nie wymaga zgody licencjodawcy lub dysponenta urządzenia informatycznego, oprogramowania lub usługi cyfrowej. 1e. Postanowienia umów sprzeczne z art. 33 ust. 1–1d są nieważne.”; b) ust. 2 otrzymuje brzmienie: 2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie urządzenia informatycznego lub oprogramowania, informuje pozostałe zespoły CSIRT poziomu krajowego o fakcie podjęcia badań oraz urządzeniu informatycznym lub oprogramowaniu, którego badanie dotyczy.”. c) po ust. 4b dodaje się ust. 4c w brzmieniu:	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten rozszerza uprawnienia przewodniczącego Kolegium i Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, dając im większą swobodę działania.

		„4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik publikuje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.”;	
33.	Art. 34 ust. 1	w art. 34 ust. 1 otrzymuje brzmienie: „1. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco oraz SOC zewnętrzne współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Określone w nim zostały zasady współpracy między organami krajowego systemu cyberbezpieczeństwa a organami ścigania.
34.	Art. 34a	30) po art. 34 dodaje się art. 34a i 34b w brzmieniu: „Art. 34a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco przekazują informacje o incydentach telekomunikacyjnych Prezesowi UKE w celu realizacji obowiązków, o których mowa w art. 20h ust. 1 pkt 1. 2. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco raz na pół roku przygotowują sprawozdania dotyczące liczby i rodzajów poważnych incydentów telekomunikacyjnych Prezesowi UKE oraz Pełnomocnikowi. 3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają z Prezesem UKE sposób i tryb przekazywania informacji, o których mowa w ust. 1 Art. 34b. CSIRT GOV, CSIRT MON i CSIRT NASK współpracują z Prezesem UKE oraz CSIRT Telco przy wykonywaniu ustawowych zadań.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis stanowi podstawę dla wymiany informacji między CSIRT-ami poziomu krajowego a CSIRT-ami sektorowymi oraz CSIRT TELCO
35.	Art. 35	w art. 35 ust. 5 otrzymuje brzmienie: "5.CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać Pełnomocnikowi do publikacji na stronie podmiotowej Pełnomocnika w Biuletynie Informacji Publicznej informacje o podatnościach, incydentach krytycznych oraz o cyberzagrożeniach: 1) jeżeli przekazywanie tych informacji przyczyni się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów, 2) wyłącznie w zakresie niezbędnym do realizacji tych celów, oraz 3) jeżeli publikacja informacji nie będzie naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.";	
36.	Art. 36	Art. 36 ust. 2 otrzymuje brzmienie: „2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Pełnomocnika, ministra właściwego do spraw informatyzacji oraz Rządowego Centrum Bezpieczeństwa.”, b) po ust. 2 dodaje się ust. 2a w brzmieniu: “2a. W posiedzeniach Zespołu może uczestniczyć Pełnomocnik.” c) w ust. 6 zdanie pierwsze otrzymuje brzmienie: „Dyrektor Rządowego Centrum Bezpieczeństwa na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1, zawiadamia niezwłocznie członków Zespołu i Pełnomocnika o terminie i miejscu posiedzenia Zespołu.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten reguluje kwestie związane z udziałem Rządowego Centrum Bezpieczeństwa w sprawach krajowego systemu cyberbezpieczeństwa.
37.	Art. 36a	Art. 36a. W wypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.
38.	Art. 36b-36g	Art. 36b. 1. Do zadań CSIRT INT należy zapewnianie wsparcia w obsłudze incydentów zgłaszanych przez: 1) jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 2) Agencję Wywiadu. 2. W zakresie określonym w ust. 1 CSIRT INT współpracuje z CSIRT GOV. 3. Do zadań CSIRT INT w ramach wspierania podmiotów określonych w ust. 1 należy: 1) przyjmowanie zgłoszeń o incydentach w podmiotach publicznych; 2) reagowanie na incydenty w podmiotach publicznych; 3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo w podmiotach publicznych; 4) współpraca z podmiotami publicznymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych; 5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty w podmiotach publicznych oraz wymiany informacji o cyberzagrożeniach; 6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie podnoszenia świadomości o cyberzagrożeniach; 7) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych, podmiotów o których mowa w ust. 1 , w szczególności przez: a) wykonywanie testów bezpieczeństwa w porozumieniu z podmiotami, o których mowa w ust. 1, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach. Art. 36c. CSIRT INT niezwłocznie, nie później niż w ciągu 8 godzin, przekazuje zgłoszenie, o którym mowa w art. 22 ust. 1a , do CSIRT GOV.	

		Rozdział 6b Ocena bezpieczeństwa Art. 36d 1. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy albo CSIRT Telco mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. 2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu. 3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych: 1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. 2020 r. poz. 27 i 2320, z 2021 r. poz. 2333, z 2022 r. poz. 22); 2) akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 oraz z 2022 r. poz. 655). 4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest: a) w przypadku podmiotów określonych w art. 26 ust. 5 – CSIRT MON; b) w przypadku podmiotów określonych w art. 26 ust. 6 pkt 1 lit. a – k i pkt 1a – CSIRT NASK; c) w przypadku podmiotów określonych w art. 26 ust. 7 pkt 1 – 4 – CSIRT GOV. 5. CSIRT GOV, CSIRT MON albo CSIRT NASK przeprowadza ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej w uzgodnieniu z organem właściwym do spraw cyberbezpieczeństwa. 6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej za zgodą organu właściwego do	

		spraw cyberbezpieczeństwa dla danego sektora oraz właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK. 7. CSIRT INT może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu, o którym mowa w art. 36b ust. 1, za zgodą CSIRT GOV. 8. CSIRT Telco może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego przedsiębiorcy komunikacji elektronicznej za zgodą właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK oraz Prezesa UKE. Art. 36e 1. Ocena bezpieczeństwa może być przeprowadzona za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w formie pisemnej lub elektronicznej pod rygorem nieważności. 2. Ocena bezpieczeństwa powinna być prowadzona z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie. 3. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe albo CSIRT Telco uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa. 4. CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b Kodeksu karnego, oraz ich używać w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a Kodeksu karnego. 5. Używając urządzeń lub programów komputerowych, o których mowa w ust. 4, CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może uzyskać dostęp do informacji dla niej nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub	

		inne szczególne jej zabezpieczenie, lub może uzyskać dostęp do całości lub części systemu informatycznego. 6. Informacje uzyskane przez CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe albo CSIRT Telco w wyniku przeprowadzania oceny bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe i CSIRT Telco oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. 7. Po przeprowadzeniu oceny bezpieczeństwa CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowe albo CSIRT Telco sporządza i przekazuje podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Art. 36f. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy albo CSIRT Telco informuje niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych. Art. 36g. Rada Ministrów może określić, w drodze rozporządzenia sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36e ust. 6, a także może określić wzory niezbędnych druków, mając na uwadze rodzaj materiałów podlegających zniszczeniu.”;	
39.	Art. 37	w art. 37: a) ust. 1 otrzymuje brzmienie: „1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2020 r. poz. 2176 oraz z 2021 r. poz. 1598 i 1641) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641).”,	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.

		b) ust. 2 i 3 otrzymują brzmienie: „2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent operatorem usługi kluczowej, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu. 3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, informacje o incydentach istotnych lub wystąpić do organu właściwego do spraw cyberbezpieczeństwa dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu, albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.”;	
40.	Art. 39	w art. 39: a) w ust. 1 wyrazy „ CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy i CSIRT Telco przetwarzają dane pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami”; b) użyte w ust. 2 oraz ust. 5–9, w różnej liczbie wyrazy „i sektorowe zespoły cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie wyrazami „CSIRT sektorowy i CSIRT Telco”, c) w ust. 3: – wprowadzenie do wyliczenia otrzymuje brzmienie: “CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe i CSIRT Telco przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami”, – pkt 2 otrzymuje brzmienie:	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsze zmiany związane są z objęciem sektora telekomunikacji ustawą o krajowym systemie cyberbezpieczeństwa.

		„2) dotyczące telekomunikacyjnych urządzeń końcowych”; – po pkt 4 dodaje się pkt 5 w brzmieniu: “5) gromadzone przez przedsiębiorców komunikacji elektronicznej w związku ze świadczeniem usług komunikacji elektronicznej”, d) w ust. 4: – wprowadzenie do wyliczenia otrzymuje brzmienie: “W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes UKE przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami:” – w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu: „4) gromadzone przez przedsiębiorców komunikacji elektronicznej.”; e) ust. 5 i 6 otrzymują brzmienie 5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8, art.. 36b – 36c, art. 44 ust. 1–3 oraz art. 44a ust. 3 –5. 6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8, art. 44 ust. 1–3 oraz art. 44a ust. 3 –5, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco w terminie 5 lat od zakończenia obsługi incydentu lub incydentu telekomunikacyjnego, którego dotyczą. f) w ust. 7 po wyrazach „CSIRT GOV” dodaje się wyrazy „,CSIRT INT, CSIRT Telco”; g) w ust. 8 i 9 po wyrazach „CSIRT MON, CSIRT NASK” dodaje się wyrazy „CSIRT Telco”; h) po ust. 9 dodaje się ust. 10 w brzmieniu: „10. Dane, o których mowa w ust. 4, są usuwane lub anonimizowane przez ministra właściwy do spraw informatyzacji, dyrektora Rządowego	

		Centrum Bezpieczeństwa, Pełnomocnika, organy właściwe do spraw cyberbezpieczeństwa oraz Prezesa UKE niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z niniejszej ustawy.”;	
41.	Art. 40	w art. 40: a) w ust. 1 wyrazy „CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy, CSIRT Telco”, b) w ust. 2– 3 wyrazy „CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Zmiana wynika z przyjęcia nowego nazewnictwa w tej dziedzinie.
42.	Art. 42 ust. 8	w art. 42: a) w ust. 1: – pkt 4 otrzymuje brzmienie: „4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych bezzwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych;”, – w pkt 5 po wyrazach „CSIRT MON” dodaje się wyrazy „i CSIRT INT”, – w pkt 7 wyraz „lub” zastępuje się przecinkiem, a po wyrazie „CSIRT MON” dodaje się wyrazy ”lub CSIRT INT”, b) w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się skrótem „ENISA”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Zmiana wynika z wprowadzenia wcześniej skrótu „ENISA”.
43.	Art. 44	w art. 44: a) ust. 1 otrzymuje brzmienie: „1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 do ustawy, do którego zadań należy: 1) przyjmowanie zgłoszeń o incydentach; 2) reagowanie na incydenty;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Zmiany te wynikają z nowej roli CSIRT-ów sektorowych.

		3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych; 4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych; 5) współpraca z CSIRT GOV, CSIRT MON i CSIRT NASK w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; 6) współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach; 7) współpraca z CSIRT Telco w reagowaniu na incydenty poważne, będącymi również poważnymi incydentami telekomunikacyjnymi.”, b) po ust. 1 dodaje się ust. 1a–1c w brzmieniu: 1a. CSIRT sektorowy niezwłocznie, nie później niż 8 godzin od jego otrzymania, przekazuje zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4 do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK. 1b. CSIRT sektorowy może, w szczególności: 1) zapewniać we współpracy z CSIRT GOV, CSIRT MON i CSIRT NASK dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń wśród operatorów usług kluczowych danego sektora lub podsektora; 2) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które ich dotyczą; 3) wspierać, w uzgodnieniu z operatorem usługi kluczowej, wykonywanie przez niego obowiązków określonych w art. 11 ust. 1–3, art. 12 i art. 13; 4) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu	Nazwa sektorowego zespołu cyberbezpieczeństwa została zmieniona na CSIRT sektorowy. W przeciwieństwie do dotychczasowego, fakultatywnego trybu ustanawiania zespołu, w projekcie przewidziano obowiązek ustanowienia CSIRT sektorowego dla danego sektora lub podsektora przez organ właściwy. CSIRT sektorowy będzie odpowiadał za przyjmowanie zgłoszeń o incydentach w sektorze lub podsektorze, dla którego został ustanowiony, a także za reagowanie na zgłoszone incydenty. Zakres obowiązków zostanie więc poszerzony - obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi kluczowej w reagowaniu na incydenty. CSIRT sektorowy będzie również dokonywał dynamicznej analizy ryzyka i incydentów jak również gromadził informacje o cyberzagrożeniach.

		poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRT GOV, CSIRT MON albo CSIRT NASK5) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w danym sektorze, w szczególności przez: a) wykonywanie testów bezpieczeństwa w porozumieniu z organami właściwymi do spraw cyberbezpieczeństwa i operatorami usług kluczowych, b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach. 1c. Realizacja zadań, o których mowa w ust. 1b pkt 5, odbywa się w uzgodnieniu z właściwym CSIRT GOV, CSIRT MON i CSIRT NASK.”, c) uchyla się ust. 2, d) ust. 4 otrzymuje brzmienie: „4. Organ właściwy do spraw cyberbezpieczeństwa informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań.”, e) dodaje się ust. 5–13 w brzmieniu: „5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadań CSIRT sektorowego jednostkom jemu podległym albo przez niego nadzorowanym albo organowi przez niego nadzorowanemu. 6. Organ właściwy do spraw cyberbezpieczeństwa może, w drodze porozumienia, wyznaczyć spośród jednostek jemu podległych albo przez niego nadzorowanych jednostkę, która będzie wykonywała zadania CSIRT sektorowego dla kilku sektorów. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu zasady sprawowania nadzoru nad CSIRT sektorowym. 7. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT GOV, CSIRT MON albo CSIRT NASK realizację zadań CSIRT sektorowego. 8. Powierzenie, o którym mowa w ust. 7 następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa:	

		1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytutem Badawczym; 2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego; 3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej. 9. W porozumieniu, o którym mowa w ust. 8, określa się zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań oraz zasady ich finansowania. 10. Komunikat o zawarciu porozumienia, o którym mowa w ust. 6 i 8, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. W komunikacie wskazuje się informacje o: 1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami; 2) terminie, od którego porozumienie będzie obowiązywało. 11. Organ właściwy do spraw cyberbezpieczeństwa, informuje Pełnomocnika, o zawarciu porozumienia, o którym mowa w ust. 6 i 8. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.	
44.	Art. 44b	Art. 44b 1. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego. W sprawozdaniu za rok, w którym utworzony został CSIRT sektorowy, zawiera się informacje dotyczące jego utworzenia oraz funkcjonowania. . 2. Prezes UKE raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT Telco. W sprawozdaniu za rok, w którym utworzony	W zakresie w jakim przepis ten dotyczy CSIRT sektorowych, nie stanowi on implementacji przepisów europejskich.

		został CSIRT Telco, zawiera się informacje dotyczące jego utworzenia oraz funkcjonowania.”;	
45.	Art. 45 ust. 1 pkt 7 i 8	w art. 45 w ust. 1 w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 i 8 w brzmieniu: „7) wydawanie poleceń zabezpieczających; 8) prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
46.	Art. 46	w art. 46: a) ust. 2 otrzymuje brzmienie: „2. Pełnomocnik, CSIRT GOV, CSIRT MON, CSIRT NASK korzystają z systemu teleinformatycznego, o którym mowa w ust. 1.”, b) po ust. 2 dodaje się ust. 2a – 2d w brzmieniu: „2a. CSIRT sektorowe, CSIRT INT, CSIRT Telco, Prezes UKE korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości. 2b. Operatorzy usług kluczowych korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie niezbędnym do realizowania obowiązków, o których mowa w rozdziale 3. 2c. Szczegółowe zasady korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, określa porozumienie zawarte pomiędzy ministrem właściwym do spraw informatyzacji, a podmiotem, o którym mowa w ust. 2 – 2b. 2d. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2 – 2b, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”; c) uchyla się ust. 3;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. W związku z r nową rolą systemu informatycznego S46 konieczne było dodanie przepisów związanych z jego wykorzystaniem.
47.	Art. 48	w art. 48 w pkt 1 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT”;	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również

			usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.
48.	Art. 51 pkt 5	w art. 51: a) pkt 5 otrzymuje brzmienie: 5) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów w czasie stanu wojennego oraz w czasie wojny;" b) pkt 7 otrzymuje brzmienie: „7) ocenę cyberzagrożeń oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;";	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis uzupełnia zakres przedmiotowy ustawy o kwestie niewynikające z aktu o cyberbezpieczeństwie.
49.	Tytuł rozdziału 11	tytuł rozdziału 11 otrzymuje brzmienie: „Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych, SOC zewnętrznych i przedsiębiorców komunikacji elektronicznej"	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
50.	Art. 52a	Art. 52a. W celu zabezpieczenia realizacji przewidzianych w ustawie zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, o których mowa w art. 36a, art. 42 w zw. z art. 41 pkt 6, 9 i 11, art. 44 ust. 8 pkt 3, art. 51, art. 52 i art. 67e ust. 1, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.";".	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

51.	Art. 53 ust. 1 pkt 1i pkt 2	w art. 53: a) w ust. 1 – pkt 1 otrzymuje brzmienie: „1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi SOC, zewnętrznego, o którym mowa w art. 2 pkt 37, wymogów, o których mowa w art. 14 ust. 3–7 oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b;"; – w pkt 2 lit. a i b otrzymują brzmienie: „a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania cyberzagrożeniom i zgłaszania incydentów poważnych oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b, b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b;"; – po pkt 2 dodaje się pkt 3 w brzmieniu: – po pkt 2 dodaje się pkt 3 w brzmieniu: „3) Prezes UKE w zakresie wypełniania przez przedsiębiorców komunikacji elektronicznej obowiązków określonych w art. 20a ust. 2 i 3, art. 20b ust. 2 i 4, art. 20d ust. 1 i art. 20f oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b.", b) w ust. 2 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu: „3) Prezes UKE prowadzi kontrole w zakresie, o którym mowa w ust. 1 w pkt 3, oraz nakłada kary pieniężne na przedsiębiorców komunikacji elektronicznej.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Niniejsza zmiana związana jest z wprowadzeniem SOC-ów do ustawy o krajowym systemie cyberbezpieczeństwa.

52.	Art. 54 ust. 3	w art. 54 dodaje się ust. 3 w brzmieniu: „3. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 3, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.”;	Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.
53.	Art. 54a	Art. 54a. Prezes UKE może, po otrzymaniu wniosku od CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego.”;	Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.
54.	Art. 56 ust. 3	w art. 56 po ust. 2 dodaje się ust. 3 w brzmieniu: „3. Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt.”;	Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.
55.	Art. 59	„Art. 591. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy do spraw cyberbezpieczeństwa, minister właściwy do spraw informatyzacji lub Prezes UKE uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. 2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze. 3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy do spraw cyberbezpieczeństwa, ministra właściwego do spraw informatyzacji lub Prezesa UKE o sposobie wykonania zaleceń.”.	Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.
56.	Art. 59a	1. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje: 1) ministra właściwego do spraw informatyzacji; 2) Polskie Centrum Akredytacji; 3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;	Niniejszy przepis określa kogo obejmuje krajowy system certyfikacji cyberbezpieczeństwa. Służy on wyraźnemu wskazaniu jakie podmioty biorą udział w procesie certyfikacji. Przepis ten ma więc charakter porządkujący i służy skutecznemu wdrożeniu przepisów Aktu o Cyberbezpieczeństwie.

