SEJM
RZECZYPOSPOLITEJ POLSKIEJ
IX kadencja

Druk nr 2045

Warszawa, 8 października 2021 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej i na podstawie art. 32 ust. 2 regulaminu Sejmu niżej podpisani posłowie wnoszą projekt ustawy:

- o Agencji Cyberbezpieczeństwa.

Do reprezentowania wnioskodawców w pracach nad projektem ustawy upoważniamy pana posła Krzysztofa Gawkowskiego.

(-) Rafał Adamczyk; (-) Magdalena Biejat; (-) Wiesław Buż; (-) Jacek Czerniak; (-) Marek Dyduch; (-) Agnieszka Dziemianowicz-Bąk; (-) Monika Falej; (-) Krzysztof Gawkowski; (-) Daria Gosek-Popiołek; (-) Arkadiusz Iwaniak; (-) Maciej Konieczny; (-) Maciej Kopiec; (-) Katarzyna Kotula; (-) Paweł Krutul; (-) Marcin Kulasek; (-) Robert Kwiatkowski; (-) Beata Maciejewska; (-) Paulina Matysiak; (-) Wanda Nowicka; (-) Robert Obaz; (-) Małgorzata Prokop-Paczkowska; (-) Marek Rutka; (-) Joanna Scheuring-Wielgus; (-) Małgorzata Sekuła-Szmajdzińska; (-) Joanna Senyszyn; (-) Anita Sowińska; (-) Wiesław Szczepański; (-) Jan Szopiński; (-) Krzysztof Śmiszek; (-) Tomasz Trela; (-) Katarzyna Ueberhan; (-) Dariusz Wieczorek; (-) Zdzisław Wolski.

Tłoczono z polecenia Marszałka Sejmu Rzeczypospolitej Polskiej

Projekt

Ustawa

z dnia ... 2021 roku

o Agencji Cyberbezpieczeństwa[1]

Rozdział I
Postanowienia ogólne

Art. 1. Ustawa reguluje zakres i zasady działania oraz strukturę Agencji Cyberbezpieczeństwa.

Art. 2. Ilekroć w ustawie mowa o:

1) danych - rozumie się przez to dane wytwarzane i dostarczane w postaci cyfrowej;
2) sprzęcie elektronicznym - rozumie się przez to urządzenie umożliwiające przechowywanie lub przetwarzanie danych, którego prawidłowe działanie uzależnione jest od dopływu prądu elektrycznego, obecności pól elektromagnetycznych lub połączenia z innym urządzeniem.

Art. 3. Tworzy się Agencję Cyberbezpieczeństwa, zwaną dalej "AC".

Art. 4. Do zadań AC należy:

1) koordynacja krajowego systemu cyberbezpieczeństwa;
2) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania

[1] W niniejszej ustawie dokonuje się zmian następujących ustaw: ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych 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 (Dz.U. z 2019 r. poz. 1398);

3) prowadzenie działań prewencyjno-edukacyjnych związanych z cyberbezpieczeństwem w sektorze publicznym i prywatnym;
4) budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;
5) podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego;
6) podejmowanie działań kryptologicznych i ochraniających cybernetyczne zasoby państwa;
7) reagowanie na incydenty związane z bezpieczeństwem cybernetycznym i współpraca operacyjna z innymi służbami specjalnymi w celu likwidacji zagrożeń;
8) koordynowanie i rozwijanie krajowego systemu cyberbezpieczeństwa;
9) wspieranie jednostek nauki i szkolnictwa wyższego w zakresie bezpieczeństwa w cyberprzestrzeni;
10) monitorowanie rozwoju nowoczesnych technologii i ich wpływu na życie człowieka;
11) ocena i zarządzanie ryzykiem cyfrowym;
12) wymiana informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie.

Art. 5. 1. Działalność AC jest finansowana z odrębnej części budżetu państwa.

2. Koszty realizacji zadań AC, w zakresie których – ze względu na wyłączenie ich jawności – nie mogą być stosowane przepisy o finansach publicznych, rachunkowości i zamówieniach publicznych, są finansowane z utworzonego na ten cel funduszu operacyjnego.

2. Fundusz operacyjny nie może przekraczać 20% rocznego budżetu AC.

3. Szef AC określa w drodze zarządzenia szczegółowe zasady tworzenia funduszu operacyjnego i gospodarowania nim.

Art. 6. 1. Szef AC w zakresie wykonywania zadania, o którym mowa w art. 4 pkt 1 koordynuje działania podmiotów, o których mowa w art. 4 pkt 1-18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

2. AC w ramach swojej działalności współpracuje z innymi podmiotami, o których mowa w art. 7 ust. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa

Art. 7. 1. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne są obowiązani, w zakresie swojego działania, do współdziałania z AC.

2. Podmioty, o których mowa w ust. 1, w ramach współdziałania są zobowiązane do:

1) wdrażania zaleceń Szefa AC dotyczących podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności;
2) stosowania oprogramowania spełniającego standardy AC;
3) umożliwienia przeprowadzenia kontroli bezpieczeństwa systemów teleinformatycznych, zabezpieczeń danych i sprzętu elektronicznego;
4) umożliwienia pracownikom uczestniczenia w szkoleniu, o którym mowa w art. 16.