		4) dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje wyroby procesowi oceny zgodności zgodnie z ustawą. 2. Nadzór nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa w zakresie oceny zgodności sprawuje minister właściwy do spraw informatyzacji.	W punkcie 4 wskazany jest również wyraźnie dobrowolność poddania swoich wyrobów ocenie zgodności. Ust. 2 wskazuje wyraźnie organ nadzoru nad systemem certyfikacji cyberbezpieczeństwa tj. ministra właściwego do spraw informatyzacji. Kwestia ta jest następnie uszczegóławiana w kolejnych przepisach.
57.	Art. 59 d-g	3. Minimalne działania w zakresie oceny danego produktu ICT, usługi ICT czy procesu ICT obejmują: 1) w przypadku krajowego poziomu uzasadnienia zaufania ”podstawowy” – przegląd dokumentacji technicznej lub działania o równoważnym skutku, 2) w przypadku krajowego poziomu uzasadnienia zaufania ”istotny” – sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności oraz testowanie w celu wykazania, że w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa lub działania o równoważnym skutku, 3) w przypadku krajowego poziomu uzasadnienia zaufania ”wysoki” – obejmują sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, testowanie, czy w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne, nowoczesne funkcjonalności bezpieczeństwa oraz ocenę sprawdzającą za pomocą testów penetracyjnych ich odporność na zaawansowane atak lub działania o równoważnym skutku.	Akt o cyberbezpieczeństwie pozwala również Państwom Członkowskim na tworzenie krajowych programów certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami. To narzędzie pozwoli na rozwój rynku certyfikacji oraz umożliwi nam reagowanie na cyberzagrożenia w obszarach, które nie będą zagospodarowane przez Unie Europejską. Przyjęte przepisy są jak najbardziej zbliżone do przepisów aktów o cyberbezpieczeństwie opisujących europejskie programy certyfikacji cyberbezpieczeństwa. Dzięki temu będziemy mogli również stosunkowo łatwo przenieść wykorzystane przez nas rozwiązania na poziom europejski o ile pojawi się taka potrzeba. Celem krajowych programów certyfikacji cyberbezpieczeństwa jest zapewnienie, by produkty ICT, usługi ICT i procesy ICT certyfikowane zgodnie z takimi programami spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub

			dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT w niniejszym rozporządzeniu. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo trudne. Zwłaszcza, że mówimy tu o tak różnych przedmiotach jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład poprzez odesłanie do norm lub specyfikacji technicznych, w przypadku gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów zapewni skuteczność tych programów. Trzeba wskazać, że ta różnorodność wpływa na wszelkie aspekty tych programów np. w przypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady poprzez jego aktualizacje podczas gdy wykrycie określonej podatności w przenośnej pamięci usb może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w programie może wymagać

			zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy. W związku z tym minister właściwy do spraw informatyzacji powinien mieć swobodę opracowywania takiego programu. Następnie przygotowany program będzie przyjmowany w drodze rozporządzenia Rady Ministrów. Zapewni to odpowiednią rangę takiego programu oraz pozwoli wypowiedzieć się o nim wszystkim zainteresowanym podmiotom. Projektowane art. 59d-59g wyznaczają elementy krajowych programów certyfikacyjnych oraz wskazują poziomy uzasadnienia zaufania do których będą odwoływać się certyfikaty. Przepisy te zostały przygotowane na wzór odpowiednich przepisów aktu o cyberbezpieczeństwie przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania jakie musi spełniać produkt by uzyskać certyfikat określonego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Dzięki temu możliwa będzie promocja krajowych programów certyfikacyjnych w całej Unii

			Europejskiej i stosunkowo łatwe przenoszenie ich na poziom europejski. Ponadto takie rozwiązanie zapewni porównywalność certyfikatów krajowych z dokumentami z innych państwach członkowskich oraz sprawi, że certyfikaty będą bardziej czytelne dla zagranicznych klientów.
58.	Art. 59j	Art. 59j. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności. 2. Ocena zgodności jest dobrowolna. 3. Warunki techniczne przeprowadzania oceny zgodności określają europejskie lub krajowe programy certyfikacji cyberbezpieczeństwa.	Ten przepis wskazuje możliwość poddawania produktów, usług i procesów ICT ocenie zgodności. Ma on dwojaki cel wskazuje ogólną zasadę dotyczącą poddawania tych wyrobów ocenie zgodności oraz wskazuje, że warunki przeprowadzania tej oceny określają zarówno europejskie jak i krajowe programy certyfikacji cyberbezieczeństwa. Wyraźne odwołanie do tych programów jest konieczne by nie powstały wątpliwości związane z tym gdzie określone są owe warunki. Uwzględnienie w ust. 3 krajowych programów wynika z wprowadzenia przepisów, które umożliwią tworzenie takich dokumentów w ramach krajowego porządku prawnego.
59.	Art. 59l	Art. 59l. 1. Wniosek o certyfikację produktu ICT, usługi ICT lub procesu ICT składa jego dostawca do jednostki oceniającej zgodność. 2. Wniosek o certyfikację zawiera co najmniej: 1) nazwę albo imię i nazwisko wnioskującego oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania; 2) informacje potwierdzające spełnianie kryteriów certyfikacji; 3) wskazanie zakresu wnioskowanej certyfikacji. 3. Do wniosku dołącza się dokumenty potwierdzające spełnianie wymagań określonych we właściwym programie certyfikacyjnym. 4. Wniosek składa się na piśmie w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.	Przepis ten reguluje formalności związane z procesem certyfikacji. Określone w nim zostały szczegóły związane z wnioskiem o certyfikację. Wskazuje on wyraźnie przedsiębiorcy ubiegającemu się o certyfikację jakie dokładnie informacje musi przekazać by pomyślnie zakończyć proces certyfikacji. Eliminuje to ewentualne wątpliwości w tym zakresie. Wskazane też zostało kto może taki wniosek złożyć. To doprecyzowanie zapewni sprawny przebieg procesów certyfikacyjnych.

60.	Art. 59r	Art. 59r. 1. Dostawca, który poddał produkt ICT, usługę ICT lub proces ICT ocenie zgodności z wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa i potwierdził ich zgodność, wydaje krajową deklarację zgodności. 2. Krajowa deklaracja zgodności, odwołuje się do określonych w krajowym programie certyfikacji cyberbezpieczeństwa specyfikacji technicznych, norm i procedur, w tym kontroli mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom. 3. Produkt ICT, usługa ICT lub proces ICT spełniają wymagania określone w programie certyfikacji przez cały okres na jaki została wydana deklaracja zgodności. 4. Krajowa deklaracja zgodności wydawana jest wyłącznie dla produktów ICT, usług ICT lub procesów ICT odpowiadających wymaganiom dla krajowego poziomu uzasadnienia zaufania „podstawowy”.	Przepis ten sprawia, że te same zasady, jakie mają zastosowania do deklaracji zgodności wydanych w ramach europejskich programów certyfikacji cyberbezpieczeństwa będą również stosowane do deklaracji wydanych w ramach krajowych programów certyfikacyjnych.
61.	Art. 59u	Art. 59u. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa produktów ICT, usług ICT lub procesów IT, dla których została wydana krajowa deklaracja zgodności, udostępnia publicznie informacje zawierające: 1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT; 2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem; 3) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa; 4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatnościach związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa.	Przepis ten nakłada na przedsiębiorców, którzy uzyskali certyfikację w ramach krajowych programów certyfikacyjnych analogiczne obowiązki jak te spoczywające na tych, którzy podjęli działania w ramach europejskich programów certyfikacyjnych (art. 55 aktu o cyberbezpieczeństwie). Celem jest by krajowe i europejskie programy były do siebie jak najbardziej zbliżone oraz gwarantowały analogiczne poziomy cyberbezpieczeństwa. Przekazywanie danych użytkownikom produktów jest bardzo istotnym elementem zapewniającym cyberbezpieczeństwo. Użytkownicy, by prawidłowo korzystać z programów, potrzebują informacji o sposobie korzystania z udostępnionych im wyrobów. Brak tego przepisu prowadziłby do sytuacji w której użytkownicy produktów certyfikowanych w ramach krajowych programów certyfikacyjnych byliby w

		2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności.	gorszej sytuacji od tych korzystających z produktów certyfikowanych w ramach programów europejskich. By uniknąć takiej sytuacji oraz by zwiększyć poziom cyberbezpieczeństwo w sektorze przedsiębiorstw wprowadzono niniejszy przepis.
62.	Art. 62	w art. 62 w ust. 1: a) w pkt 1 i 2 wyrazy ,,CSIRT MON, CSIRT NASK i CSIRT GOV'' zastępuje się wyrazami "CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT i CSIRT sektorowy"; b) w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7 - 8 w brzmieniu: „7) wydawanie ostrzeżeń, 8) zwracaniem się ze zleceniem, o którym mowa w art. 26 ust. 2a.”;	Niniejsza ustawa oprócz implementacji przepisów aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.
63.	Art. 62a-62c	Art. 62a. 1. Pełnomocnik może wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje. 2. Rekomendacje Pełnomocnika są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika. 4. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium. 5. Podmiot krajowego systemu cyberbezpieczeństwa, uwzględnia rekomendacje w zarządzaniu ryzykiem , jeżeli zostały do niego skierowane.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
64.	Art. 64	Art. 64 Przy Radzie Ministrów działa Kolegium, jako organ opiniodawczo–doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowych, CSIRT Telco, CSIRT INT, Prezesa UKE i organów właściwych do spraw cyberbezpieczeństwa.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

65.	Art. 64a	„Art. 64a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT GOV, CSIRT MON, CSIRT NASK lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny. 2. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT GOV, CSIRT MON, CSIRT NASK lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 66a ust. 2, sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. 3. Zadania, o których mowa w ust. 1 i 2, są wykonywane w ramach ustawowych zadań odpowiednio CSIRT GOV, CSIRT MON, CSIRT NASK lub CSIRT INT.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie
66.	Art. 65	w art. 65 a) w ust. 1: - pkt 2 otrzymuje brzmienie: „2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, CSIRT sektorowe, CSIRT Telco, CSIRT INT, i organy właściwe do spraw cyberbezpieczeństwa powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania cyberzagrożeniom;” - pkt 4 otrzymuje brzmienie: „4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, CSIRT Telco, CSIRT INT i organów właściwych do spraw cyberbezpieczeństwa;”; - w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		„8) decyzji o w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.”. b) w ust. 2 przed wyrazami „Rady Ministrów” dodaje się wyraz „Prezesa”; c) po ust. 2 dodaje się ust. 3 w brzmieniu: „3. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo może również rozpatrywać poszczególne sprawy w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”;	
67.	Art. 66 ust. 1 pkt 4 oraz ust. 4	w art. 66: a) w ust. 1 pkt 4 otrzymuje brzmienie: „4) członkowie Kolegium: a) minister właściwy do spraw wewnętrznych, b) minister właściwy do spraw informatyzacji, c) minister właściwy do spraw energii, d) Minister Obrony Narodowej, e) minister właściwy do spraw zagranicznych, f) Szef Kancelarii Prezesa Rady Ministrów, g) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej, h) minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego, i) Przewodniczący Komisji Nadzoru Finansowego, j) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni, k) Prokurator Generalny. b) ust. 4 otrzymuje brzmienie: „4. W posiedzeniach Kolegium uczestniczą również: 1) Dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca; 2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca; 3) Szef Agencji Wywiadu albo jego zastępca;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Artykuł ten uzupełnia skład Kolegium do Spraw Cyberbezpieczeństwa co przyczyni się do zwiększenia roli Kolegium oraz lepszego przepływu informacji między organami działającymi w sprawach cyberbezpieczeństwa.

		4) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca; 5) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca; 6) Szef Służby Wywiadu Wojskowego albo jego zastępca; 7) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego albo jego zastępca."; c) w ust. 5 po pkt. 2, kropkę zastępuje się średnikiem i dodaje się pkt 3–8 w brzmieniu: ,,3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1; 4) może zlecić CSIRT GOV, CSIRT MON, CSIRT NASK lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1; 5) może zlecić CSIRT GOV, CSIRT MON, CSIRT NASK lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2; 6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1; 7) powołuje zespół opiniujący, o którym mowa w art. 66a ust. 10 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład.; 8) rozstrzyga spór, o którym mowa w art. 66a ust. 10 pkt 2, wskazując właściwego członka zespołu opiniującego."; d) w ust. 7 po wyrazach „CSIRT NASK," dodaje się wyrazy „CSIRT INT,";	
68.	Art. 66a-66e	„Art. 66a. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dostawcy sprzętu lub oprogramowania, które jest wykorzystywane przez: 1) podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 1–2, 3–20,	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, 3) właścicieli lub posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, – zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka". 2. Dostawcą sprzętu lub oprogramowania, o którym mowa w ust. 1, jest dostawca produktów ICT, usług ICT lub procesów ICT. 3. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się, jeżeli ustawa nie stanowi inaczej, przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy. 4. Stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka; 5. Do postępowania może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny, który w poprzednim roku obrotowym, uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504). Przepisy art.31 § 2 i § 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio. 6. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania. 7. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka.	W art. 66a została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. W rozumieniu tego artykułu dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT. Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Postępowanie nie będzie dotyczyło wszystkich produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez: 1) podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych, czy podmioty publiczne (ok. 4000 podmiotów); 2) przedsiębiorców telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, o których mowa w art. 176a ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (ok. 100 podmiotów); 3) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej w uzasadnieniu zwani operatorami infrastruktury krytycznej (ok. 130 podmiotów); 4) przedsiębiorców o szczególnym znaczeniu gospodarczo obronnym. Podmioty te są szczególnie ważne dla zapewnienia społeczno-ekonomicznego bezpieczeństwa państwa,

		8. Zawiadomienie, o którym mowa w ust. 7, udostępnia się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania. 9. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się. 10. Opinia, o której mowa w ust. 9 zdanie pierwsze, zawiera analizę: 1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego; 2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem: a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie, b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności tam gdzie nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem, c) struktury własnościowej dostawcy sprzętu lub oprogramowania,	dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu w trakcie świadczenia usług na rzecz państwa i obywateli. Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie miał zastosowanie Kodeks postępowania administracyjnego z zastrzeżeniem przepisów wskazanych w tej nowelizacji. Dzięki temu dostawca sprzętu lub oprogramowania będzie miał szanse obrony swoich praw. Decyzja ministra właściwego do spraw informatyzacji będzie miała formę decyzji administracyjnej, co pozwoli dostawcy na składanie środków odwoławczych przewidzianych w kodeksie oraz złożenie skargi na decyzję administracyjną do Wojewódzkiego Sądu Administracyjnego. Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek Przewodniczącego Kolegium. Gdy postępowanie zostanie wszczęte z urzędu to minister właściwy ds. informatyzacji będzie zobowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Wniosek Przewodniczącego Kolegium o wszczęcie postępowania będzie zawierał: dane identyfikujące dostawcę sprzętu lub oprogramowania, a także wskazanie zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy uwzględnianych w

		d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania; 3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.5.2019, str. 1–12, z późn. zm.); 4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania; 5) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt 1–4, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania; 6) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy. 11. Sporządzając opinię, o której mowa w ust. 7, Kolegium uwzględnia: 1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego; 2) analizy, o których mowa w art. 64a ust. 1 i 2. 12. Procedura sporządzenia opinii, o której mowa w ust. 9, przebiega w następujący sposób: 1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzą przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium; 2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, na podstawie analizy określony w ust. 10, które	postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. Immanentnym elementem wniosku będzie także opinia Kolegium w zakresie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka dla podmiotów. W takim przypadku Minister nie będzie zasięgał opinii Kolegium, ponieważ otrzyma ją we wniosku. Art. 66a ust. 6 zawiera wskazanie elementów analizy która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G). W ramach opinii będzie zawarta analiza dostawcy sprzętu lub oprogramowania na podstawie aspektów technicznych i nietechnicznych. Analizowane będą powiązania dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego oraz powiązania z podmiotami wobec których Unia Europejska zastosowała sankcje za cyberataki. Innym nietechnicznym aspektem będzie analiza zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania. Do technicznych aspektów opinii należy analiza: 1) liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

		następnie przekazuje zespołowi, o którym mowa w pkt 1. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego; 3) jeżeli nie zostały wykonane analizy, o których mowa w art. 64a ust. 1 i 2, Przewodniczący Kolegium zleca ich wykonanie; 4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii; 5) uzgodnienie opinii następuje na posiedzeniu Kolegium; 6) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji. 13. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi. 14. Decyzja, o której mowa w ust. 13, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka. 15. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 13, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra. 16. Decyzja, o której mowa w ust. 13, podlega natychmiastowemu wykonaniu. 17. Od decyzji, o której mowa w ust. 13, nie przysługuje wniosek o ponowne rozpatrzenie sprawy. Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 13, podmioty, o których mowa w art. 66a ust. 1 pkt 1–4:	2) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów o których mowa w ust. 1 pkt 1-4 oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania; 3) treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy. Podkreślić należy, że nie jest możliwe ograniczenie się w analizie dostawcy sprzętu lub oprogramowania wyłącznie do aspektów technicznych oferowanych przez niego produktów ICT, usług ICT czy procesów ICT. Postęp technologiczny umożliwił nie tylko poprawę jakości komunikacji ale także umożliwił nowe formy ingerencji państw trzecich w bezpieczeństwo narodowe. Coraz więcej urządzeń jest stale podłączonych do globalnej sieci, co powoduje że w każdej chwili jest przesyłana ogromna ilość danych. Dla służb wywiadowczych obcych państw są to potencjalnie potężne zasoby informacyjne, które mogą zostać wykorzystane przeciwko Polsce. Ponadto dostęp do urządzeń stale podłączonych do sieci poprzez ukryte (lub celowo zaprojektowane) podatności mógłby skutkować przejęciem kontroli nad znaczną liczbą urządzeń używanych przez podmioty krajowego systemu cyberbezpieczeństwa, czy operatorów infrastruktury krytycznej. W konsekwencji niezbędne jest aby istniała prawna formuła zidentyfikowania dostawcy wysokiego ryzyka i ograniczenia używania oferowanego przez niego sprzętu lub oprogramowania.

		1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka; 2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13. 2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy. 3. Do czasu wycofania sprzętu, o którym mowa w ust. 1 – 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. 4. Podmioty, o których mowa w art. 66 ust. 1 pkt 1–4, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129, 1598, 2054 i 2269 oraz z 2022 r. poz. 25), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 13. 5. W przypadku gdy podmioty, o których mowa w art. 66 ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129, 1598, 2054 i 2269 oraz z 2022 r. poz. 25), nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13, produkt, usługę lub proces określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13, a w przypadku produktów, usług lub procesów ICT wykorzystywanych do	

		wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 5 lat. Art. 66c. 1. Podmioty, o których mowa w art. 66 ust. 1 pkt 1–4, są obowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 66a ust. 13. 2. Uprawnionymi organami do żądania informacji, o których mowa w ust. 1, są wobec: 1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa; 2) SOC zewnętrznych – minister właściwy do spraw informatyzacji; 3) przedsiębiorców telekomunikacyjnych – Prezes UKE; 4) podmiotów publicznych – właściwe organy nadzorcze lub minister właściwy do spraw informatyzacji; 5) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym – ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2 tej ustawy; 3. Wniosek zawiera: 1) wskazanie podmiotu obowiązanego do przekazania informacji; 2) datę wydania; 3) wskazanie zakresu żądanych informacji; 4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni; 5) uzasadnienie 6) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 2d. 4. Minister właściwy do spraw informatyzacji może zwrócić się do uprawnionych organów, o których mowa w ust. 2 pkt 1 lub ust. 2 pkt 3–6, o żądanie informacji, o których mowa w ust. 1.	

		Art. 66d. 1. Sąd administracyjny rozpatruje skargę na decyzje, o której mowa w art. 66a ust. 13, na posiedzeniu niejawnym, w składzie trzech sędziów. 2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych. Art. 66e. Minister właściwy do spraw informatyzacji prowadzi i udostępnia przy użyciu systemu teleinformatycznego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 66a ust. 13.”;	
69.	Art. 67	w art. 67 w ust. 1 po pkt 3 dodaje się pkt 3a w brzmieniu: „3a) Szefa Agencji Wywiadu – w odniesieniu do działalności CSIRT INT;”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
70.	Art. 67a-67e	Art. 67a. 1. Pełnomocnik w przypadku uzyskania informacji wskazującej na możliwość wystąpienia incydentu krytycznego, może wydać ostrzeżenie w celu poinformowania o cyberzagrożeniu: 1) podmiotów, o których mowa w art. 4 pkt 1–16; 2) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 3) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907 i 2140); 4) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepisy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zawierają dodanie dwóch specjalnych środków – ostrzeżenia oraz polecenia zabezpieczającego. Ich stosowanie będzie ograniczone do niektórych grup podmiotów gospodarki i społeczeństwa. Będą mogły być stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) lub po zaistnieniu incydentu krytycznego, w celu skoordynowania efektywnej reakcji (polecenie zabezpieczające). Incydent

		2. Do ostrzeżenia nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 3. Pełnomocnik, przed wydaniem ostrzeżenia, przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą: 1) istotność cyberzagrożenia; 2) prawdopodobieństwo wystąpienia incydentu krytycznego; 3) rodzaje ryzyk; 4) skuteczność zalecenia określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu krytycznego lub alternatywnych metod zapewnienia cyberbezpieczeństwa. 4. Ostrzeżenie zawiera: 1) określenie rodzaju lub rodzajów podmiotów wskazanych w ust. 1, będących jego adresatami; 2) zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego; 3) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 3; 4) datę wejścia w życie ostrzeżenia. 5. Pełnomocnik odwołuje ostrzeżenie po: 1) uzyskaniu informacji o ustaniu zagrożenia wystąpienia incydentu krytycznego; 2) przeprowadzaniu przeglądu i ustaleniu, że nie jest zasadne jego utrzymanie. 6. Pełnomocnik przeprowadza przegląd ostrzeżenia nie rzadziej niż raz na rok od jego wydania. W ramach przeglądu ostrzeżeń Pełnomocnik może przeprowadzić analizę, o której mowa w ust. 3. 7. Pełnomocnik udostępnia: 1) informację o wydanym ostrzeżeniu, a także o odwołaniu ostrzeżenia, 2) listę wydanych i odwołanych ostrzeżeń – w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika, a także na stronie internetowej urzędu obsługującego Pełnomocnika.	krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie - po przeprowadzeniu należytej oceny - może być uznany przez CSIRT poziomu krajowego za incydent krytyczny. Pełnomocnik będzie mógł wydać ostrzeżenie, które będzie miękkim, niewiążącym środkiem wskazującym na ryzyko związane z możliwością wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko wystąpienia tego incydentu. Instrument ten jest wzorowany na ostrzeżeniach wydawanych przez czeską Narodową Agencję Bezpieczeństwa Cybernetycznego i Informacji. Z kolei minister właściwy do spraw informatyzacji będzie mógł wydać w formie decyzji administracyjnej polecenie zabezpieczające w przypadku wystąpienia incydentu krytycznego. Polecenie zabezpieczające będzie wydawane w sytuacji zapewnienia koordynacji reakcji na incydent krytyczny oraz konieczności ograniczenia skutków tego incydentu. Przed wydaniem ostrzeżenia lub polecenia zabezpieczającego niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie

		8. Informacja o wydaniu ostrzeżenia może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1. 9. Zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego może polegać na: 1) przeprowadzeniu szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzeniu środków ochrony proporcjonalnych do zidentyfikowanych ryzyk; 2) dokonaniu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością; 3) wdrożeniu określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność; 4) dokonaniu określonej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności; 5) prowadzeniu wzmożonego monitorowania zachowania systemu; 6) odstąpieniu od korzystania z określonego sprzętu lub oprogramowania; 7) wprowadzeniu reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL. Art. 67b. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające. 2. Polecenie zabezpieczające dotyczy nieokreślonej liczby: 1) podmiotów, o których mowa w art. 4 pkt 1–16; 2) właścicieli oraz posiadaczy samoistnych i zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 3) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych; 4) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji	przeprowadzana wspólnie z Zespołem. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny. Zarówno ostrzeżenie jak i polecenie będą musiały zawierać: 1) wskazanie rodzajów ryzyk; 2) wskazanie rodzajów podmiotów, których dotyczy; 4) datę wejścia w życie; 5) uzasadnienie zawierające wyniki analizy. Ostrzeżenie jako miękki środek będzie zawierało zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu. Katalog możliwych zaleceń został wskazany w art. 67a ust. 8. Z kolei polecenie zabezpieczające jako mocniejszy środek, będzie zawierało wskazanie określonego zachowania, które zmniejszy skutki incydentu lub zapobiegnie jego rozprzestrzenianiu się. Katalog zachowań został wskazany w art. 67b ust. 9. Decyzja o zastosowaniu się do ostrzeżenia przez operatorów usług kluczowych będzie należeć do nich samych, przepis jedynie zobowiązuje ich do uwzględnienia ostrzeżenia podczas procesu szacowania ryzyka.

		elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE. 3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy stosuje się odpowiednio. 4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne udostępnienie informacji na stronie podmiotowej ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej. 5. Minister właściwy do spraw informatyzacji, przed wydaniem polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę , obejmującą: 1) istotność cyberzagrożenia; 2) rodzaje ryzyk; 3) przewidywane lub zaistniałe skutki incydentu krytycznego, 4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się; 5) przewidywane finansowe, społeczne i prawne skutki wydania polecenia zabezpieczającego. 6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. 7. Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. 8. Przedstawiciele podmiotów, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Dyrektora Rządowego Centrum Bezpieczeństwa do udziału w pracach Zespołu lub posiedzeniach Zespołu w związku z przygotowywaniem analizy, o której mowa w ust. 5. 9. Polecenie zabezpieczające zawiera:	

		1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy; 2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się, oraz 3) termin jego wdrożenia. 10. Przez zachowanie, o którym mowa w ust. 9 pkt 2, rozumie się: 1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk, 2) nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością, 3) nakaz zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność, 4) nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności, 5) nakaz wzmożonego monitorowania zachowania systemu, 6) zakaz korzystania z określonego sprzętu lub oprogramowania, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego, 7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu określonego w art. 67b ust. 2, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT GOV, CSIRT MON lub CSIRT NASK jako przyczyna trwającego incydentu krytycznego, 8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania, 9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych, lub 10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.	

		11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5. 12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata. 13. Polecenie zabezpieczające wygasa: 1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub 2) po upływie czasu na które zostało wydane. 14. Polecenie zabezpieczające podlega natychmiastowej wykonalności. 15. Minister właściwy do spraw informatyzacji ogłasza polecenie zabezpieczające w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Informacje o poleceniu zabezpieczającym udostępnia się również na stronie podmiotowej ministra w Biuletynie Informacji Publicznej lub na stronie internetowej urzędu obsługującego ministra. 16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy. 18. Nadzór nad wykonywaniem polecenia zabezpieczającego sprawują organy właściwe do sprawowania nadzoru nad danym podmiotem. Art. 67c. 1. Skargę na decyzję, o której mowa w art. 67b ust. 1, wnosi się w terminie 2 miesięcy, od dnia, w którym decyzja została ogłoszona w dzienniku urzędowym ministra właściwego do spraw informatyzacji. 2. Sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia, , jeżeli dotyczą tej samej decyzji. 3. Wniosek o przywrócenie terminu na złożenie skargi jest niedopuszczalny. Art. 67d 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 66b i art. 66c oraz art. 67b.	

		2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o: 1) decyzjach wydanych na podstawie art. 66a ust. 13; 2) wydanych poleceniach zabezpieczających. Art. 67e. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26 ustawy. 2. Decyzja, o której mowa w ust. 1, określa w szczególności: 1) zakres powierzonych zadań; 2) czas realizacji powierzonych zadań lub sposób ich odwołania; 3) w razie potrzeby – szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV; 4) zasady informowania Kolegium o stanie realizacji powierzonych zadań. 3. Realizacja zadań, o których mowa w ust. 1, dokonywana jest przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych.”;	
71.	Art. 73	w art. 73: a) w ust. 1 – w pkt 4 wyraz „osoby” zastępuje się wyrazem „osób”, – w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 i 15 w brzmieniu: „14) z własnej winy nie korzysta z systemu, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11; 15) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 3.”; b) po ust. 1 dodaje się ust. 1a–1c w brzmieniu: „1a. Jednostka oceniająca zgodność, która: 1) nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne, 2) nie wykonuje obowiązku określonego w art. 59zb ust. 1 – podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Wprowadzone w tych ustępach przepisy karne odnoszą się do obowiązków niezwiązanych z aktem o cyberbezpieczeństwie.

		gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem". 1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających, w chwili jego wydania, wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia. 1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która: 1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w, 2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w, 3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa, 4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji, 5) nie wykonuje obowiązku określonego w art. 59s – podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.", c) po ust. 2 dodaje się ust. 2a–2d w brzmieniu: „2a. Karze pieniężnej podlega podmiot określony w art. 66a ust. 1 pkt 1–4, który nie dostosował się do obowiązków określonych w art. 66b. 2b. Karze pieniężnej podlega podmiot, którego dotyczy polecenie zabezpieczające, który: 1) nie wdrożył w terminie zachowania określonego w poleceniu zabezpieczającym,	

		2) odstąpił od wykonywania zachowania, określonego w poleceniu zabezpieczającym, przed wygaśnięciem polecenia zabezpieczającego 2c. Na podmiot publiczny, który nie wyznaczył osób, o których mowa w art. 21, może być nałożona kara pieniężna, jeżeli brak wyznaczenia tych osób uniemożliwia lub utrudnia wymianę informacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa a tym podmiotem.”. 2d. Na podmiot, który nie wypełnia obowiązków informacyjnych, o których mowa w art. 66c, może zostać nałożona kara pieniężna, jeżeli przemawia za tym charakter lub zakres naruszenia.”, d) w ust. 3: – pkt 9 otrzymuje brzmienie: „9) ust. 1 pkt 10 i 15, wynosi do 100 000 zł;”, – po pkt 11 dodaje się pkt 11a w brzmieniu: „11a) ust. 1 pkt 14 wynosi do 100 000 zł;” – dodaje się pkt 14–17 w brzmieniu: „14) ust. 2a, wynosi: a) w przypadku podmiotów określonych w art. 66a ust. 1 pkt 1–4, z wyjątkiem podmiotów publicznych, do 3% jego całkowitego rocznego światowego obrotu podmiotu z poprzedniego roku obrotowego, b) w przypadku podmiotów publicznych do 100 000 zł; 15) ust. 2b, wynosi: a) w przypadku podmiotów określonych w art. 67b ust. 2 z wyjątkiem podmiotów publicznych, do 3% całkowitego rocznego światowego obrotu podmiotu z poprzedniego roku obrotowego, b) w przypadku podmiotów publicznych do 100 000 zł; 16) ust. 2c, wynosi do 10 000 zł; 17) ust. 2d.wynosi do 50 000 zł”, e) dodaje się ust. 6 – 7 w brzmieniu: 6. Niezależnie od kary pieniężnej, o której mowa w ust. 2c, minister właściwy do spraw informatyzacji może nałożyć, w drodze decyzji, na kierującego	

		podmiotem publicznym, o którym mowa w art. 4 pkt 7–15, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek, 7. Niezależnie od kary pieniężnej, o której mowa w ust. 2d, można nałożyć na kierującego podmiotem, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego tego podmiotu lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.”;	
72.	Art. 74 ust. 1	1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten wskazuje organ właściwy do wydawania kar.
73.	Art. 74 ust. 1b-2	dodaje się ust. 1a i 1b w brzmieniu: „1a. Karę pieniężną, o której mowa w art. 73 ust. 1a–1c, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji. 1b. Karę pieniężną, o której mowa w art. 73 ust. 2a nakłada, w drodze decyzji: 1) w przypadku przedsiębiorców komunikacji elektronicznej – Prezes UKE; 2) w przypadku operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej – organ właściwy do spraw cyberbezpieczeństwa; d) w przypadku podmiotów określonych w art. 66a ust. 1, innych niż przedsiębiorcy komunikacji elektronicznej, operatorzy usług kluczowych, dostawcy usług cyfrowych – minister właściwy do spraw informatyzacji.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Przepis ten wskazuje organ właściwy do wydawania kar.

		1c. Karę pieniężną, określoną w art. 73 ust. 2b nakłada, w drodze decyzji: 1) w przypadku przedsiębiorców komunikacji elektronicznej, którzy nie są krajowymi instytucjami płatniczymi – Prezes UKE; 2) w przypadku operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej – organ właściwy do spraw cyberbezpieczeństwa; 3) w przypadku krajowych instytucji płatniczych – Komisja Nadzoru Finansowego; 4) w przypadku podmiotów określonych w art. 67b ust. 1, innych niż przedsiębiorcy komunikacji elektronicznej, operatorzy usług kluczowych, dostawcy usług cyfrowych, krajowe instytucje płatnicze,– minister właściwy do spraw informatyzacji. 1d. Karę pieniężną, o której mowa w art. 73 ust. 2c, nakłada w drodze decyzji minister właściwy do spraw informatyzacji. 1e. Karę pieniężną o której mowa w art. 73 ust. 2d i 7 może nałożyć w drodze decyzji organ uprawniony do żądania informacji zgodnie z właściwością określoną w art. 66c ust. 2.”, c) ust. 2 otrzymuje brzmienie: „2. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.”;	
74.	Art.74a	„Art. 74a 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ust. 2a lub 2b, podmiot, wobec którego wszczęto to postępowanie, jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej. 2. W przypadku gdy podmiot, wobec którego wszczęto postępowanie w sprawie nałożenia kary pieniężnej, o której mowa o której mowa w art. 73 ust. 2a lub 2b:	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		1) nie dostarczył danych niezbędnych do określenia podstawy wymiaru kary pieniężnej lub 2) dostarczone przez ten podmiot dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej – organ uprawniony do nałożenia kary ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu.”;	
75.	Art. 75a-75b	„Art. 75a. 1. Organ właściwy do spraw cyberbezpieczeństwa nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT sektorowego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44 ust. 1a. 2. Szef Agencji Wywiadu nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT INT, jeżeli nie został wykonany obowiązek, o którym mowa w art. 36c. 3. Minister właściwy do spraw informatyzacji nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT Telco, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44a ust. 5. 4. Kara pieniężna, o której mowa w ust. 1 - 3, nakładana jest w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek. Art. 75b. Wpływy z tytułu kar pieniężnych, o których mowa w art. 75 i art. 75a, stanowią przychód Funduszu Cyberbezpieczeństwa.”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
76.	76d – 76s	68) przed art. 77 dodaje się oznaczenie i tytuł działu oraz oznaczenie i tytuł rozdziału w brzmieniu: „DZIAŁ III. STRATEGICZNA SIEĆ BEZPIECZEŃSTWA Rozdział 1 Operator strategicznej sieci bezpieczeństwa Art. 76d. 1. W celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, tworzy się strategiczną sieć bezpieczeństwa, będącą siecią telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.

		2. Strategiczna sieć bezpieczeństwa jest uruchamiana oraz zarządzana przez Operatora strategicznej sieci bezpieczeństwa. 3. Prezes Rady Ministrów może określić, w drodze rozporządzenia, minimalne wymagania techniczne jakie musi spełniać strategiczna sieć bezpieczeństwa oraz minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo–technicznej. Art. 76e. 1. Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa, spośród podmiotów spełniających łącznie następujące warunki: 1) będących jednoosobową spółką Skarbu Państwa; 2) będących przedsiębiorcą telekomunikacyjnym; 3) posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 76d ust. 1 lub które zobowiązały się do jej pozyskania; 4) posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej; 5) posiadających świadectwo bezpieczeństwa przemysłowego; 6) dających rękojmię należytego wykonywania zadań Operatora strategicznej sieci bezpieczeństwa - pod warunkiem wyrażenia zgody na pełnienie funkcji Operatora strategicznej sieci bezpieczeństwa. Art. 76f. 1. Operator strategicznej sieci bezpieczeństwa w celu realizacji zadań, o których mowa w art. 76d ust. 1, świadczy usługi telekomunikacyjne oraz może świadczyć usługi związane z zapewnieniem udogodnień towarzyszących oraz usług z zakresu cyberbezpieczeństwa. 2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 111 ust. 2 pkt 2 i 3 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Wykorzystanie częstotliwości użytkowanych jako	

		rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3. 3. Wykorzystanie częstotliwości, o których mowa w art. 76t ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 143 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się odpowiednio. Art. 76g. 1. Operator strategicznej sieci bezpieczeństwa świadczy usługi, na potrzeby realizacji zadań określonych w art. 76d ust.1, na rzecz: 1) Kancelarii Prezydenta RP, 2) Kancelarii Sejmu, 3) Kancelarii Senatu, 4) Kancelarii Prezesa Rady Ministrów, 5) Biura Bezpieczeństwa Narodowego, 6) urzędów obsługujących organy administracji rządowej, organy jednostek samorządu terytorialnego oraz podmiotom podległym tym organom albo przez nie nadzorowanym, wykonującym zadania z zakresu: a) ochrony bezpieczeństwa i porządku publicznego, b) bezpieczeństwa i obronności państwa, c) bezpieczeństwa ekonomicznego, d) ochrony granicy państwa, e) ochrony ludności i obrony cywilnej, f) zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, g) dostaw energii, h) ochrony interesów Rzeczypospolitej Polskiej, i) ochrony zdrowia, j) weterynaryjnej ochrony zdrowia publicznego, k) nadzoru sanitarnego, l) ochrony środowiska, m) sprawiedliwości, n) sądownictwa, o) prokuratury,	

		p) systemu powiadamiania ratunkowego; 7) Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej, 8) podmiotów wykonujących na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa – na wniosek tych podmiotów. 2. Podmioty, o których mowa w ust. 1, korzystają z usług telekomunikacyjnych w ruchomej publicznej sieci telekomunikacyjnej świadczonych przez Operatora strategicznej sieci bezpieczeństwa, przy pomocy strategicznej sieci bezpieczeństwa, w zakresie niezbędnym do zapewnienia w tych podmiotach realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. 3. Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego nie mają obowiązku korzystania z sieci, o której mowa w ust. 2. 4. Prezes Rady Ministrów może zobowiązać Operatora strategicznej sieci bezpieczeństwa do świadczenia usług, o których mowa w art. 76f ust. 1: 1) właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym - na wniosek organu, we właściwości którego znajduje się określony system infrastruktury krytycznej, lub 2) przedsiębiorcom realizującym zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny - na wniosek Ministra Obrony Narodowej.. 5. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Państwowa Straż Pożarna, Służba Ochrony Państwa oraz Policja mogą zlecić Operatorowi strategicznej sieci bezpieczeństwa świadczenie usługi wsparcia technicznego, z uwzględnieniem aktualnego poziomu wiedzy naukowo–technicznej	

		dotyczącego nowoczesnych systemów łączności. Usługi wsparcia technicznego mogą polegać w szczególności na utrzymaniu, rozbudowie i modyfikacji sieci teleinformatycznych w zakresie sieci rozległych oraz zestawienia i utrzymania łączy dostępowych do takich sieci. 6. Świadczenie usług, o których mowa w ust. 1-5 oraz art. 76f ust. 1, przez Operatora strategicznej sieci bezpieczeństwa wymaga zawarcia umowy pomiędzy Operatorem strategicznej sieci bezpieczeństwa a właściwym podmiotem, o którym mowa w ust. 1 i 2. 7. Umowa, o której mowa w ust. 6, określa w szczególności obowiązek zapewnienia przez Operatora strategicznej sieci bezpieczeństwa usług telekomunikacyjnych o określonej jakości, dostępności, pojemności i wydajności, w tym w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, a w przypadku wydania rozporządzenia, o którym mowa w art. 76d ust. 3, także obowiązek zapewnienia określonego w rozporządzeniu poziomu bezpieczeństwa sieci i usług. 8. W przypadku uporczywego niewywiązywania się przez Operatora z obowiązków wynikających z umowy, o której mowa w ust. 6, podmiot na rzecz którego Operator świadczy usługi może rozwiązać taką umowę, informując Prezesa Rady Ministrów o przyczynach rozwiązania umowy. 9. W wypadku, o którym mowa w ust. 8, podmiot może zlecić świadczenie usług objętych umową, o której mowa w ust. 6, operatorowi telekomunikacyjnemu innemu niż Operator strategicznej sieci bezpieczeństwa, dającemu rękojmię zapewnienia bezpieczeństwa świadczonych usług na poziomie nie niższym niż określony w rozwiązanej umowie z Operatorem strategicznej sieci bezpieczeństwa lub w rozporządzeniu wydanym na podstawie art. 76d ust. 3. Art. 76h. W związku z ochroną istotnych interesów bezpieczeństwa państwa, przy zawieraniu umów, o których mowa w art. 76g ust. 6, dotyczących realizacji zadań, o których mowa w art. 76d ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.	

		Art. 76i. 1. Prezes UKE może dokonywać analizy cen usług telekomunikacyjnych stosowanych przez Operatora strategicznej sieci bezpieczeństwa, o których mowa w art. 76g ust. 2. 2. Podmioty, o których mowa w art. 76g ust. 1,Operatora strategicznej sieci bezpieczeństwa mogą wnioskować o dokonanie analizy, o której mowa w ust. 1. 3. Prezes UKE dokonuje analizy, o której mowa w ust. 1, w terminie 2 miesięcy, od złożenia wniosku, o którym mowa w ust. 2. 4. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę , których dotyczą, podmiot zobowiązany do zawarcia umowy z Operatora strategicznej sieci bezpieczeństwa może rozpocząć procedurę zawarcia umowy o świadczenie usług telekomunikacyjnych z innym dostawcą usług. Prezes UKE informuje Operatora strategicznej sieci bezpieczeństwa o wynikach analizy, o której mowa w ust. 1 5. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę a, których dotyczą, Operator strategicznej sieci bezpieczeństwa w terminie 7 dni, od dnia otrzymania informacji, o której mowa w ust. 4, jest obowiązany przedstawić nową ofertę podmiotowi zobowiązanemu do zawarcia umowy z Operatorem strategicznej sieci bezpieczeństwa. Prezes UKE, na wniosek operatora strategicznej sieci bezpieczeństwa, dokonuje analizy cen usług telekomunikacyjnych przedstawionych w nowej ofercie w terminie 21 dni, od otrzymania wniosku. O wyniku analizy informowany jest podmiot, do którego ta oferta została skierowana. 6. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 5, przekraczają koszty oraz rozsądną marżę, Prezes UKE wydaje decyzję zastępującą albo zmieniającą umowę, uwzględniając przedłożoną ofertę oraz określa cenę świadczonych usług na poziomie odpowiadającym kosztom oraz rozsądnej marży. Art. 76j. 1. Operator strategicznej sieci bezpieczeństwa przekazuje Prezesowi UKE informacje o zawartej umowie na świadczenie usług za	

		pośrednictwem strategicznej sieci bezpieczeństwa, w szczególności cenę oraz zakres świadczonych usług, w terminie 14 dni od dnia zawarcia umowy. 2. Operator strategicznej sieci bezpieczeństwa jest obowiązany do przekazywania na żądanie Prezesa UKE informacji niezbędnych do wykonywania przez Prezesa UKE jego uprawnień i obowiązków, w terminie 21 dni od otrzymania żądania. Art. 76k. 1. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2022 r. poz. 884), zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do infrastruktury technicznej, w tym współkorzystanie z niej, w celu realizacji zadań, o których mowa w art. 76d ust. 1. 2. Dostęp do infrastruktury technicznej jest odpłatny, chyba że strony umowy postanowią inaczej. 3. Opłaty z tytułu dostępu do infrastruktury technicznej określa się w wysokości, która umożliwia zwrot części kosztów, które ponosi operator sieci w związku z utrzymaniem tej infrastruktury oraz z zapewnieniem dostępu. 4. Warunki dostępu, o którym mowa w ust. 1, w tym techniczne, eksploatacyjne i finansowe warunki współpracy, określa umowa zawarta w formie pisemnej lub elektronicznej pomiędzy Operatorem strategicznej sieci bezpieczeństwa a operatorem sieci. Przepisy art. 19 ust. 1 – 2a, 4 i 5, art. 20, 24 i 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio. 5. W przypadku odmowy udzielenia dostępu do infrastruktury technicznej przez operatora sieci lub niezawarcia umowy o dostępie do infrastruktury technicznej w terminie 2 miesięcy od dnia złożenia wniosku o taki dostęp, Operator strategicznej sieci bezpieczeństwa może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do infrastruktury technicznej. 6. Do wniosku do Prezesa UKE o wydanie decyzji w sprawie dostępu do infrastruktury technicznej dołącza się:	

		1) wniosek w sprawie zawarcia umowy o dostępie do infrastruktury technicznej; 2) potwierdzenie doręczenia drugiej stronie lub potwierdzenie nadania przesyłką poleconą wniosku, o którym mowa w pkt 1; 3) dokumenty z negocjacji prowadzonych z drugą stroną, o ile druga strona podjęła negocjacje; 4) projekt umowy o dostępie do infrastruktury technicznej, z zaznaczeniem tych części umowy, co do których strony nie doszły do porozumienia. 7. Strony są obowiązane przedłożyć Prezesowi UKE, na jego żądanie, w terminie 14 dni, swoje stanowiska wobec rozbieżności oraz dokumenty niezbędne do rozpatrzenia wniosku. 8. Prezes UKE wydaje decyzję w sprawie dostępu do infrastruktury technicznej, w celu realizacji przez Operatora strategicznej sieci bezpieczeństwa zadań, o których mowa w art. 76d ust. 1, w terminie 2 miesięcy od dnia złożenia wniosku o jej wydanie przez Operatora strategicznej sieci bezpieczeństwa, biorąc pod uwagę w szczególności konieczność zapewnienia niedyskryminacyjnych i proporcjonalnych warunków dostępu. 9. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, w terminie 14 dni od dnia otrzymania zawiadomienia o wszczęciu postępowania o wydanie decyzji w sprawie dostępu do infrastruktury technicznej, przedstawia Prezesowi UKE uzasadnienie wysokości opłat z tytułu dostępu do infrastruktury technicznej, w którym uwzględnia kryteria, o których mowa w ust. 3. 10. Decyzja w sprawie dostępu do infrastruktury technicznej w zakresie nią objętym zastępuje umowę o tym dostępie. 11. W przypadku zawarcia przez zainteresowane strony umowy o dostępie do infrastruktury technicznej, decyzja o dostępie do infrastruktury technicznej wygasa z mocy prawa w części objętej umową. 12. Decyzja w sprawie dostępu do infrastruktury technicznej może zostać zmieniona przez Prezesa UKE na wniosek każdej ze stron, której ona	

		dotyczy, lub z urzędu, w przypadkach uzasadnionych potrzebą zapewnienia ochrony interesów odbiorców usług świadczonych przez podmioty wykonujące zadania z zakresu użyteczności publicznej lub użytkowników końcowych lub zapewnienia ochrony skutecznej konkurencji. 13. W postępowaniu w sprawie zmiany decyzji w sprawie dostępu do infrastruktury technicznej przepisy ust. 3 oraz ust. 8-10 stosuje się odpowiednio. Art. 76l. 1. Na potrzeby realizacji zadań, o których mowa w art. 76d ust. 1: 1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa, 2) jednostka samorządu terytorialnego, oraz 3) właściciel lub zarządca nieruchomości – zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do nieruchomości, w tym do budynku, polegający na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości. 2. Warunki dostępu, o którym mowa w ust. 1, określa odpowiednio umowa zawarta pomiędzy Operatorem strategicznej sieci bezpieczeństwa a podmiotami, o których mowa w ust. 1. Przepisy art. 19 ust. 1-2a, 4 i 5, art. 20 i 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio. 3. Umowa, o której mowa w ust. 2, jest zawierana w formie pisemnej lub elektronicznej. 4. Dostęp, o którym mowa w ust. 1, jeżeli podmiotem zapewniającym dostęp jest: 1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu jest nieodpłatny; 2) jednostka samorządu terytorialnego, właściciel lub zarządca nieruchomości, jest nieodpłatny, przy czym Operator strategicznej sieci bezpieczeństwa ponosi:	

		a) proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością, b) proporcjonalną część kosztów, które wystąpiły po stronie udostępniającego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu, c) koszty przywrócenia nieruchomości do stanu poprzedniego. 5. W przypadku odmowy udzielenia dostępu do nieruchomości przez podmioty, o których mowa w ust. 1, lub niezawarcia umowy o dostępie do nieruchomości w terminie miesiąca od dnia złożenia wniosku o taki dostęp każda ze stron może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do nieruchomości. 6. Przepisy art. 76k ust. 6-8 oraz ust. 10-13 stosuje się odpowiednio. Art. 76m. 1. Od decyzji Prezesa UKE dotyczącej dostępu telekomunikacyjnego, o którym mowa w art. 76k ust. 5 oraz art. 76l ust. 5, przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów. Art. 76n. Operatorowi strategicznej sieci bezpieczeństwa przysługuje prawo pierwokupu sieci telekomunikacyjnych będących własnością: 1) Skarbu Państwa lub innych państwowych osób prawnych, w szczególności podmiotów, o którym mowa w art. 4 pkt 1, 2, 4, 5, 7 i 8 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, 2) jednostek samorządu terytorialnego. 2. Podmioty o których mowa w ust. 1 pkt 1-2 informują Operatora strategicznej sieci bezpieczeństwa o zamiarze zbycia sieci telekomunikacyjnych, określając termin na skorzystanie z prawa pierwokupu nie krótszy niż 2 tygodnie. 3. W przypadku braku odpowiedzi od Operatora strategicznej sieci bezpieczeństwa w wyznaczonym terminie, przyjmuje się, że Operator strategicznej sieci bezpieczeństwa zrezygnował ze skorzystania z prawa pierwokupu. Art. 76o. 1. W sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 40 lit. a, w przypadku pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703-713 MHz i 758-768 MHz, Operator	

		strategicznej sieci bezpieczeństwa może zażądać od podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz udostępnienia zasobów częstotliwości z tego zakresu. 2. Podmiot dysponujący rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz jest obowiązany udostępnić Operatorowi strategicznej sieci bezpieczeństwa zasoby częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz niezwłocznie, nie później niż w ciągu jednej godziny, z wyjątkiem częstotliwości, które zostały udostępnione Siłom Zbrojnym Rzeczypospolitej Polskiej. 3. Operator strategicznej sieci bezpieczeństwa, występując z żądaniem, o którym mowa w ust. 1, informuje podmiot dysponujący rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz o czasie i zasięgu terytorialnym tego udostępnienia. 4. Żądanie, o którym mowa w ust. 1, jest przekazywane za pośrednictwem kanału komunikacji, o którym mowa w art. 76o. 5. Okres udostępnienia zasobów częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz na rzecz Operatora strategicznej sieci bezpieczeństwa jest ograniczony do okresu występowania sytuacji szczególnego zagrożenia, o której mowa w ust. 1, oraz sytuacji pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703-713 MHz i 758-768 MHz przez Operatora strategicznej sieci bezpieczeństwa, przy czym nie może być dłuższy niż 72 godziny. W przypadku ustania okoliczności, o których mowa w ust. 1, Operator strategicznej sieci bezpieczeństwa niezwłocznie zwalnia udostępnione zasoby częstotliwości. 6. Operator strategicznej sieci bezpieczeństwa może ponawiać żądanie udostępnienia częstotliwości na kolejne 72 godziny, z zastrzeżeniem ust. 5 zdanie drugie. 7. Zasięg terytorialny udostępnienia zasobów częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz nie może przekraczać obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1. 8. Operator strategicznej sieci bezpieczeństwa przekazuje w postaci elektronicznej na elektroniczną skrzynkę podawczą Prezesa UKE uzasadnienie żądania, o którym mowa w ust. 1, w terminie 1 dnia od dnia	

		wystąpienia z tym żądaniem do podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz. 9. Przepis ust. 8 stosuje się odpowiednio w przypadku ponowienia żądania, o którym mowa w ust. 6. 10. Uzasadnienie, o którym mowa w ust. 8, zawiera: 1) opis sytuacji szczególnego zagrożenia, o której mowa w ust. 1; 2) wskazanie przyczyn pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703-713 MHz i 758-768 MHz; 3) wskazanie obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1. 11. Prezes UKE może w ciągu 1 dnia od dnia otrzymania uzasadnienia, o którym mowa w ust. 8, zażądać od Operatora strategicznej sieci bezpieczeństwa dodatkowych wyjaśnień względem tego uzasadnienia. Do czasu uzyskania wyjaśnień, uzasadnienie uważa się za niezłożone. 12. W przypadku niezłożenia uzasadnienia, w terminie o którym mowa w ust. 8, lub nieprzedstawienia wyjaśnień, o których mowa w ust. 11, Operator strategicznej sieci bezpieczeństwa nie może, do czasu wykonania powyższych obowiązków, ponownie żądać od tego samego podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz udostępnienia zasobów częstotliwości z tego zakresu. 13. Prezes UKE udostępnia na wniosek podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788, od którego Operator strategicznej sieci bezpieczeństwa zażądał udostępnienia tych częstotliwości, uzasadnienie, o którym mowa w ust. 8, lub uzasadnienie wydłużenia czasu udostępnienia zasobów częstotliwości. 14. W sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 40 lit. a, Operator strategicznej sieci bezpieczeństwa jest obowiązany udostępnić Siłom Zbrojnym Rzeczypospolitej Polskiej udostępnione mu przez podmiot dysponujący rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz zasoby częstotliwości z tego zakresu niezwłocznie, nie później niż w ciągu jednej godziny, na czas na jaki zostały mu udostępnione. Przepisy ust. 3, 5, 7-8 i 10 stosuje się odpowiednio.	

		Art. 76p. Podmiot posiadający rezerwację częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz określa kanał komunikacji elektronicznej, umożliwiający niezwłoczną wymianę komunikatów z Operatorem strategicznej sieci bezpieczeństwa i przekazuje informację o tym kanale do Operatora strategicznej sieci bezpieczeństwa w terminie 14 dni od otrzymania decyzji w sprawie rezerwacji częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz. Art. 76q. W zakresie nieuregulowanym w ustawie do Operatora strategicznej sieci bezpieczeństwa stosuje się przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Art. 76r. 1. W przypadku, w którym podmiot wyznaczony na Operatora strategicznej sieci bezpieczeństwa przestaje spełniać którąkolwiek z przesłanek, o których mowa w art. 76e ust. 1, Prezes Rady Ministrów może: 1) odwołać Operatora strategicznej sieci bezpieczeństwa, wskazując termin tego odwołania, oraz 2) wyznaczyć nowego Operatora strategicznej sieci bezpieczeństwa za jego zgodą, wskazując termin objęcia tej funkcji. 2. Prezes Rady Ministrów, po zasięgnięciu opinii dotychczasowego Operatora strategicznej sieci bezpieczeństwa wyznacza termin odwołania dotychczasowego operatora oraz wyznaczenia nowego. 3. Prezes Rady Ministrów, w drodze zarządzenia, określa sposób przekazania majątku trwałego nabytego z wykorzystaniem środków publicznych, w celu wykonywania zadań, o których mowa w art. 76d ust. 1, na rzecz nowego Operatora strategicznej sieci bezpieczeństwa. Art. 76s. W przypadku, o którym mowa w art. 76r ust. 1: 1) podmiot wyznaczony na nowego Operatora strategicznej sieci bezpieczeństwa jest następcą prawnym i wstępuje w ogół praw i obowiązków dotychczasowego Operatora strategicznej sieci bezpieczeństwa w zakresie realizacji zadań, o których mowa w art. 76d ust. 1; 2) umowy, o których mowa w art. 76g ust. 6, wygasają z mocy prawa w terminie 3 miesięcy od wyznaczenia nowego Operatora strategicznej sieci bezpieczeństwa.	

77.	Art. 93 ust. 8 i ust. 23	w art. 93 uchyla się ust. 8 i ust. 23	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
78.	Załącznik nr 1	w załączniku nr 1 do ustawy: a) w wierszu „Ochrona zdrowia” w kolumnie trzeciej „Rodzaj podmiotów: – skreśla się wiersz czwarty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2020 r. poz. 944).”, – skreśla się wiersz piąty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”, b) w wierszu „Infrastruktura cyfrowa” w kolumnie trzeciej „Rodzaj podmiotów” po wierszu „Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).” dodaje się wiersz w brzmieniu „Operator strategicznej sieci bezpieczeństwa”;	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
79.	Dział VIIA Prawa Telekomunikacyjnego	**Art. 2.** W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. 2021 r. poz. 576) uchyla się dział VIIA.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie.
80.	Ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowy	**Art. 3.** W ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz.U. z 2020 r. poz. 735 oraz z 2021 r. poz. 159, 255, 1551 i 1561) w art. 13 w ust. 1 w pkt 30 kropkę zastępuje się średnikiem i dodaje się pkt 31 w brzmieniu: „31) podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445).”.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie

	m (Dz.U. z 2020 r. poz. 735 oraz z 2021 r. poz. 159, 255, 1551 i 1561)		
81.	Art. 4 Ustawy zmieniającej	**Art. 4** W ustawie z dnia 11 września 2019 r. Prawo zamówień publicznych, w art. 226 ust. 1 w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu: „19. Obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2020 r. poz. 1369, z 2021 r. poz. 2333 i 2445) oraz usługę ICT lub proces ICT, określone w tej decyzji	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie
82.	Art. 5 ustawy zmieniającej	**Art. 5.** 1. Operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą systemu teleinformatycznego od 1 stycznia 2023 r. 2. Operator usługi kluczowej, któremu została doręczona decyzja o uznaniu za operatora usługi kluczowej po dniu 1 lipca 2022 r., w terminie 6 miesięcy rozpoczyna korzystanie z systemu, o którym mowa w art. 46 ustawy zmienianej w art. 1.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie
83.	Art. 6 Ustawy zmieniającej	**Art. 6.** Do postępowań o udzielenie zamówienia publicznego, wszczętych przed dniem wejścia w życie niniejszej ustawy, , stosuje się przepisy ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.
84.	Art. 7 ustawy zmieniającej	**Art. 7.** 1. Do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK. 2. Agencja Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym do czasu otrzymania informacji o osiągnięciu zdolności operacyjnej przez CSIRT INT, zgłaszają incydenty w podmiocie publicznym do CSIRT GOV.	
85.	Art. 8 ustawy zmieniającej	**Art. 8.** 1. Narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK–PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała. 2. Określone w ust. 1 nabycie narzędzia do uwierzytelnienia dwuskładnikowego nie rodzi zobowiązań podatkowych, z wyjątkiem ewentualnych zobowiązań z zakresu podatku VAT.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.
86.	Art. 9 ustawy zmieniającej	**Art. 9.** 1. Z dniem wejścia w życie ustawy: 1) wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej przed wejściem w życie niniejszej ustawy stają się SOC wewnętrznymi; 2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się SOC zewnętrznymi; 3) sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym staje się CSIRT sektorowym. 2. Podmioty publiczne oraz podmiot, o którym mowa w art. 7 ust. 1 pkt 7 ustawy – Prawo o szkolnictwie wyższym, wyznaczają osoby, o których mowa w art. 21 ustawy zmienianej w art. 1 w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy. 3. Organ właściwy ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy. 4. Organ właściwy do spraw cyberbezpieczeństwa publikuje komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w Dzienniku Urzędowym Monitor Polski. 5. Minister właściwy do spraw informatyzacji powołuje CSIRT Telco w terminie 18 miesięcy od dnia wejścia w życie ustawy.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		6. Minister właściwy do spraw informatyzacji publikuje komunikat o osiągnięciu przez CSIRT Telco zdolności operacyjnej w Dzienniku Urzędowym Monitor Polski. 7. Szef Agencji Wywiadu informuje jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym o osiągnięciu przez CSIRT INT zdolności operacyjnej. 6. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych: 1) urzędu obsługującego Pełnomocnika, 2) zespołów CSIRT GOV, CSIRT MON, CSIRT NASK, – a także jest przekazywana za pomocą systemu informacyjnego, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. 7. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT Telco jest również publikowana na stronach internetowych: 1) urzędu obsługującego Pełnomocnika, 2) zespołów CSIRT GOV, CSIRT MON, CSIRT NASK, 3) Prezesa UKE w tym na stronie podmiotowej Prezesa UKE w Biuletynie Informacji Publicznej, – a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 8. Przedsiębiorca komunikacji elektronicznej: a) do dnia publikacji komunikatu, o którym mowa w ust. 7 zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d, ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa do CSIRT GOV, CSIRT MON albo CSIRT NASK zgodnie z właściwością określoną w art. 26 tej ustawy; b) zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d, ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa do CSIRT Telco od dnia publikacji komunikatu, o którym mowa w ust. 7.	

		9. Do dnia publikacji komunikatu, o którym mowa w ust. 7, w uzgodnieniach, o których mowa w art. 34 ust. 1a oraz 34a ust. 3, nie bierze udziału CSIRT Telco. 10. Operator usługi kluczowej realizuje obowiązki, o których mowa w art. 11 ust. 3 pkt 1–3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej. 11. Operator usługi kluczowej wykonuje po raz pierwszy obowiązek, o którym mowa w art. 9 ust. 2 ustawy zmienianej w art. 1, w terminie 14 dni od dnia wejścia w życie niniejszej ustawy. 12. CSIRT GOV, CSIRT MON lub CSIRT NASK dostosowują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1, do przepisów ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą. 13. Porozumienia w sprawie korzystania z systemu, o którym mowa w art. 46 ustawy zmienianej w art. 1, zawarte przed datą wejścia w życie niniejszej ustawy, zachowują ważność.	
87.	Art. 10 i 14 ustawy zmieniającej	**Art. 10.** Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa w terminie do 1 miesiąca od wejścia w życie ustawy. **Art. 11.** Z dniem … w art. 76t ust. 1–2 ustawy zmienianej w art. 1 otrzymują brzmienie: „1. Prezes UKE, przydziela w drodze przydziału, o którym mowa w art. 72 ust. 1 ustawy Prawo komunikacji elektronicznej, Operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe z zakresu 703–713 MHz oraz 758–768 MHz. Przepisy art. 73–79 ustawy Prawo komunikacji elektronicznej stosuje się odpowiednio. 2. Do decyzji, o której mowa w ust. 1, przepisy art. 68, art 69 ust. 1, art. 80, art. 82, art. 84, art. 85 oraz art. 89 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio. **Art. 12.** Z dniem … art. 76u otrzymuje brzmienie: „Art. 76u 1. Częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz Prezes UKE może przydzielić przedsiębiorcy telekomunikacyjnemu lub konsorcjum	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		przedsiębiorców telekomunikacyjnych w drodze przetargu, o którym mowa w art. 104 ust. 3 ustawy Prawo komunikacji elektronicznej, do świadczenia wyłącznie usług hurtowych. 2. Wśród kryteriów przetargu, o którym mowa w ust. 1, oprócz kryteriów wskazanych w art. 117 ust. 1 ustawy Prawo komunikacji elektronicznej jest zapewnienie przy świadczeniu usług odpowiedniego poziomu bezpieczeństwa oraz niezawodności sieci i usług. 3. Prezes UKE, spośród kryteriów, o których mowa w ust. 2 oraz w art. 117 ust. 1 pkt 1 i 2 ustawy Prawo komunikacji elektronicznej, dokonuje w dokumentacji przetargowej wyboru najistotniejszego kryterium oceny ofert w przetargu, mając na uwadze cele polityki regulacyjnej i stan konkurencji na rynku.”. **Art. 13.** Z dniem … w art. 76f ust. 2 i 3 otrzymują brzmienie: „2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno–rządowym w rozumieniu art. 62 ust. 2 pkt 2 i 3 ustawy z dnia … Prawo komunikacji elektronicznej. Wykorzystanie częstotliwości użytkowanych jako rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3. 3. Wykorzystanie częstotliwości, o których mowa w art. 76t ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 138 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.”. **Art. 14.** Z dniem … w art. 76l ust. 1 otrzymuje brzmienie: „1. Do dostępu, o którym mowa w art. 76j ust. 1 oraz art. 76k ust. 1, stosuje się przepisy art. 169 ust. 1 i 2, art. 170–172, art. 176 ustawy z dnia ... – Prawo komunikacji elektronicznej z zastrzeżeniem, że umowa o tym dostępie jest przekazywana przez Operatora bezpiecznej sieci strategicznej, oraz odpowiednio przepisy działu III rozdziału 3 ustawy z dnia … 2021 r. – Prawo komunikacji elektronicznej.”	

88.	Art. 13	Art. 13.W latach 2022 – 2023 w budżecie państwa tworzy się rezerwę celową na utworzenie i funkcjonowanie CSIRT sektorowych i CSIRT Telco, o których mowa w art. 44 i 44a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.
89.	Art. 14	**Art. 14.** 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – Gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. - 0 zł 2) w 2023 r. – 0 zł 3) w 2024 r. -5,787 mln zł 4) w 2025 r. – 5,977 mln zł 5) w 2026 r. – 6,157 mln zł 6) w 2027 r. – 6,343 mln zł 7) w 2028 r. – 6,534 mln zł 8) w 2029 r. – 6,725 mln zł 9) w 2030 r. – 6,922 mln zł 10) w 2031 r. – 7,124 mln zł 2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – Gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. – 0 zł 2) w 2023 r. – 0 zł 3) w 2024 r. – 5,393 mln zł 4) w 2025 r. – 5,569 mln zł 5) w 2026 r. – 5,736 mln zł 6) w 2027 r. – 5,909 mln zł 7) w 2028 r. – 6,086 mln zł 8) w 2029 r. – 6,263 mln zł 9) w 2030 r. – 6,446 mln zł 10) w 2031 r. – 6,634 mln zł	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. – 10,453 mln zł 2) w 2023 r. – 15,992 mln zł 3) w 2024 r. – 74,690 mln zł 4) w 2025 r. – 71,574 mln zł 5) w 2026 r. – 71,468 mln zł 6) w 2027 r. – 75,964 mln zł 7) w 2028 r. – 80,305 mln zł 8) w 2029 r. – 90,573 mln zł 9) w 2030 r. – 91,433 mln zł 10) w 2031 r. – 84,060 mln zł 4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 - Transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. - 0 zł 2) w 2023 r. – 0 zł 3) w 2024 r. -5,787 mln zł 4) w 2025 r. – 5,977 mln zł 5) w 2026 r. – 6,157 mln zł 6) w 2027 r. – 6,343 mln zł 7) w 2028 r. – 6,534 mln zł 8) w 2029 r. – 6,725 mln zł 9) w 2030 r. – 6,922 mln zł 10) w 2031 r. – 7,124 mln zł 5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 - Zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. – 0 zł 2) w 2023 r. – 0 zł 3) w 2024 r. – 5,787 mln zł 4) w 2025 r. – 5,977 mln zł	

		5) w 2026 r. – 6,157 mln zł 6) w 2027 r. – 6,343 mln zł 7) w 2028 r. – 6,534 mln zł 8) w 2029 r. – 6,725 mln zł 9) w 2030 r. – 6,922 mln zł 10) w 2031 r. – 7,124 mln zł 6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 - Energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 r. – 0 zł 2) w 2023 r. – 0 zł 3) w 2024 r. – 6,168 mln zł 4) w 2025 r. – 6,370 mln zł 5) w 2026 r. – 6,562 mln zł 6) w 2027 r. – 6,760 mln zł 7) w 2028 r. – 6,964 mln zł 8) w 2029 r. – 7,168 mln zł 9) w 2030 r. – 7,378 mln zł 10) w 2031 r. – 7,593 mln zł 7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 59 – Agencja Wywiadu, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi: 1) w 2022 – 6,803 mln zł; 2) w 2023 – 5,856 mln zł; 3) w 2024 – 6,129 mln zł; 4) w 2025 – 6,331 mln zł; 5) w 2026 – 6,523 mln zł; 6) w 2027 – 6,721 mln zł; 7) w 2028 – 6,925 mln zł; 8) w 2029 – 7,129 mln zł; 9) w 2030 – 7,339 mln zł; 10) w 2031 – 7,554 mln zł.	

		8. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętych na dany rok budżetowy maksymalnych limitów wydatków, o których mowa w ust. 1, zostaną zastosowane mechanizmy korygujące polegające na: 1) ograniczeniu finansowania działalności CSIRT sektorowego ; 2) ograniczeniu finansowania działalności CSIRT INT; 3) ograniczeniu finansowania działalności CSIRT Telco. 9. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1, dokonuje minister właściwy do spraw gospodarki morskiej. 10. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1, dokonuje minister właściwy do spraw gospodarki wodnej. 11. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1 i 3, dokonuje minister właściwy do spraw informatyzacji. 12. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1, dokonuje minister właściwy do spraw transportu. 13. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i przynajmniej cztery razy do	

		roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1, dokonuje minister właściwy do spraw zdrowia. 14. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 1, dokonuje minister właściwy do spraw energii. 15. Szef Agencji Wywiadu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 8 pkt 2, dokonuje Szef Agencji Wywiadu w uzgodnieniu ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych.	
90.	Art. 15 – 18 ustawy zmieniającej	Art. 15. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą. 2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1. 3. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 175a ust. 2a ustawy zmienianej w art. 2, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 20a ust. 6 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą. 4. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 175d ustawy zmienianej w art. 2, zachowują moc do dnia wejścia w życie	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa.

		przepisów wykonawczych wydanych na podstawie art. 20d ust. 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą. Art. 16. Postanowienia umów, o których mowa w art. 33 ust. 1c ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, obowiązujących w dniu wejścia w życie ustawy, sprzeczne z art. 33 ust. 1-1d ustawy zmienianej w art. 1 niniejszej ustawy w brzmieniu nadanym tą ustawą, są nieważne. Art. 17. 1.Do czasu osiągnięcia przez Operatora strategicznej sieci bezpieczeństwa pełnej zdolności operacyjnej do świadczenia usług, o których mowa w art. 76g ust. 2 ustawy zmienianej w art. 1 niniejszej ustawy, podmioty, o których mowa w tym przepisie, mogą zawierać umowy na świadczenie usług, o których mowa, także z innymi operatorami telekomunikacyjnymi. 2. Prezes Rady Ministrów podaje do publicznej wiadomości informacje o osiągnięciu pełnej zdolności operacyjnej do świadczenia usług przez Operatora strategicznej sieci bezpieczeństwa. Art. 18. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.	
91.	Załącznik 3	KATEGORIE FUNKCJI KRYTYCZNYCH DLA BEZPIECZEŃSTWA SIECI I USŁUG 1. Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu. 2. Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi. 3. Zarządzanie łącznością ze urządzeniami użytkowników i przydzielanie zasobów radiowych. 4. Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm. 5. Zarządzanie połączeniami ze sprzętem użytkownika i sesjami. 6. Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.	Niniejsza ustawa oprócz implementacji aktu o cyberbezpieczeństwie wprowadza również zmiany związane z Toolboxem 5G, jak również usprawnienia dotyczące funkcjonowania krajowego systemu cyberbezpieczeństwa. Niniejszy przepis nie dotyczy kwestii związanych z aktem o cyberbezpieczeństwie. Wskazane tu zostały najważniejsze funkcje, których będą dotyczyły wcześniej wskazane rozwiązania.

		7. Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników. 8. Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych. 9. Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych. 10. Zabezpieczenia połączeń z innymi sieciami.	

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

zmieniające rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych

Na podstawie art. 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z dnia 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (Dz. U. poz. 1806) w załączniku wprowadza się następujące zmiany:

1) w wierszu „Ochrona zdrowia”:
   a) w kolumnie trzeciej wyrazy „Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia” zastępuje się wyrazami „Jednostka podległa ministrowi właściwemu do spraw zdrowia lub przez niego nadzorowana”,
   b) uchyla się wiersz „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej, w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne”,
   c) uchyla się wiersz „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna, w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne”,
   d) po wierszu „Przedsiębiorca prowadzący działalność gospodarczą polegającą na prowadzeniu apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne" dodaje się wiersz w brzmieniu określonym w załączniku nr 1 do rozporządzenia;

2) w wierszu „Infrastruktura cyfrowa” po wierszu „Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD)” dodaje się wiersz w brzmieniu określonym w załączniku nr 2 do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załączniki
do rozporządzenia
Rady Ministrów
z dnia
(poz.)

Załącznik nr 1

		Jednostka będąca administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym	System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego	a) liczba użytkowników zależnych od usługi kluczowej: nie dotyczy, b) zależność innych sektorów, o których mowa w załączniku nr 1 do ustawy, od usługi świadczonej przez ten podmiot: nie dotyczy, c) wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: nie dotyczy, d) udział podmiotu świadczącego usługę kluczową w rynku: nie dotyczy, e) zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: nie dotyczy, f) zdolność podmiotu do

				utrzymywania wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia: nie dotyczy, g) inne czynniki charakterystyczne dla danego podsektora: zapewnienie dostępu do usługi dla wszystkich usługobiorców

Załącznik nr 2

		Operator strategicznej sieci bezpieczeństwa	Strategiczna sieć bezpieczeństwa	a) liczba użytkowników zależnych od usługi kluczowej: nie dotyczy, b) zależność innych sektorów, o których mowa w załączniku nr 1 do ustawy, od usługi świadczonej przez ten podmiot: nie dotyczy, c) wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne: nie dotyczy, d) udział podmiotu świadczącego usługę kluczową w rynku: nie dotyczy, e) zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent: nie dotyczy, f) zdolność podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi kluczowej

				przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia: nie dotyczy, g) inne czynniki charakterystyczne dla danego podsektora: zapewnienie dostępu do usługi dla wszystkich usługobiorców

UZASADNIENIE

Wykaz usług kluczowych jest wykorzystywany przez organy właściwe do spraw cyberbezpieczeństwa w procesie wydawania decyzji administracyjnych w sprawie uznania za operatora usługi kluczowej przedsiębiorcy bądź podmiotu należącego do jednego z sektorów wymienionych w załączniku do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W trakcie postępowania ww. organy dokonują oceny, czy usługa świadczona przez stronę postępowania znajduje się w załączniku do niniejszego rozporządzenia. W kolejnych krokach w oparciu o stworzony wykaz organy określają, czy świadczenie usługi kluczowej zależy od systemów informacyjnych oraz jaki jest poziom skutku zakłócającego dla świadczonej usługi kluczowej.

Ustawą z dnia … dokonano zmian w załączniku nr 1 do ustawy. Usunięto niektóre rodzaje podmiotów oraz dodano nowe. Zachodzi więc konieczność zmiany rozporządzenia, aby zapewnić jego zgodność ze znowelizowanym tekstem projektu ustawy oraz umożliwić wydanie wobec nowych podmiotów decyzji o uznaniu za operatora usługi kluczowej.

W załączniku do rozporządzenia w wierszu dotyczącym sektora „Ochrona zdrowia" usunięto wiersze dotyczące podmiotów leczniczych, w których przedsiębiorstwie funkcjonuje dział farmacji szpitalnej lub apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.

Wiersz *Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia* otrzymał brzmienie*: Jednostka podległa ministrowi właściwemu do spraw zdrowia lub przez niego nadzorowana*. Za operatora usługi kluczowej mogłaby być uznana każda jednostka podległa lub nadzorowana przez ministra właściwego do spraw zdrowia, która np. zarządza danymi epidemiologicznymi.

Dodano wiersz dotyczący jednostki będącej administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym. Jako usługę kluczową wskazano System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego. Jest to system teleinformatyczny, który umożliwia:

- przyjęcie zgłoszeń alarmowych i powiadomień o zdarzeniach z numerów alarmowych (112, 999);
- dysponowanie zespołów ratownictwa medycznego (ZRM);

- rejestrowanie zdarzeń medycznych;
- lokalizację poszczególnych zdarzeń, miejsc pobytu ZRM i ich statusów na mapie, która stanowi zintegrowany z systemem moduł (Uniwersalny Moduł Mapowy).

Z kolei w sektorze „Infrastruktura cyfrowa" dodano wiersz dotyczący Operatora strategicznej sieci bezpieczeństwa. Jako usługę kluczową wskazano strategiczną sieć bezpieczeństwa, która jest siecią telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stworzoną w celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2023 r. poz. 7022).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowane rozporządzenie nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów zmieniające rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Ustawą z dnia … dokonano zmian w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa. Usunięto niektóre rodzaje podmiotów oraz dodano nowe. Zachodzi więc konieczność zmiany rozporządzenia, aby zapewnić jego zgodność ze znowelizowanym tekstem ustawy oraz umożliwić wydanie wobec nowych podmiotów decyzji o uznaniu za operatora usługi kluczowej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

W załączniku do rozporządzenia w wierszu dotyczącym sektora „Ochrona zdrowia” usunięto wiersze dotyczące podmiotów leczniczych, w których przedsiębiorstwie funkcjonuje dział farmacji szpitalnej lub apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.

Dodano wiersz dotyczący jednostki będącej administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym. Jako usługę kluczową wskazano System Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego. Jest to system teleinformatyczny, który umożliwia:

- przyjęcie zgłoszeń alarmowych i powiadomień o zdarzeniach z numerów alarmowych (112, 999);
- dysponowanie zespołów ratownictwa medycznego (ZRM);
- rejestrowanie zdarzeń medycznych;
- lokalizację poszczególnych zdarzeń, miejsc pobytu ZRM i ich statusów na mapie, która stanowi zintegrowany z systemem moduł (Uniwersalny Moduł Mapowy).

Z kolei w sektorze „Infrastruktura cyfrowa” dodano wiersz dotyczący Operatora strategicznej sieci bezpieczeństwa. Jako usługę kluczową wskazano strategiczną sieć bezpieczeństwa, która jest siecią telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stworzoną w celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Jednostka będąca administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym	1	Wynika z ustawy o Państwowym Ratownictwie Medycznym	Pozytywne. Administrator Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego zostanie wyznaczony na

mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym			operatora usługi kluczowej.
Operator strategicznej sieci bezpieczeństwa - przedsiębiorca telekomunikacyjny, jednoosobowa spółka Skarbu Państwa	1	Wynika to z art. 76d ustawy o krajowym systemie cyberbezpieczeństwa	Pozytywne. Operator zostanie wyznaczony na operatora usługi kluczowej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do konsultacji publicznych oraz opiniowania zgodnie z przepisami Regulaminu prac Rady Ministrów.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Rozporządzenie nie spowoduje skutków finansowych dla jednostek sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z … r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedmiotowy projekt nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.						
	sektor mikro-, małych i średnich przedsiębiorstw	Przedmiotowy projekt nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.						
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt będzie miał pozytywny wpływ na ich funkcjonowanie poprzez lepsze zabezpieczenie kluczowych usług takich jak przekazywanie informacji w systemie ratownictwa medycznego.						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Operator strategicznej sieci bezpieczeństwa oraz administrator Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego będą musieli wypełnić obowiązki dla operatora usługi kluczowej.

9. Wpływ na rynek pracy		
Nałożenie obowiązków na Operator strategicznej sieci bezpieczeństwa oraz administratora Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego może wiązać się z wygenerowaniem nowych miejsc pracy dla specjalistów z zakresu cyberbezpieczeństwa.		
10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☒ zdrowie
Omówienie wpływu	Projekt pozytywnie wpłynie na obszary zdrowia i informatyzacji poprzez objęcie większą ochroną, kluczowych podmiotów.	
11. Planowane wykonanie przepisów aktu prawnego		
Rozporządzenie wejdzie w życie po upływie 14 dni od dnia jego ogłoszenia.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
W związku z charakterem wprowadzanych zmian nie jest konieczna ewaluacja skutków projektu.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
Brak		

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

zmieniające rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej

Na podstawie art. 10 ust. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2023 r. poz. 913 i …) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (Dz. U. poz. 2080) zarządza się następujące zmiany:

1) w tytule rozporządzenia wyrazy „cyberbezpieczeństwa systemu informacyjnego” zastępuje się wyrazami „bezpieczeństwa systemu informacyjnego”;
2) w § 1 wyrazy „cyberbezpieczeństwa systemu informacyjnego” zastępuje się wyrazami „bezpieczeństwa systemu informacyjnego”.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

UZASADNIENIE

Wskutek zmian dokonanych nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa nastąpiła konieczność uspójnienia treści rozporządzenia Rady Ministrów z dnia 16 października 2018 r. *w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej* nową siatką pojęciową.

W ustawie dotychczasowe pojęcie „cyberbezpieczeństwa" zostało zastąpione „bezpieczeństwem systemów informacyjnych" przy zachowaniu tego samego znaczenia normatywnego. Z tego powodu w rozporządzeniu dokonuje się zmian, polegających na zamianie pojęcia „cyberbezpieczeństwa systemu informacyjnego" na „bezpieczeństwa systemu informacyjnego".

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2023 r. poz. 702).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projektowane rozporządzenie nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny" oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów zmieniające rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 10 ust. 5 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ……) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W ustawie o krajowym systemie cyberbezpieczeństwa dotychczasowe pojęcie „cyberbezpieczeństwa" zostało zastąpione „bezpieczeństwem systemów informacyjnych" przy zachowaniu tego samego znaczenia normatywnego. Z tego powodu w rozporządzeniu dokonuje się zmian, polegających na zamianie pojęcia „cyberbezpieczeństwa systemu informacyjnego" na „bezpieczeństwa systemu informacyjnego". W związku z tym konieczne było ujednolicenie terminologii w aktach wykonawczych do tej ustawy.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Ujednolicenie terminologii wykorzystywanej w ustawie o krajowym systemie cyberbezpieczeństwa oraz w aktach wykonawczych do niej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Operatorzy usług kluczowych	396	Wykaz operatorów usług kluczowych	Konieczność dostosowania terminologii w dokumentacji.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do konsultacji publicznych i opiniowania zgodnie z przepisami Regulaminu pracy Rady Ministrów, w tym projekt zostanie skonsultowany z organizacjami zrzeszającymi operatorów usług kluczowych.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2023 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0

budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wprowadzone zmiany nie spowodują skutków finansowych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą musieli dostosować terminologię używaną w dokumentacji do zmian w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą musieli dostosować terminologię używaną w dokumentacji do zmian w rozporządzeniu.						
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt nie będzie miał wpływu na funkcjonowanie rodzin, obywateli i gospodarstw domowych.						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☒ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:

Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy
Projekt nie zmienia obciążeń regulacyjnych.	

9. Wpływ na rynek pracy
Projekt nie wpływa na rynek pracy.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Projekt nie wpływa na pozostałe obszary.

11. Planowane wykonanie przepisów aktu prawnego
Rozporządzenie wejdzie w życie po upływie 14 dni od dnia jego ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
W związku z charakterem wprowadzanych zmian nie jest konieczna ewaluacja skutków projektu.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia

w sprawie minimalnych środków technicznych i organizacyjnych jakie mają obowiązek stosować przedsiębiorcy telekomunikacyjni dostarczający sieć piątej generacji (5G) celem zapewnienia jej bezpieczeństwa

Na podstawie art. 20a ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …) zarządza się, co następuje:

§ 1. Rozporządzenie określa minimalny zakres środków technicznych i organizacyjnych, zwanych dalej „środkami", o których mowa w art. 20a ust. 2 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …), jakie mają obowiązek stosować przedsiębiorcy telekomunikacyjni dostarczający sieć piątej generacji (5G), określoną w dokumencie technicznym - Raporcie ETSI TR 121 915 V.15.0.0. (2019-10) lub dokumencie go zastępującym, celem zapewnienia bezpieczeństwa tej sieci.

§ 2. Przedsiębiorca telekomunikacyjny dostarczający sieć piątej generacji (5G)**:**

1) opracowuje i aktualizuje dokumentację dotyczącą bezpieczeństwa sieci lub usług komunikacji elektronicznej zawierającą opis środków, o których mowa w pkt 2-15;
2) opracowuje i aktualizuje wykaz elementów infrastruktury telekomunikacyjnej i systemów teleinformatycznych w których wystąpienie incydentu telekomunikacyjnego będzie miało istotny wpływ na funkcjonowanie sieci lub usług o znaczeniu kluczowym dla funkcjonowania przedsiębiorcy, zwanych dalej „kluczową infrastrukturą";
3) identyfikuje zagrożenia bezpieczeństwa sieci lub usług komunikacji elektronicznej;
4) ocenia prawdopodobieństwo wystąpienia oddziaływania zagrożeń na bezpieczeństwo sieci lub usług komunikacji elektronicznej;
5) zapewnia i stosuje środki minimalizujące skutki wystąpienia oddziaływań zagrożeń na bezpieczeństwo sieci lub usług komunikacji elektronicznej;

[1)] Minister Cyfryzacji kieruje działem administracji rządowej - informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 792).

6) ustanawia zasady i procedury dostępu do kluczowej infrastruktury i przetwarzanych danych, obejmujące przypisanie odpowiedzialności za kluczową infrastrukturę w zakresie odpowiednim do realizowanych zadań;
7) zabezpiecza dostęp do kluczowej infrastruktury, monitoruje ten dostęp i wskazuje środki reagowania na nieuprawniony dostęp lub próbę takiego dostępu;
8) ustanawia zasady bezpiecznego zdalnego przetwarzania danych;
9) stosuje, wynikające z oceny prawdopodobieństwa wystąpienia oddziaływania zagrożeń, środki zabezpieczające dla poszczególnych kategorii danych;
10) zawierając umowy mające istotny wpływ na funkcjonowanie sieci lub usług komunikacji elektronicznej, identyfikuje zagrożenia dla bezpieczeństwa tych sieci lub usług, związane z zawieranymi umowami;
11) zapewnia monitorowanie i dokumentowanie funkcjonowania sieci i usług komunikacji elektronicznej mające na celu wykrycie incydentu telekomunikacyjnego, i ustalenie przyczyn takiego incydentu telekomunikacyjnego;
12) ustala wewnętrzne procedury zgłaszania incydentów telekomunikacyjnych, oraz umożliwia użytkownikom końcowym dokonywanie zgłoszeń wszelkich incydentów telekomunikacyjnych;
13) przeprowadza analizę bezpieczeństwa sieci lub usług komunikacji elektronicznej:
    a) co najmniej raz na dwa lata,
    b) po każdym:
        – wykrytym poważnym incydencie telekomunikacyjnym, oraz
        – wykryciu podatności zwiększającej poziom ryzyka wystąpienia poważnego incydentu telekomunikacyjnego, w zakresie objętym wykrytą podatnością.
14) stosuje strategię skutkującą brakiem uzależnienia się od jednego producenta poszczególnych elementów sieci telekomunikacyjnej przy jednoczesnym zapewnieniu interoperacyjności usług;
15) zapewnia podwyższanie odporności na zakłócenia sieci i usług komunikacji elektronicznej.

2. Przedsiębiorca telekomunikacyjny prowadzi dokumentację działań, o których mowa w ust. 1.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

UZASADNIENIE

Niniejsze rozporządzenie stanowi wykonanie upoważnienia ustawowego z art. 20a ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Ustanawia ono minimalne środki techniczne i organizacyjne, które mają obowiązek stosować przedsiębiorcy telekomunikacyjni dostarczający sieć 5G.

Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowane rozporządzenie nie wpływa na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Stosownie do postanowień § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) oraz zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2023 r. poz. 702).

Projekt rozporządzenia nie wymaga uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia z właściwymi instytucjami i organami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

w sprawie w sprawie progów uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny

z dnia

Na podstawie art. 20d ust. 3 ustawy z dnia ……. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) zarządza się, co następuje:

§ 1. Przedsiębiorca komunikacji elektronicznej uznaje incydent telekomunikacyjny za poważny incydent telekomunikacyjny w przypadku, gdy zostało spełnione co najmniej jedno z poniższych kryteriów:

1) incydent telekomunikacyjny dotyczył on co najmniej 10 000 użytkowników danej usługi i skutkuje naruszeniem dostępności, autentyczności, integralności lub poufności sieci lub usług komunikacji elektronicznej, innych usług związanych lub dostępnych za ich pośrednictwem lub przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej:
   a) od 1 do 2 godzin, gdy incydent telekomunikacyjny miał wpływ na więcej niż 15% użytkowników danej usługi,
   b) powyżej 2 do 4 godzin, gdy incydent telekomunikacyjny miał wpływ na więcej niż 10% użytkowników danej usługi,
   c) powyżej 4 do 6 godzin, gdy incydent telekomunikacyjny miał wpływ na więcej niż 5% użytkowników danej usługi,
   d) powyżej 6 do 8 godzin, gdy incydent telekomunikacyjny miał wpływ na więcej niż 2% użytkowników danej usługi,
   e) powyżej 8 godzin, gdy incydent telekomunikacyjny miał wpływ na więcej niż 1% użytkowników danej usługi;

[1)] Minister Cyfryzacji kieruje działem administracji rządowej - informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 792).

2) incydent telekomunikacyjny skutkował niedostępnością numerów alarmowych i liczba użytkowników danego przedsiębiorcy komunikacji elektronicznej pozbawionych możliwości wykonywania połączeń z numerami alarmowymi przekroczyła:
   a) 10 000 przez co najmniej 15 minut lub
   b) 100 000;
3) incydent telekomunikacyjny miał wpływ na zachowanie tajemnicy telekomunikacyjnej dotyczącej co najmniej 100 użytkowników;
4) obszar dotknięty incydentem telekomunikacyjnym przekroczył obszar jednego powiatu, z wyłączeniem miast na prawach powiatu, w rozumieniu ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym;
5) incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz.122);
6) incydent telekomunikacyjny uniemożliwia wykonywanie obowiązków przedsiębiorcy komunikacji elektronicznej z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

UZASADNIENIE

Rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 20d ust. 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projektowany akt zastąpi rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług i co do zasady powtarza ono jego postanowienia, dostosowując je do terminologii używanej w ustawie o krajowym systemie cyberbezpieczeństwa.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia nie jest sprzeczny z prawem Unii Europejskiej.

Projektowane rozporządzenie nie dotyczy majątkowych praw i obowiązków przedsiębiorców lub praw i obowiązków przedsiębiorców wobec organów administracji publicznej.

Projektowane rozporządzenie nie wpływa na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Stosownie do postanowień § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) oraz zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt rozporządzenia zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2023 r. poz. 702).

Projekt rozporządzenia nie wymaga uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia z właściwymi instytucjami i organami Unii Europejskiej, w tym Europejskim Bankiem Centralnym.

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie w sprawie progów uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji, **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 20d ust. 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z dołączeniem do krajowego systemu cyberbezpieczeństwa przedsiębiorców telekomunikacyjnych i wprowadzeniem pojęcia incydentu telekomunikacyjnego konieczne było wprowadzenie progów uznania takiego incydentu za poważny incydent telekomunikacyjny. Rozporządzenie to zastępuje dotychczasowe Rozporządzenie Ministra Cyfryzacji z dnia 20 września 2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie wskazuje progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Przedsiębiorcy telekomunikacyjni	3868	Rejestr przedsiębiorców telekomunikacyjnych[1]	Wskazanie progów klasyfikacji incydentów telekomunikacyjnych jako poważnych incydentów telekomunikacyjnych.
Podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów	Brak danych	-	Wskazanie progów klasyfikacji incydentów telekomunikacyjnych jako poważnych incydentów telekomunikacyjnych.
Prezes Urzędu Komunikacji Elektronicznej	1	Informacja ogólnodostępna	Prezes Urzędu Komunikacji Elektronicznej będzie nadzorował przedsiębiorców komunikacji elektronicznej

1) https://bip.uke.gov.pl/rpt/ stan na dzień 28.02.2023 r.

			w zakresie realizowania obowiązków zapewniania bezpieczeństwa sieci i usług komunikacji elektronicznej. Będzie obowiązany do utworzenia CSIRT Telco działającego na rzecz przedsiębiorców komunikacji elektronicznej, do którego będą zgłaszane poważne incydenty telekomunikacyjne.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do uzgodnień i opiniowania zgodnie z regulaminem prac Rady Ministrów.

Projekt zostanie również przekazany w ramach konsultacji publicznych do organizacji zrzeszających przedsiębiorców komunikacji elektronicznej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wprowadzone zmiany nie spowodują skutków finansowych w sektorze finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z … r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedmiotowy projekt precyzuje jakie incydenty telekomunikacyjne przedsiębiorcy komunikacji elektronicznej będą obowiązani zgłaszać do CSIRT Telco.						
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt służy zapewnieniu bezpieczeństwa i ciągłości świadczenia usług telekomunikacyjnych.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Projekt precyzuje jakie dokładnie incydenty telekomunikacyjne będą stanowić poważne incydenty telekomunikacyjne, które podlegają zgłoszenie do CSIRT Telco. CSIRT Telco będzie mógł udzielić wsparcia takiemu przedsiębiorcy tak aby jak najsprawniej obsłużyć dany incydent telekomunikacyjny.

9. Wpływ na rynek pracy

Projekt nie wpływa na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozporządzenie przyczyni się do wzrostu bezpieczeństwa usług telekomunikacyjnych.
11. Planowane wykonanie przepisów aktu prawnego	
Rozporządzenie wejdzie w życie z upływem 14 dni od dnia jego ogłoszenia.	
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?	
Regularnie monitorowana będzie liczba zgłoszonych poważnych incydentów telekomunikacyjnych a także przyczyny ich wystąpienia	
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)	
Brak	

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie sposobu niszczenia materiałów zawierających informacje uzyskane w wyniku przeprowadzonej przez zespoły CSIRT oceny bezpieczeństwa oraz wzoru protokołu i trybu pracy komisji

Na podstawie art. 36g ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ……) zarządza się, co następuje:

§ 1. Rozporządzenie określa:

1) sposób niszczenia materiałów zawierających informacje, o których mowa w art. art. 36e ust. 6 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zwanych dalej „materiałami”;
2) wzór protokołu wymaganego przy niszczeniu materiałów;
3) tryb pracy komisji.

§ 2. Użyte w rozporządzeniu sformułowanie CSIRT oznacza zespół CSIRT przeprowadzający ocenę bezpieczeństwa, o której mowa w art. 36d ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

§ 3. 1. Zniszczenie materiałów zarządza kierownik podmiotu prowadzącego CSIRT, niezwłocznie po zakończeniu oceny bezpieczeństwa.

2. Kierownik podmiotu prowadzącego CSIRT powołuje trzech członków komisji biorących udział w niszczeniu materiałów.

3. W skład komisji, o której mowa w ust. 2, wchodzą wyłącznie pracownicy, funkcjonariusze lub żołnierze CSIRT przeprowadzającego ocenę bezpieczeństwa.

§ 4. 1. Zniszczenia materiałów dokonuje się przez:

1) trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, na których informacje zostały utrwalone, w sposób uniemożliwiający odtworzenie treści tych zapisów;
2) fizyczne zniszczenie materiałów i dokumentów sporządzonych na ich podstawie, za pomocą urządzeń niszczących w sposób uniemożliwiający ich ponowne odczytanie.

2. Trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, o którym mowa w ust. 1 pkt 1, jest wykonywane przez co najmniej siedmiokrotne nadpisanie całej przestrzeni tych nośników lub ich kopii dowolnym jawnym ciągiem bajtów.

3. W przypadku gdy trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, o którym mowa w ust. 1 pkt 1, nie jest możliwe, nośniki te lub ich kopie uszkadza się w sposób uniemożliwiający ich odczytanie albo dokonuje się ich fizycznego zniszczenia.

§ 5. Protokół zniszczenia materiałów, zatwierdzony przez kierownika podmiotu prowadzącego CSIRT przeprowadzającej ocenę bezpieczeństwa, jest sporządzany w jednym egzemplarzu, który pozostaje w komórce organizacyjnej dokonującej zniszczenia.

§ 6. 1. Wzór zarządzenia o zniszczeniu materiałów jest określony w załączniku nr 1 do rozporządzenia.

2. Wzór protokołu komisyjnego zniszczenia materiałów jest określony w załączniku nr 2 do rozporządzenia.

§ 7. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

PREZES RADY MINISTRÓW

Załączniki
do rozporządzenia
Rady Ministrów
z dnia

Załącznik nr 1

WZÓR ZARZĄDZENIA O ZNISZCZENIU MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE UZYSKANE W WYNIKU PRZEPROWADZENIA OCENY BEZPIECZEŃSTWA

…… *Pieczęć*

…… *(klauzula tajności po wypełnieniu)*

…… *Znak sprawy*

…… *miejscowość i data*

Zarządzenie nr ……

Na podstawie art. 32a ust. 9 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ……)

ZARZĄDZAM USUNIĘCIE INFORMACJI / ZNISZCZENIE MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE / ZNISZCZENIE DOKUMENTÓW SPORZĄDZONYCH NA PODSTAWIE INFORMACJI UTRWALONYCH NA INFORMATYCZNYCH NOŚNIKACH DANYCH[1)]

uzyskane/ych w wyniku przeprowadzania oceny bezpieczeństwa w okresie od.....do..... w sprawie nr .....
(numer sprawy)

prowadzonej przez na podstawie zarządzenia nr ..... z dnia.....

W celu realizacji przedmiotowego zarządzenia powołuję komisję w składzie:

1. .....
2. .....
3. .....

[1)] Niepotrzebne skreślić.

KIEROWNIK PODMIOTU
PROWADZĄCEGO CSIRT

……

(klauzula tajności po wypełnieniu)

Załącznik nr 2

WZÓR PROTOKOŁU ZNISZCZENIA MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE UZYSKANE W WYNIKU PRZEPROWADZENIA OCENY BEZPIECZEŃSTWA

…… ……
Pieczęć *(klauzula tajności po wypełnieniu)*

…… ……
Znak sprawy *miejscowość i data*

Egzemplarz pojedynczy

PROTOKÓŁ ZNISZCZENIA MATERIAŁÓW ZAWIERAJĄCYCH INFORMACJE UZYSKANE W WYNIKU PRZEPROWADZENIA OCENY BEZPIECZEŃSTWA

Komisja powołana na podstawie zarządzenia nr .....z dnia ..... w składzie:

1. .....
2. .....
3. .....

w dniu dokonała usunięcia zapisów informacji uzyskanych / zniszczenia materiałów zawierających informacje uzyskane / zniszczenia dokumentów sporządzonych na podstawie informacji utrwalonych na nośnikach uzyskanych* w wyniku przeprowadzenia oceny bezpieczeństwa prowadzonej przez ..... w okresie od..... do ..... .

Wykaz zniszczonych informacji / materiałów / dokumentów:

.....
.....
.....
.....
.....
.....

Numer strony/liczba stron

……

(klauzula tajności po wypełnieniu)

*) Niepotrzebne skreślić.

……..

(klauzula tajności po wypełnieniu)

.....

.....

.....

.....

.....

.....

Podpisy członków komisji:

1. .....
2. .....
3. .....

KIEROWNIK PODMIOTU

PROWADZĄCEGO CSIRT

Wykonano w egz. pojedynczym:

Wykonał: ……

numer strony/liczba stron

……..

(klauzula tajności po wypełnieniu)

UZASADNIENIE

Projekt rozporządzenia stanowi wykonanie upoważnienia ustawowego zawartego z art. 36g ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, zgodnie z którym Rada Ministrów określi, w drodze rozporządzenia sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36e ust. 6 przywołanej ustawy, a także może określić wzory niezbędnych druków, mając na uwadze rodzaj materiałów podlegających zniszczeniu.

W § 4 projektu wskazano, iż niszczenie materiałów odbywa się w sposób komisyjny i protokolarny. Zniszczenie materiałów zarządza kierownik podmiotu prowadzącego zespół CSIRT, niezwłocznie po zakończeniu oceny bezpieczeństwa. Jednocześnie w projekcie określono sposoby niszczenia materiałów, mając na względzie rodzaj materiału podlegającego zniszczeniu. W związku z powyższym, wskazano, iż zniszczenia materiałów dokonuje się poprzez:

1) trwałe usunięcie zapisów informacji utrwalonych na informatycznych nośnikach danych lub ich kopiach, na których informacje zostały utrwalone, w sposób uniemożliwiający odtworzenie treści tych zapisów;
2) fizyczne zniszczenie materiałów i dokumentów sporządzonych na ich podstawie, za pomocą urządzeń niszczących w sposób uniemożliwiający ich ponowne odczytanie.

Dodatkowo w projekcie przewidziano rozwiązanie w sytuacji, gdy usunięcie z nośników utrwalonych na nich zapisów nie jest możliwe. W takim przypadku nośniki winne zostać uszkodzone w sposób uniemożliwiający ich odczytanie albo fizycznie zniszczone.

W załączniku nr 1 do rozporządzenia określono wzór formularza zarządzenia kierownika podmiotu prowadzącego CSIRT o zniszczeniu materiałów zawierających informacje uzyskane w wyniku przeprowadzenia oceny bezpieczeństwa. Z kolei w załączniku nr 2 do rozporządzenia określono wzór formularza protokołu zniszczenia materiałów zawierających informacje uzyskane w wyniku przeprowadzenia oceny bezpieczeństwa.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Projekt nie był przedstawiany instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, celem uzyskania opinii, dokonania konsultacji albo uzgodnienia, ponieważ przepisy przedmiotowego projektu rozporządzenia pozostają poza zakresem prawa Unii Europejskiej.

Projekt będzie podlegał udostępnieniu na stronie podmiotowej Ministra Cyfryzacji w Biuletynie Informacji Publicznej, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 384) projekt będzie podlegał także udostępnieniu w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Przedmiot projektowanej regulacji pozostaje poza zakresem prawa Unii Europejskiej.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie sposobu niszczenia materiałów zawierających informacje uzyskane w wyniku przeprowadzonej przez zespoły CSIRT oceny bezpieczeństwa oraz wzoru protokołu i trybu pracy komisji **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji, **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 36g ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Wprowadzone zmiany w ustawie o krajowym systemie cyberbezpieczeństwa w zakresie przeprowadzania oceny bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa sprawiły, że zespoły CSIRT poziomu krajowego będą mogły uzyskiwać dostęp do informacji prawnie chronionych podmiotów, których bezpieczeństwo jest badane. Ze względu na potencjalnie wrażliwy charakter tych informacji, konieczne jest ustanowienie jasnych procedur zniszczenia takich informacji tak aby nikt nieuprawniony nie mógł uzyskać do nich dostępu.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Przyjęcie prostych zasad postępowania w zakresie niszczenia informacji uzyskanych w ramach badania bezpieczeństwa. W związku z tym, wskazano, iż niszczenie materiałów odbywa się w sposób komisyjny i protokolarny. Zniszczenie materiałów zarządza kierownik podmiotu prowadzącego zespół CSIRT, niezwłocznie po zakończeniu oceny bezpieczeństwa. Jednocześnie w projekcie określono sposoby niszczenia materiałów, mając na względzie rodzaj materiału podlegającego zniszczeniu.

Dodatkowo w projekcie przewidziano rozwiązanie w sytuacji, gdy usunięcie z nośników utrwalonych na nich zapisów nie jest możliwe. W takim przypadku nośniki winne zostać uszkodzone w sposób uniemożliwiający ich odczytanie albo fizycznie zniszczone.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Zespoły CSIRT poziomu krajowego – CSIRT GOV, CSIRT MON, CSIRT NASK	3	Informacje ogólnodostępne	Pozytywne. Określa jasny sposób postępowania z pozyskanymi w ramach oceny bezpieczeństwa wrażliwymi informacjami.
CSIRT Telco	1	Informacje ogólnodostępne	
CSIRT sektorowy	7	Informacje ogólnodostępne	
CSIRT INT	1	Informacje ogólnodostępne	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do konsultacji publicznych i opiniowania zgodnie z przepisami Regulaminu pracy Rady Ministrów, w tym projekt zostanie skonsultowany z organizacjami zrzeszających podmioty krajowego systemu cyberbezpieczeństwa.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Rozporządzenie nie spowoduje skutków finansowych dla sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedmiotowy projekt nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo						

		przedsiębiorców (Dz. U. z 2023 r. poz. 221).
	sektor mikro-, małych i średnich przedsiębiorstw	Przedmiotowy projekt nie określa zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej, w związku z czym odstąpiono od analiz i oceny przewidywanych skutków społeczno-gospodarczych, wskazanych w art. 66 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt nie będzie miał wpływu na funkcjonowanie rodzin, obywateli i gospodarstw domowych.
Niemierzalne		
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

Projekt przewiduje wprowadzenie dodatkowej procedury z której przeprowadzenia będzie sporządzany protokół. Jest to niezbędny dla zagwarantowania, że wszystkie wrażliwe informacje pozyskane w ramach oceny bezpieczeństwa zostaną usunięte.

9. Wpływ na rynek pracy

Projekt nie wpływa na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Projekt ma pozytywny wpływ na cyberbezpieczeństwo gdyż gwarantuje podmiotom poddającym się ocenie bezpieczeństwa, że ich wrażliwe informacje nie będą wykorzystane przeciwko nim.

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia jego ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
Ewaluacja będzie przeprowadzana w przypadku zgłoszenia przez zespoły CSIRT postulatów w zakresie wprowadzonej procedury.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Brak

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie krajowego programu certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT

Na podstawie art. 59d ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ….) zarządza się, co następuje:

§ 1. Ustanawia krajowy program certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT, zwany dalej „programem”.

§ 2. Krajowy program certyfikacji cyberbezpieczeństwa obejmuje następujące produkty ICT:

1) ……;
2) ...…….;
3) …… .

§ 3. W celu uzyskania certyfikatu odwołującego się do krajowego poziomu uzasadnienia zaufania podstawowy produkt ICT należy:

1) ……;
2) ……;
3) …… .

§ 4. W celu uzyskania certyfikatu odwołującego się do krajowego poziomu uzasadnienia zaufania istotny produkt ICT należy:

1) ……;
2) …….;
3) ……. .

§ 5. W celu uzyskania certyfikatu odwołującego się do krajowego poziomu uzasadnienia zaufania istotny produkt ICT należy:

1) ……;
2) ……;
3) …… .

§ 6. Na potrzeby niniejszego rozporządzenia dokumentację techniczną produktu ICT stanowią:

1) ……;
2) ……;
3) …… .

§ 7. W celu wykazania, że produkt ICT spełnia wymagania odwołujące się do poziomu uzasadnienia zaufania podstawowy należy:

1) ……;
2) ……;
3) …… .

§ 8. W celu wykazania, że produkt ICT spełnia wymagania odwołujące się do poziomu uzasadnienia zaufania istotny należy:

1) ……;
2) ……;
3) …… .

§ 9. W celu wykazania, że produkt ICT spełnia wymagania odwołujące się do poziomu uzasadnienia zaufania wysoki należy:

1) ……;
2) ……;
3) …… .

§ 10. 1. Dokumentacje techniczną w rozumieniu niniejszego rozporządzenia stanowią:

1) ……;
2) ……;
3) …… .

2. Elementy dokumentacji technicznej zawierające informacje mogące wpłynąć na jego zdolność do zapewniania ochrony przed cyberzagrożeniami muszą być przechowywane w sposób uniemożliwiający zapoznania się z nimi osobom nieupoważnionym.

3. Dokumentacja techniczna przechowywana jest przez cały okres ważności certyfikatu.

§ 11. 1. Dostawca przekazuje do jednostki oceniającej zgodność, która wydała certyfikat, wszystkie informacje mogące mieć wpływ na spełnienie przez dany produkt wymagań określonych w programie.

2. Przez cały okres ważności certyfikatu jednostka oceniająca zgodność ma dostęp do dokumentacji technicznej produktu ICT.

§ 12. 1. Certyfikat wydawany jest na okres 5 lat.

2. Certyfikat może zostać przedłużony na następne 5 lat, w przypadku gdy produkt ICT dla którego został wydany wciąż spełnia odpowiednie wymagania.

§ 13. Wzór certyfikatu jest określony w załączniku nr 1 do rozporządzenia.

§ 14. 1.W ramach krajowego programu certyfikacji cyberbezpieczeństwa ….. dla krajowego poziomu uzasadnienia zaufania podstawowy dozwolone jest wydawanie krajowej deklaracji zgodności.

2. Sporządzana deklaracja zgodności jest udostępniona publicznie przez cały okres na jaki została wydana.

3. Wzór krajowej deklaracji zgodności jest określony w załączniku nr 2 do rozporządzenia.

§ 15. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia

PREZES RADY MINISTRÓW

Załączniki
do rozporządzenia
Rady Ministrów
z dnia
(poz.)

Załącznik nr 1

Wzór Certyfikatu

Załącznik nr 2

Wzór Krajowej Deklaracji Zgodności

UZASADNIENIE

Projektowany akt stanowi wykonanie delegacji ustawowej zawartej w art. 59d ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 ….), która upoważnia Radę Ministrów do określenia w drodze rozporządzenia krajowego programu certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT, zawierającego: wskazanie, czy w ramach programu jest dozwolone wydanie deklaracji zgodności, dokumentację techniczną i sposób jej przechowywania, treść i wzór graficzny krajowych certyfikatów cyberbezpieczeństwa i krajowych deklaracji zgodności okres dostępności krajowych deklaracji zgodności, dokumentacji technicznej oraz innych istotnych informacji, szczegółowe wymagania z zakresu cyberbezpieczeństwa odpowiadające poszczególnym krajowym poziomom uzasadnienia zaufania, szczegółowe metody stosowane w celu wykazania, że zostały spełnione wymagania odpowiadające określonemu krajowemu poziomowi uzasadnienia zaufania, sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymaganiami krajowych certyfikatów cyberbezpieczeństwa lub deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymaganiami cyberbezpieczeństwa, warunki wydawania, utrzymywania, przedłużania i odnawiania ważności certyfikatów.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Projekt nie był przedstawiany instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, celem uzyskania opinii, dokonania konsultacji albo uzgodnienia, ponieważ przepisy przedmiotowego projektu rozporządzenia pozostają poza zakresem prawa Unii Europejskiej.

Projekt będzie podlegał udostępnieniu na stronie podmiotowej Ministra Cyfryzacji w Biuletynie Informacji Publicznej, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 384) projekt będzie podlegał także udostępnieniu

w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Przedmiot projektowanej regulacji pozostaje poza zakresem prawa Unii Europejskiej.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie e krajowego programu certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji, **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 59d ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W celu zwiększenia cyberbezpieczeństwa urządzeń wykorzystywanych powszechnie w branży IT oraz promocji najlepszych standardów w dziedzinie cyberbezpieczeństwa Rada Ministrów przyjmuje rozporządzenie ustanawiające krajowy program certyfikacji cyberbezpieczeństwa dla….

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie ustanawia krajowy program certyfikacji cyberbezpieczeństwa ….

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do uzgodnień i opiniowania zgodnie z przepisami Regulaminu pracy Rady Ministrów.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0-10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0

Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wprowadzone zmiany nie spowodują skutków finansowych w sektorze finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt służy zapewnieniu bezpieczeństwa i ciągłości świadczenia usług telekomunikacyjnych.						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Projekt ustanawia krajowy program certyfikacji cyberbezpieczeństwa ….	

9. Wpływ na rynek pracy

Projekt nie wpływa na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozporządzenie przyczyni się do wzrostu bezpieczeństwa usług telekomunikacyjnych.

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie wejdzie w życie z upływem 14 dni od dnia jego ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak

Projekt

ROZPORZĄDZENIE

MINISTRA CYFRYZACJI[1)]

z dnia

w sprawie wzoru protokołu pobrania próbki produktu ICT do badań

Na podstawie art. 59zb ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ……) zarządza się, co następuje:

§ 1. Rozporządzenie określa wzór protokołu pobrania próbki produktu ICT do badań.

§ 2. Wzór protokołu, o którym mowa w ust. 1, jest określony w załączniku do rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

[1)] Minister Cyfryzacji kieruje działem administracji rządowej - informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 26 kwietnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 792).

Załącznik
do rozporządzenia
Ministra Cyfryzacji
z dnia
(poz.)

Wzór

Protokołu pobrania próbki produktu ICT do badań

UZASADNIENIE

Niniejsze rozporządzenie stanowi wykonanie delegacji ustawowej z art. 59zb ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i ……) i określa wzór protokołu pobrania próbki produktu ICT do badań. Projektowane rozwiązania zostały przyjęte w celu umożliwienia identyfikacji próbki produktu ICT oraz zapewnienia jednolitości i przejrzystości protokołów, a także transparentności procesów kontrolnych.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt nie podlega notyfikacji zgodnie z trybem przewidzianym w przepisach dotyczących sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, ponieważ nie zawiera przepisów technicznych.

Projekt nie był przedstawiany instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, celem uzyskania opinii, dokonania konsultacji albo uzgodnienia, ponieważ przepisy przedmiotowego projektu rozporządzenia pozostają poza zakresem prawa Unii Europejskiej.

Projekt będzie podlegał udostępnieniu na stronie podmiotowej Ministra Cyfryzacji w Biuletynie Informacji Publicznej, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Zgodnie z § 52 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 384) projekt będzie podlegał także udostępnieniu w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Przedmiot projektowanej regulacji pozostaje poza zakresem prawa Unii Europejskiej.

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie wzoru protokołu pobrania próbki produktu ICT do badań **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Janusz Cieszyński – Minister Cyfryzacji, **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, e-mail: sekretariat.dc@mc.gov.pl	**Data sporządzenia** 29.05.2023 **Źródło** upoważnienie ustawowe z art. 59zb ust. 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i …..) **Nr w Wykazie prac**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W celu umożliwienia identyfikacji próbki produktu ICT oraz zapewnienia jednolitości i przejrzystości protokołów, a także transparentności procesów kontrolnych.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozporządzenie wydawane jest w celu umożliwienia identyfikacji próbki produktu ICT oraz zapewnienia jednolitości i przejrzystości protokołów, a także transparentności procesów kontrolnych.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Z uwagi na szczegółowość regulacji odstąpiono od analizy prawno-porównawczej projektu na tle innych państw.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do konsultacji publicznych i opiniowania zgodnie z przepisami Regulaminu pracy Rady Ministrów, w tym zostanie skonsultowany z organizacjami zrzeszających przedsiębiorców komunikacji elektronicznej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2022 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0

JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	**0**	**0**	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
Fundusz Cyberbezpieczeństwa	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Wprowadzone zmiany nie spowodują skutków finansowych w sektorze finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z … r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe, osoby starsze i niepełnosprawne	Projekt służy zapewnieniu bezpieczeństwa i ciągłości świadczenia usług telekomunikacyjnych.						
Niemierzalne								

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy
Projekt wzór protokołu pobrania próbki produktu ICT do badań.	

9. Wpływ na rynek pracy

Projekt nie wpływa na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozporządzenie przyczyni się do wzrostu bezpieczeństwa usług telekomunikacyjnych.

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie wejdzie w życie z upływem 14 dni od dnia jego ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak

Wykaz podmiotów, które zgłosiły zainteresowanie pracami nad projektem **ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UD68),** w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa – w kolejności wpływu zgłoszeń.

Lp.	Nazwa podmiotu	Data wpływu zgłoszenia
1.	Jarosław Rostek, „EXCOGITATE" Sp. z o. o.	29.09.2020 r.
2.	Marcin Kuś, „Signum Edward Kuś"	30.09.2020 r.
3.	Rafał Górski, „Loopus Górski Opęchowski" sp.j	12.10.2020 r.

WZÓR URZĘDOWEGO FORMULARZA ZGŁOSZENIA ZAINTERESOWANIA PRACAMI NAD PROJEKTEM ZAŁOŻEŃ PROJEKTU USTAWY, PROJEKTEM USTAWY LUB PROJEKTEM ROZPORZĄDZENIA

ZGŁOSZENIE

ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ZGŁOSZENIE ZMIANY DANYCH*

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa o

(tytuł projektu założeń projektu ustawy, projektu ustawy lub projektu rozporządzenia - zgodnie z jego treścią udostępnioną w Biuletynie Informacji Publicznej lub informacją zamieszczoną w wykazie prac legislacyjnych Rady Ministrów, Prezesa Rady Ministrów albo ministrów)

A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM

1. Nazwa/imię i nazwisko**

EXCOGITATE SP. Z O.O.

2. Adres siedziby/adres miejsca zamieszkania**

3. Adres do korespondencji i adres e-mail

B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM

Lp.	Imię i nazwisko	Adres
1	JAROSŁAW ROSTEK	
2		
3		
4		
5		

C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĘDĄCEGO PRZEDMIOTEM OCHRONY

UWAGI ZGŁOSZONE W ODDZIELNYM PLIKU ZAŁĄCZONYM DO FORMULARZA

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

D. ZAŁĄCZONE DOKUMENTY	
1	UWAGI DO PROJEKTU
2	
3	
4	
5	
6	
7	
8	

E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych**
zgłoszenia dokonanego dnia .....
(podać datę z części F poprzedniego zgłoszenia)

F. OSOBA SKŁADAJĄCA ZGŁOSZENIE

Imię i nazwisko	Data	Podpis
JAROSŁAW ROSTEK	29-09-2020	

G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia .....

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, treść: „— Zgłoszenie zmiany danych" skreśla się.

** Niepotrzebne skreślić (kliknąć dwukrotnie na tekst).

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz. 1080)), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Warszawa, 29 września 2020

Sz. P. Marek Zagórski
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowny Panie Ministrze,

W odpowiedzi na zaproszenie Ministerstwa Cyfryzacji do konsultacji w sprawie projektu ustawy zmieniającej Ustawę o krajowym systemie cyberbezpieczeństwa oraz Ustawę Prawo zamówień publicznych (propozycja z 8 września 2020 r.), pragniemy zgłosić kluczowe uwagi do projektu.

Ustawa w oczywisty sposób narusza zasady niedyskryminacji i uczciwej konkurencji przedsiębiorstw oraz podważa wielostronne oraz dwustronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami. Projekt ustawy oznacza, że rynek biznesowy będzie podlegał wpływom politycznym, co nie sprzyja wolnej konkurencji. Będzie to miało istotny negatywny wpływ na otoczenie biznesowe i całą branżę ICT w Polsce.

Przedstawiamy nastepujące szczegółowe uwagi:

1. **Nadmierna ochrona handlu tworzy bariery handlowe i tarcia.**
   Jednostronny protekcjonizm handlowy wpłynie negatywnie na rozwój gospodarczy Polski. WTO stopniowo ustanowiła międzynarodowy porządek, którego rdzeniem jest ONZ, oraz wielostronny system handlowy, którego rdzeniem jest WTO. Naruszenie zasad międzynarodowego systemu handlowego, budowanego przez dziesięciolecia, utrudniłoby utrzymanie ładu handlowego i mogłoby wywołać tarcia handlowe między Polską, a innymi krajami.

2. **KSC może skutkować brakiem uczciwej konkurencji.**
   Protekcjonizm zagroziłby konkurencyjności polskiej gospodarki cyfrowej. W perspektywie krótkoterminowej, stosowanie protekcjonizmu w celu ograniczenia sprzedaży produktów z innych krajów wydaje się pomagać niekonkurencyjnym branżom i przedsiębiorstwom. W przypadku polskiej branży ICT pozbawi to branżę ICT i przedsiębiorstwa motywacji do większych inwestycji i ulepszania technologii, prowadząc do spadku konkurencyjności produktów. Z drugiej strony branża i przedsiębiorstwa w innych krajach podejmą więcej kroków w celu poprawy konkurencyjności. W rezultacie międzynarodowa konkurencyjność polskiej branży ICT i przedsiębiorstw będzie ulegać dalszemu osłabieniu.

3. **Wbrew podstawowej zasadzie wolnego handlu w gospodarce rynkowej, protekcjonizm niszczy ekosystem branży i zwiększa koszty dostaw.**
   Wolność i wzajemność są podstawą i warunkiem wstępnym handlu międzynarodowego. Poparcie dla wolnego handlu i sprzeciw wobec protekcjonizmu to podstawowe wartości i podstawowe zasady WTO. Żaden kraj nie jest w stanie w pełni posiadać wszystkich zasobów, technologii i zdolności wymaganych do nowej ery globalnej modernizacji technologicznej i przemysłowej. Ochrona handlu może jedynie osłabić globalny system wolnego handlu i utrudnić odbudowę światowej gospodarki w czasie po epidemii.

4. **Potencjalny wpływ na dwustronne oraz wielostronne umowy handlowe i inwestycyjne podpisane przez Polskę z innymi krajami.**
   Projekt zmiany ustawy KSC podważy wielostronne umowy handlowe podpisane przez Polskę z innymi krajami, np. Porozumienie WTO/GATT. Projekt zmiany ustawy KSC narusza zasadę równych i wzajemnych korzyści oraz klauzulę największego uprzywilejowania (KNU) w WTO, a także zasadę równej ochrony i traktowania KNU obiecaną w dwustronnych umowach handlowych i inwestycyjnych między Polską, a innymi krajami.

Jako podmiot odpowiedzialności społecznej, mamy za zadanie aktywnie rozpowszechniać racjonalne rozwiązania. Mając na uwadze utrzymanie dobrego kontaktu środowiska biznesowego z rządem wnosimy o rozważenie następujących uwag do projektu zmiany ustawy KSC:

1. **Ministerstwo Cyfryzacji powinno zorganizować otwartą debatę i zaprosić odpowiednie ministerstwa, izby gospodarcze, operatorów i inne zainteresowane strony do pochylenia się i pełnego omówienia kwestii poruszonych w projekcie.**
2. **Rząd powinien w pełni ocenić wpływ projektu, w tym koszty i straty, na konkurencję handlową, legalność, społeczno-gospodarcze i międzynarodowe stosunki handlowe oraz klimat inwestycyjny w Polsce.**
3. **Zasadniczo, zablokowanie niektórych dostawców nie może rozwiązać problemów związanych z bezpieczeństwem cybernetycznym. Wnosimy o przyjęcie spójnej strategii w ramach UE, w celu zarządzania za pomocą jasnych specyfikacji technicznych i zharmonizowanych norm, zamiast wykluczania dostawców z określonych krajów. Postulujemy odwołanie się do modelu niemieckiego i równe traktowanie wszystkich dostawców, nie tylko z powodów nietechnicznych.**

Z punktu widzenia racjonalności ekonomicznej, rząd musi promować dwustronny wolny handel i zmniejszać bariery w swobodnym przepływie towarów i usług. Rząd powinien ogłosić przepisy ustawowe i wykonawcze oraz środki, które sformułował i wdrożył, a także ich zmiany, jak również powinien informować o nich Światową Organizację Handlu.

Na koniec proponujemy cztery konkretne propozycje zmian do projektu KSC:

1. Art. 2 pkt 29: art. 66b ust. 1 pkt 2: „Konsekwencje oceny"

Przepisy projektu: brak zapisów dotyczących mechanizmu rekompensat

Propozycja zmiany: należy dodać ust. 3 oraz 4 w art. 66b po ust. 2.:

„3. Operatorzy telekomunikacyjni otrzymują odszkodowanie za koszty związane z wymianą sprzętu lub oprogramowania;

4. Rekompensata jest obliczana na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia. Rekompensata jest wypłacana w ciągu 30 dni przez Prezesa UKE na podstawie dokumentów uzupełniających."

Uzasadnienie: Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE. Zaproponowane regulacje w praktyce oznaczają de facto „wywłaszczenie" operatorów z posiadanego sprzętu, w tym znaczeniu, że muszą się pozbyć sprzętu wcześniej zakupionego, pomimo, że gdyby niewprowadzone nowe regulacje mogliby korzystać z tego sprzętu dłużej. W konsekwencji będą musieli ponieść wydatki związane z koniecznością zakupu nowego sprzętu, a ponadto wydatki związane z usuwaniem z sieci istniejącego sprzętu.

2. Art. 2 pkt. 29: art. 66c pkt. 1 "Plan naprawczy"

Przepis projektu: W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, sporządzenia i dostarczenia w terminie 3 miesięcy planu i harmonogramu odstąpienia od dostawcy usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko.

Propozycja zmiany: cyfrę i słowo „3 miesięcy" zastępuje się cyfrą i słowem „1 roku", skreślić „dostawca" tak, aby plan dotyczył konkretnego sprzętu i oprogramowania zamiast dostawcy. „W szczególnie uzasadnionych przypadkach Pełnomocnik może zażądać od podmiotu krajowego systemu cyberbezpieczeństwa, którego dotyczy ocena, do sporządzenia i dostarczenia w terminie 1 roku planu i harmonogramu odstąpienia od usługi, sprzętu lub oprogramowania, którego dotyczy ocena określająca wysokie ryzyko."

Uzasadnienie: Okres 3 miesięcy na sporządzenie i przedstawienie planu oraz harmonogramu odstąpienia od sprzętu i oprogramowania usługodawcy jest praktycznie niemożliwy do zrealizowania. Jednocześnie, jak zostało wskazanie powyżej, wszelkie środki związane z oceną powinny być stosowane do oprogramowania i do sprzętu, a nie w stosunku do dostawcy.

3. Operatorzy telekomunikacyjni powinni otrzymać rekompensatę za koszty poniesione w związku z wymianą sprzętu lub oprogramowania, a rekompensatę powinno obliczać się na podstawie wydatków poniesionych na zakup infrastruktury lub oprogramowania, z uwzględnieniem amortyzacji i kosztów usunięcia.

Uzasadnienie:

1) Wprowadzenie przepisów art. 66b Projektu spowoduje oczywiste dla operatorów telekomunikacyjnych koszty, niezawinione przez nich, spowodowane nowymi regulacjami, które to koszty powinny być operatorom zrekompensowane przez Skarb Państwa reprezentowany przez Prezesa UKE.

4. Ustanowienie wspólnego unijnego mechanizmu certyfikacji krytycznego sprzętu i oprogramowania. Wymaganie od dostawców oświadczenia o wiarygodności. Ustalenie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu teleinformatycznego. Nawiązanie do modelu niemieckiego.

Uzasadnienie:

1) Ustalenie obiektywnych i jasnych kryteriów, upewnienie się, że wyniki zastosowanych kryteriów oceny są prawidłowe.

2) Skuteczniejszym będzie zmotywowanie dostawców do samokontroli i złożenia oświadczenia o wiarygodności.

3) Nietechnologiczne kryteria są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.

Przedmiot	Stanowisko	Problem	Przepis	Propozycja
Metody Kontroli Cyberbezpieczeń stwa	Ustanowienie warunków dla oceny ryzyka	1. Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie dla wszystkich aktywów. 2. Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego zidentyfikowanego ryzyka a nie zakładanego ryzyka. 3. ust. 13 regulacji z dnia 6 kwietnia 2020 w zakresie minimalnych zasad technicznych i organizacyjnych oraz metod zakłada, że spółki telekomunikacyjne przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności wykrycia, to wymaga pokrycia większości scenariuszy oceny ryzyka.	Art. 66a ust. 1	Ocenę ryzyka przeprowadza się wyłącznie: 1. W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie. 2. Wystąpiły poważne naruszenia bezpieczeństwa lub wysokie podatności, których nie można złagodzić.
Metody Kontroli Cyberbezpieczeń stwa	Przedmiotem oceny ryzyka jest sprzęt lub oprogramowanie, a nie dostawca.	1. Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzętu i oprogramowania jest nieracjonalne i nielogiczne. 2. Istotą regulacji powinno być, jak nie korzystać z tego sprzętu tak, aby stanowił on takie zagrożenie, a nie kto go sprzedaje. 3. Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania zestawu narzędzi UE.	Art. 66a -66c	Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny **sprzęt lub oprogramowanie**" w artykule. 66a -66c.
Metody Kontroli Cyberbezpieczeń stwa	Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne	1. Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. 2. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. 3. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do	Art. 66a ust. 4 pkt 2)-5)	1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. 2. Wymaga się od dostawców posiadania oświadczenia o wiarygodności. 3. Ustawienie wymagań technicznych lub

		zweryfikowania i oceny.		organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT. 4. Wprowadzenie odniesienia do modelu niemieckiego
Metody Kontroli Cyberbezpieczeń stwa	Okres na dostarczenie planu wycofania wynosi 1 rok zamiast 3 miesięcy	Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania w jest praktycznie niemożliwy do wdrożenia.	Art. 66 c section 1	Okres przygotowania i przedstawienia planu oraz harmonogramu powinien został wydłużony do jednego roku.
Mechanizm odwołań od decyzji kolegium	Zapewnić zakres pełnych i równych praw zgodnie z Kodeksem Postępowania Administracyjnego .	1. Prawo odwołania od decyzji kolegium dotyczy tylko oceny określającej wysokie ryzyko, ocena określająca średnie i niskie ryzyko nie zapewnia prawa do odwołania. 2. Odwołanie nie zawiesza wykonalności decyzji 3. Obecne postanowienie upoważnia Kolegium do działania we własnej sprawie, tym samym pozbawia stronę zainteresowaną obiektywnej i niezależnej ochrony podstawowych praw stron w postępowaniu.	Art. 66a ust.8	1. Ocena określająca średnie i niskie ryzyko powinna również upoważniać do wniesienia odwołania. 2. Wniesienie odwołania powinno zawieszać wykonalność decyzji. 3. Wynik oceny ryzyka może być przedmiotem odwołania do sądu zgodnie z postanowieniami Kodeksu Postępowania Administracyjnego. 4. Wykonalność decyzji powinna zostać zawieszona do czasu prawomocnej decyzji sądu.

Z wyrazami szacunku,

Jarosław Rostek

WZÓR URZĘDOWEGO FORMULARZA ZGŁOSZENIA ZAINTERESOWANIA PRACAMI NAD PROJEKTEM ZAŁOŻEŃ PROJEKTU USTAWY, PROJEKTEM USTAWY LUB PROJEKTEM ROZPORZĄDZENIA

ZGŁOSZENIE

ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ZGŁOSZENIE ZMIANY DANYCH*

Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa

(tytuł projektu założeń projektu ustawy, projektu ustawy lub projektu rozporządzenia - zgodnie z jego treścią udostępnioną w Biuletynie Informacji Publicznej lub informacją zamieszczoną w wykazie prac legislacyjnych Rady Ministrów, Prezesa Rady Ministrów albo ministrów)

A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM

1. Nazwa/imię i nazwisko**

Signum Edward Kuś

2. Adres siedziby/adres miejsca zamieszkania**

3. Adres do korespondencji i adres e-mail

B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM

Lp.	Imię i nazwisko	Adres
1	Marcin Kuś	
2		
3		
4		
5		

C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĘDĄCEGO PRZEDMIOTEM OCHRONY

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Wpływ na biznes, zachowanie ciągłości usług dla klientów
Dodatkowe komentarze w przesłanym załączniku

D. ZAŁĄCZONE DOKUMENTY

1	List do Ministra Cyfryzacji
2	
3	
4	
5	
6	
7	
8	

E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych**
zgłoszenia dokonanego dnia nie dotyczy
(podać datę z części F poprzedniego zgłoszenia)

F. OSOBA SKŁADAJĄCA ZGŁOSZENIE

Imię i nazwisko	Data	Podpis
Marcin Kuś	30.09.2020	

G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia .....
(podpis)

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, treść: „— Zgłoszenie zmiany danych" skreśla się.

** Niepotrzebne skreślić (kliknąć dwukrotnie na tekst).

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz. 1080)), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

Signum Edwar
ul.Paderewskieg
41-710 Ruda
NIP 6411460924 REG

Marcin Kuś

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Ruda Śląska, 30 września 2020
Sz. P. Marek Zagorski
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowny Panie Ministrze,

W celu zapewnienia większej wydajności oraz konkurencyjności włąsciwie wszystkie branże przechodzą transformację cyfrową, w wyniku czego niezbędne jest zastosowanie nowych technologii, takich jak All Cloud, Connection of Everything i Sztuczna Inteligencja (AI). Szybki rozwój technologii cyfrowych niesie ze sobą wiele nowych wyzwań w zakresie bezpieczeństwa. Wszystko to oznacza, że rośnie ryzyko związane z cyberbezpieczeństwem, a zapewnienie bezpiecznego środowiska teleinformatycznego ma kluczowe znaczenie dla zagwarantowania, że branże oparte na ICT będą miały pozytywny wpływ na całą gospodarkę.

Ministerstwo Cyfryzacji opublikowało projekt nowelizacji Krajowego Prawa o Cyberbezpieczeństwie i Prawa Zamówień Publicznych (Projekt z 7 września 2020 r.), a także zainicjowało publiczne konsultacje. Po zapoznaniu się z tym projektem stwierdzamy, że proponowane zmiany nie przyniosą pozytywnych skutków dla bezpieczeństwa cybernetycznego w Polsce. Poniżej wskazujemy na braki zaproponowanych w Projekcie przepisów:

1. **Naruszenie zasad uczciwej konkurencji:, Jeśli** zostanie przyjęty, Projekt nada Kolegium prawo wyboru dostawców, a rynek komercyjny będzie podlegał politycznej ingerencji, która nie będzie sprzyjać konkurencji rynkowej. Obecnie jest tylko trzech głównych dostawców sprzętu 5G. Ograniczenie ich liczby do jednego, spowoduje stłumienie konkurencji na rynku ICT i negatywnie wpłynie na rozwój branży.
2. **Wyraźna dyskryminacja:** Kryteria oceny ryzyka dostawcy to wyłącznie czynniki nietechniczne, takie jak relacje między dostawcą a ich krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystym, struktura własności dostawcy i możliwości kraju macierzystego dotyczące ingerencji w działania dostawców.
3. **Projekt wyraźnie dyskryminuje dostawców z niektórych regionów:** Kryteria oceny ryzyka dostawcy to jedynie czynniki nietechniczne, w tym związek między dostawcami a krajem macierzystym, przepisy dotyczące praw człowieka w kraju macierzystym, przepisy dotyczące ochrony danych osobowych w kraju macierzystego, struktura własności dostawcy i możliwości kraju macierzystego w ingerowanie w działania dostawców.

4. **Brak technicznych kryteriów oceny:** Rząd będzie podejmował interwencje w zakresie wyboru dostawcy, wskazując na dostawców wysokiego/ średniego ryzyka, zamiast ustanowić jednolite standardy techniczne i wskazać sprzęt objęty nowymi regulacjami. Operatorzy będą zobowiązani do zaprzestania kupowania sprzętu od dostawców wysokiego / średniego ryzyka oraz do wymiany całego sprzętu od dostawców wysokiego ryzyka w ciągu pięciu lat.

5. **Brak metod weryfikacji bezpieczeństwa cybernetycznego:** Projekt nie zawiera wystarczających środków do weryfikacji bezpieczeństwa cybernetycznego, aby zapewnić bezpieczeństwo i niezawodność sieci w czasie rzeczywistym.

6. **Opóźnienie we wdrożeniu 5G wpłynie na wyniki gospodarcze i zatrudnienie:** Według badania przeprowadzonego przez Komisję Europejską szacuje się, że ie5G zapewni łącznie 141 miliardów euro i 2,3 miliona miejsc pracy w 27 państwach członkowskich Unii Europejskiej.

7. **Projekt ogranicza dywersyfikację technologii i przyszły rozwój:** Każdy sprzedawca samodzielnie ocenia rynek i wyznacza własny kierunek rozwoju. Daje to nieograniczony potencjał dywersyfikacji technologicznej i przyczynia się do przyszłego rozwoju branży. =Wykluczenie jednego z najważniejszych dostawców będzie miało negatywny wpływ na badania naukowe w Polsce, różnorodność technologii i przyszły rozwój.

Podsumowując, przyjęcie Projektu nie wpłynie pozytywnie na bezpieczeństwo cybernetyczne w Polsce.

W odpowiedzi na problemy wkazane powyżej, proponujemy, co następuje:

1. Należy przestrzegać unijnego zestawu narzędzi 5G (5G EU toolbox), nieskierowanego do określonych krajów lub dostawców oraz przyjąć ujednolicone standardy techniczne i weryfikacyjne.

2. Cyberbezpieczeństwem w zakresie 5G należy zarządzać za pomocą jasnych specyfikacji technicznych i ujednoliconych standardów, a niewykluczać dostawców z określonych krajów. Model większości krajów UE, takich jak Niemcy, na którym można się z powodzeniem wzorować, to standard bezpieczeństwa cybernetycznego opracowany przez Federalną Agencję Bezpieczeństwa Informacji (BSI) oraz plan zapewnienia bezpieczeństwa sprzętu sieciowego (NESAS) opracowany przez GSMA, zgodnie, z którymi wszyscy dostawcy są traktowani jednakowo.

3. Należy przyjąć kompromisowe (hierarchiczne) rozwiązanie w kwestii zarządzania bezpieczeństwem cybernetycznym i ograniczenie do elementów krytycznych (sieć rdzeniowa), odwołując się do definicji unijnego zestawu narzędzi 5G. Stacje bazowe 5G nie są komponentami podstawowymi, więc nie wymagają żadnych ograniczeń.

a) Model niemiecki: Przyjęcie NESAS, opracowanego przez GSMA, jako standard bezpieczeństwa cybernetycznego; certyfikowanie sprzętu wszystkich dostawców oraz przyjęcie strategii wielu dostawców.
b) Model w Szwecji i Finlandii: operatorzy zarządzają bezpieczeństwem cybernetycznym, przyjmują strategię wielu dostawców i dokonują przeglądu podstawowych komponentów sieci.

4. Należy przeprowadzić pełną analizę skutków płynących z projektu nowelizacji ustawy oraz konsultacji publicznych.

5. Należy wysłuchać zdecydowanego sprzeciwu ze strony branży teleinformatycznej i opinii publicznej wobec projektu, zaangażować ekspertów w celu pełnego przedstawienia Projektu, zorganizowwaćdebatę i wysłuchać opinii wszystkich stron.

6. Należy zmienić przepisy dyskryminujące ze względu na kraj pochodzenia danego dostawcy na przepisy, które będą zgodne z prawem konkurencji UE i zasadami WTO. Należy ustanowić prawa i regulacje sprzyjające cyfrowej przyszłości kraju, wolnej konkurencji operatorów i wysokiej, jakości usług sieciowych dla obywateli kraju.

I

a) Przedmiot

Projekt nie powinien mieć zastosowania bezpośrednio do operatorów telekomunikacyjnych

b) Ustawa

Ustawa o KSC jest transpozycją dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii), a dyrektywa NIS nie ma zastosowania do operatorów telekomunikacyjnych. Prawa i obowiązki operatorów telekomunikacyjnych zostały szczegółowo określone w projekcie ustawy Prawo Komunikacji Elektronicznej (PKE), który implementuje Europejski Kodeks Łączności Elektronicznej (EECC).

c) Uzasadnienie

Dodanie przedsiębiorstwa komunikacji elektronicznej, jako podmiotu, do którego stosuje się KSC, powoduje potencjalny konflikt przepisów o randze ustawowej. Operator telekomunikacyjny jest zazwyczaj istotnym dostawcą usług dla operatorów infrastruktury kluczowej.. Dlatego PKE ma kompleksowe i szczególne wymagania wobec operatorów telekomunikacyjnych. Nakładanie się na siebie KSC i PKE spowoduje wątpliwości interpretacyjne.

d) Przepisy

art. 1 KSC art. 20a-f KSC

e) Sugestie

1. Postępowanie zgodnie z logiką prawną dyrektywy NIS i EECC.
2. KSC nie ma zastosowania do przedsiębiorstw komunikacji elektronicznej.

II

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Ustanowienie warunków dla oceny ryzyka

c) Uzasadnienie

Zestaw narzędzi UE dla działań ograniczających ryzyka dotyczy analizy ryzyka dla kluczowych aktywów, a nie wszystkich aktywów.

Podejście UE wymaga wzięcia pod uwagę planu ograniczenia ryzyka celem kontroli realnego, zidentyfikowanego ryzyka a niezakładanego ryzyka. § 2 pkt 13 Rozporządzenia Ministra Cyfryzacji z dnia 22 czerwca 2020 r. w sprawie minimalnych środków technicznych i organizacyjnych (...) przewiduje, że przedsiębiorcy telekomunikacyjni przeprowadzą okresową analizę ryzyka w zakresie naruszenia bezpieczeństwa sieci i podatności

d) Przepisy

Art. 66a ust. 1

e) Sugestie

Ocenę ryzyka przeprowadza się wyłącznie:

1) W odniesieniu do krytycznego sprzętu lub oprogramowania, które stwarzają wysokie ryzyko dla bezpieczeństwa lub integralności kluczowych usług na poziomie krajowym o znaczącym wpływie.

2), Gdy wystąpiły poważne naruszenia bezpieczeństwa lub podatności, których nie można załagodzić.

III

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Przedmiotem oceny ryzyka powinien byćsprzęt lub oprogramowanie, a nie dostawca.

c) Uzasadnienie

Łączenie zagrożeń gospodarczych, kontrwywiadowczych i terrorystycznych z dostawcą sprzęt i oprogramowania jest nieracjonalne i nielogiczne.

Ważniejszym pytaniem, od tego, kto jest sprzedawcą, powinno być pytanie, jak korzystać z sprzętu tak, aby nie stanowił onzagrożenia.

Zestaw narzędzi UE (Toolbox) przewiduje możliwość podjęcia środków ograniczających w odniesieniu do kluczowych aktywów. Polskie propozycje w projekcie wykraczają poza wymagania Zestawu Narzędzi UE

d) Przepisy

Art. 66a -66c

e) Sugestie

Zmienić słowo "dostawca sprzętu i oprogramowania" na "krytyczny sprzęt lub oprogramowanie" w artykule. 66a -66c.

IV

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne

c) Uzasadnienie

Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.

d) Przepisy

Art. 66a ust. 4 pkt 2)-5)

e) Sugestie

1. Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania.
2. Wymaganie od dostawców posiadania oświadczenia o wiarygodności.
3. Ustawienie wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT.
4. Skorzystanie z wzorca modelu niemieckiego

V

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Okres karencji powinien wynosić 10 lat zamiast 5 lat

c) Uzasadnienie

Wymiana związana z krytycznym sprzętem i oprogramowaniem będzie wymagała zmiany całego projektu sieci i ogromnej części sieci. Zajmie to dużo czasu, a wszelki pośpiech negatywnie wpłynie to na stabilność sieci. Również koszty zmiany będą bardzo wysokie. Dlatego powinny zostać rozłożone w dłuższym okresie czasu.

d) Przepisy

Art. 66 b ust. 1 pkt 2

e) Sugestie

Czas wycofania sprzętu z eksploatacji: 10 lat od daty opublikowania ogłoszenia o ocenie.

VI

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Możliwość zmiany wyniku oceny powinna mieć również zastosowanie do sprzętu lub oprogramowania wysokiego ryzyka.

c) Uzasadnienie

Dostawca sprzętu lub oprogramowania o wysokim ryzyku powinien mieć takie samo prawo i możliwość złożenia wniosku o zmianę oceny, jak dostawca o umiarkowanym i niskim ryzyku

d) Przepisy

Art. 66a ust. 7

e) Sugestie

Dostawca sprzętu lub oprogramowania wysokiego ryzyka może również przedłożyć Kolegium środki zaradcze i plan naprawczy. Jeżeli te środki zaradcze oraz plan naprawczy zostaną zaakceptowane, Kolegium może zmienić ocenę

VII

a) Przedmiot

Metody Kontroli Cyberbezpieczeństwa

b) Ustawa

Okres na dostarczenie planu wycofania wynosi rok zamiast 3 miesięcy

c) Uzasadnienie

Okres 3 miesięcy dla przygotowania i przedstawienia planu i harmonogramu dla wycofania z infrastruktury dostawcy usług sprzętu i oprogramowania jest praktycznie niemożliwy do dochowania.

d) Przepisy

Art.. 66c ust. 1

e) Sugestie

Okres przygotowania i przedstawienia planu oraz harmonogramu powinien zostać wydłużony do jednego roku.

Z wyrazami szacunku,
Signum Edward Kuś
Marcin Kuś
Podpis:

Marcin Kuś

Signum Edward Kuś
ul.Paderewskiego 17/28
41-710 Ruda Śląska
NIP 6411460924 REGON 361923506

WZÓR URZĘDOWEGO FORMULARZA ZGŁOSZENIA ZAINTERESOWANIA PRACAMI NAD PROJEKTEM ZAŁOŻEŃ PROJEKTU USTAWY, PROJEKTEM USTAWY LUB PROJEKTEM ROZPORZĄDZENIA

ZGŁOSZENIE

ZAINTERESOWANIA PRACAMI NAD PROJEKTEM - ~~ZGŁOSZENIE ZMIANY DANYCH~~*

Projekt ustawy UD68 opublikowany w dniu 8 września 2020 r.

(tytuł projektu założeń projektu ustawy, projektu ustawy lub projektu rozporządzenia - zgodnie z jego treścią udostępnioną w Biuletynie Informacji Publicznej lub informacją zamieszczoną w wykazie prac legislacyjnych Rady Ministrów, Prezesa Rady Ministrów albo ministrów)

A. OZNACZENIE PODMIOTU ZAINTERESOWANEGO PRACAMI NAD PROJEKTEM

Loopus Górski Opęchowski sp. j.

1. Nazwa/~~imię i nazwisko~~**

Loopus Górski Opęchowski sp. j.

2. Adres siedziby/~~adres miejsca zamieszkania~~**

3. Adres do korespondencji i adres e-mail

B. WSKAZANIE OSÓB UPRAWNIONYCH DO REPREZENTOWANIA PODMIOTU WYMIENIONEGO W CZĘŚCI A W PRACACH NAD PROJEKTEM

Lp.	Imię i nazwisko	Adres
1	Rafał Górski	
2		
3		
4		
5		

C. OPIS POSTULOWANEGO ROZWIĄZANIA PRAWNEGO, ZE WSKAZANIEM INTERESU BĘDĄCEGO PRZEDMIOTEM OCHRONY

Projekt ustawy będzie miał duży wpływ na sektor telekomunikacyjny.
Szczegółowy opis moich uwag znajduje się w załączniku.

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

D. ZAŁĄCZONE DOKUMENTY	
1	Pismo do Ministra Cyfryzacji
2	
3	
4	
5	
6	
7	
8	

E. Niniejsze zgłoszenie dotyczy uzupełnienia braków formalnych/zmiany danych**
zgłoszenia dokonanego dnia .....
(podać datę z części F poprzedniego zgłoszenia)

F. OSOBA SKŁADAJĄCA ZGŁOSZENIE

Imię i nazwisko	Data	Podpis
Rafał Górski	12.10.2020	

G. KLAUZULA ODPOWIEDZIALNOŚCI KARNEJ ZA SKŁADANIE FAŁSZYWYCH ZEZNAŃ

Jestem świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia
(podpis)

* Jeżeli zgłoszenie nie jest składane w trybie art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, treść: „— Zgłoszenie zmiany danych" skreśla się.

** Niepotrzebne skreślić (kliknąć dwukrotnie na tekst).

Pouczenie:

1. Jeżeli zgłoszenie ma na celu uwzględnienie zmian zaistniałych po dacie wniesienia urzędowego formularza zgłoszenia (art. 7 ust. 6 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa) lub uzupełnienie braków formalnych poprzedniego zgłoszenia (§ 3 rozporządzenia Rady Ministrów z dnia 22 sierpnia 2011 r. w sprawie zgłaszania zainteresowania pracami nad projektami aktów normatywnych oraz projektami założeń projektów ustaw (Dz. U. Nr 181, poz. 1080)), w nowym urzędowym formularzu zgłoszenia należy wypełnić wszystkie rubryki, powtarzając również dane, które zachowały swoją aktualność.
2. Część B formularza wypełnia się w przypadku zgłoszenia dotyczącego jednostki organizacyjnej oraz w sytuacji, gdy osoba fizyczna, która zgłasza zainteresowanie pracami nad projektem założeń projektu ustawy lub projektem aktu normatywnego, nie będzie uczestniczyła osobiście w tych pracach.
3. W części D formularza, stosownie do okoliczności, uwzględnia się dokumenty, o których mowa w art. 7 ust. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa, a także pełnomocnictwa do wniesienia zgłoszenia lub do reprezentowania podmiotu w pracach nad projektem aktu normatywnego lub projektu założeń projektu ustawy.
4. Część E formularza wypełnia się w przypadku uzupełnienia braków formalnych lub zmiany danych dotyczących wniesionego zgłoszenia.

© www.signform.pl Sp. z o.o., producent aktywnych formularzy, e-mail: biuro@signform.pl

Warszawa, 12 października 2020

Sz. P. Marek Zagorski
Minister Cyfryzacji
ul. Królewska 27
00-060 Warszawa

Szanowny Panie Ministrze,

w związku z ogłoszonymi przez Ministerstwo Cyfryzacji konsultacjami społecznymi Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (propozycja z 8 września 2020 r.) . Poniżej przedstawiamy nasze stanowisko dotyczące tego Projektu.

Rozwój jest celem każdego państwa, również naszego. Kluczowe elementy rozwoju to ochrona praw i interesów obywateli, poprawa infrastruktury, rozwój energetyki, przyspieszenie rozwoju wsi i rolnictwa, dokończenie modernizacji przemysłu i ochrona bezpieczeństwa narodowego. Z dużym uznaniem stwierdzamy, że Ministerstwo Cyfryzacji umieszcza w agendzie legislacyjnej ochronę cyberbezpieczeństwa.

Przeanalizowaliśmy Projekt i uważamy, że może on zaszkodzić rzeczywistym interesom obywateli, wpływając negatywnie na koszty oraz dostępność do usług telekomunikacyjnych, zatrudnienie i przyszłe możliwości. Zgłaszamy niniejszym następujące uwagi:

1. Projekt wymaga wycofania całego sprzętu danego dostawcy w ciągu 5 lat, co spowoduje, że rząd/dany sektor będzie potrzebował dużej ilości dodatkowych nakładów finansowych, a tym samym wpłynie negatywnie na proces kształtowania społeczeństwa cyfrowego.
2. Projekt doprowadzi do wzrostu kosztów po stronie operatorów, co spowoduje konieczność wprowadzenia wyższych taryf telekomunikacyjnych i wpłynie na podwyższenie abonamentu.
3. Wykluczenie poszczególnych dostawców doprowadzi do zmniejszenia konkurencji na rynku, co negatywnie wpłynie na koszty operatorów, a tym samym zaszkodzi interesom konsumentów.
4. Projektowane przepisy faktycznie zmierzają do wykluczenia dostawców przez wzgląd na ich kraj pochodzenia, co doprowadzi do stawiania barier handlowych i wpłynie negatywnie na zaufanie inwestorów zagranicznych oraz na rozwój gospodarczy Polski.
5. Projekt spowolni rozwój cyfrowy co wpłynie negatywnie na modernizację przemysłu i tworzenie nowych możliwych miejsc pracy.
6. Projekt prowadzi do opóźnienia rozwoju sieci 5G, co negatywnie wpłynie na wygodę i łatwość obywateli w korzystaniu z zaawansowanej technologii cyfrowej, np. praca zdalna, telemedycyna, zdalna edukacja, inteligentny przemysł oraz inteligentne rolnictwo.

Z punktu widzenia rzeczywistych interesów polskich obywateli oraz przedsiębiorców, sugerujemy przeprowadzenie szerokich konsultacji społecznych, pełne wysłuchanie opinii publicznej oraz dokonanie wyczerpującej analizy skutków regulacji.

Z naszej strony chcieliśmy zaproponować poniższe uwagi do Projektu:

Przedmiot	Stanowisko	Problem	Przepis	Propozycja
Czas na wymianę sprzętu wysokiego ryzyka	Okres 5 lat na wymianę sprzętu jest zbyt krótki	Wymiana sprzętu i oprogramowania uznanego za wysoce ryzykowny będzie wiązała się z koniecznością nabycia nowych komponentów i przystosowania ich do obecnej infrastruktury Należy mieć na uwadze zarówno koszty wymiany sprzętu, jak i przeszkolenia użytkowników	Art. 66 b ust. 1 pkt 2	Czas wycofania sprzętu z eksploatacji to10 lat od daty opublikowania ogłoszenia o uznaniu produktu za wysoce ryzykowny
Koszty wymiany sprzętu	Postulowane wprowadzenie rekompensat	Artykuł 66b doprowadzi do powstania istotnych kosztów dla operatorów telekomunikacyjnych, których nie powinni ponosić, spowodowanych nowymi regulacjami, które powinny być pokryte przez Skarb Państwa reprezentowany przez Prezesa UKE.	Art.66b ust. 1 i ust. 2	Przedsiębiorcy telekomunikacyjni powinni otrzymać odszkodowanie z tytułu poniesionych kosztów wymiany sprzętu lub oprogramowania.
Metody Kontroli Cyberbezpieczeństwa	Kryteria oceny ryzyka powinny być obiektywne, jasne i bezstronne	Ustalenie obiektywnych i jasnych kryteriów, gwarantujących poprawność wyników zastosowanych kryteriów oceny. Bardziej skuteczne będzie motywowanie dostawców do samodzielnego sprawdzania i składania oświadczeń o wiarygodności. Kryteria nietechnologiczne są bardzo często nieokreślone i wykorzystują niejasne pojęcia, które są bardzo trudne do zweryfikowania i oceny.	Art. 66a ust. 4 pkt 2)-5)	Ustanowienie wspólnego unijnego mechanizmu certyfikacji dla krytycznego sprzętu i oprogramowania. Wymaganie od dostawców posiadania oświadczenia o wiarygodności. Ustalenia wymagań technicznych lub organizacyjnych dla dostawców sieci telekomunikacyjnej i systemu ICT. Skorzystanie z modelu niemieckiego

Z wyrazami szacunku,

Rafał Górski

Loopus Górski Opęchowski Sp. J.

Minister do Spraw
Unii Europejskiej

DPUE.920.1030.2021.KWM(77)
Warszawa, 09 czerwca 2023 r.
Dot.: RM-0610-69-23 tekst ostateczny

Pan Łukasz Schreiber
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowny Panie Ministrze,

w związku z przedłożonym projektem ustawy pozwalam sobie wyrazić poniższą opinię.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Z wyrazami szacunku

z upoważnienia Ministra do Spraw Unii Europejskiej

Karolina Rudzińska
Podsekretarz Stanu w Kancelarii Prezesa Rady Ministrów
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
Pan Janusz Cieszyński
Minister Cyfryzacji

Telefon: +48 22 694 7540
adres email: SMUE@kprm.gov.pl
www.gov.pl/web/premier

Kancelaria Prezesa Rady Ministrów
Al. Ujazdowskie 1/3
00-583 Warszawa