3. Niewykonanie obowiązków, o których mowa w ust 2 pkt 2-4 przez podmiot sektora administracji publicznej stanowi podstawę do wystąpienia przez Szefa AC do organu sprawującego nadzór nad podmiotem z informacją o niewykonaniu

obowiązków lub z wnioskiem o podjęcie działań mających na celu ich wykonanie. W przypadku pozostałych podmiotów, które nie wykonały obowiązków, stosuje się art. 33.

Rozdział II
Struktura i organizacja Agencji Cyberbezpieczeństwa

Art. 8. 1. Na czele AC stoi Szef AC.

2. Szefa AC powołuje Prezes Rady Ministrów, po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji.

3. Prezes Rady Ministrów, na wniosek Szefa AC, powołuje zastępcę Szefa AC po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji.

4. Szefem AC lub zastępcą Szefa AC może zostać osoba, która:

1) posiada wyłącznie obywatelstwo polskie;

2) korzysta z pełni praw publicznych;

3) daje rękojmię należytego wykonywania zadań;

4) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne";

5) posiada przynajmniej 5-letnie doświadczenie w zakresie cyberbezpieczeństwa.

Art. 9. Odwołanie Szefa AC z zajmowanego stanowiska może nastąpić w przypadku:

1) rezygnacji z zajmowanego stanowiska;

2) zrzeczenia się obywatelstwa polskiego lub nabycia obywatelstwa innego państwa;

3) skazania prawomocnym wyrokiem sądu za popełnione przestępstwo lub przestępstwo skarbowe;

4) utraty predyspozycji niezbędnych do zajmowania stanowiska;

5) niewykonywania obowiązków z powodu choroby trwającej nieprzerwanie ponad miesiąc.

Art. 10. W przypadku zwolnienia stanowiska Szefa AC lub czasowej niemożności sprawowania przez niego funkcji, Prezes Rady Ministrów może powierzyć pełnienie obowiązków Szefa jego zastępcy na czas nie dłuższy niż miesiąc.

Art. 11. 1. Szef AC:

1) kieruje pracą AC;

2) reprezentuje AC w stosunkach prawnych z innymi podmiotami;

3) zarządza mieniem AC;

4) przedstawia roczną informację o stanie cyberbezpieczeństwa państwa;

5) wykonuje inne zadania określone w ustawie.

2. Szef AC może upoważnić zastępcę Szefa AC do wykonywania powierzonych mu zadań, z wyjątkiem zadań, o których mowa w ust. 1 pkt 1 i 4.

Art. 12. 1. Prezes Rady Ministrów nadaje, w drodze zarządzenia, statut AC. Statut określa organizację wewnętrzną AC, w tym tryb zatrudniania pracowników.

2. Szef AC w drodze zarządzenia nadaje regulaminy organizacyjne, w których określa ich strukturę wewnętrzną i szczegółowe zadania.

3. Szef AC może tworzyć zespoły o charakterze stałym lub doraźnym, określając ich nazwę, skład osobowy oraz szczegółowy zakres i tryb działania.

Art. 13. 1. W ramach AC działa Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, zwany dalej: "CSIRT GOV".

2. CSIRT GOV działa na podstawie przepisów ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz niniejszej ustawy.

Rozdział III
Działalność Agencji Cyberbezpieczeństwa

Art. 14. 1. Szef AC raz w tygodniu publikuje na stronie internetowej AC raport o stanie cyberbezpieczeństwa.

2. Raport, o którym mowa w ust. 1, zawiera w szczególności:

1) ogólną ocenę bezpieczeństwa cyfrowego;
2) komunikaty o ostrzeżeniach przed atakami;
3) bieżące zalecenia w zakresie cyberbezpieczeństwa.

Art. 15. 1. Szef AC przekazuje Prezesowi Rady Ministrów informację o bieżącym stanie cyberbezpieczeństwa.

2. Szczegółowy zakres informacji, o której mowa w ust. 1, oraz tryb jej przekazywania określi Prezes Rady Ministrów w drodze zarządzenia.

Art. 16. 1. AC przeprowadza szkolenia z zakresu cyberbezpieczeństwa.

2. Szkolenia dla pracowników podmiotów, o których mowa w art. 7 ust. 1, są nieodpłatne. Opłata za uczestnictwo w szkoleniu dla pracowników pozostałych podmiotów od osoby wynosi nie więcej niż 1/10 minimalnego miesięcznego wynagrodzenia za pracę, ustalanego na podstawie przepisów odrębnych.

3. Wpływy z opłaty, o której mowa w ust. 2, stanowią dochód AC.

Art. 17. 1. Szef AC publikuje standardy oprogramowania i zarządzania bezpieczeństwem informacji.

2. Standardy, o których mowa w ust. 1, tworzone są na podstawie norm międzynarodowych oraz bieżących zaleceń Szefa AC dotyczących podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności.

Art. 18. 1. Szef AC na podstawie analizy zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych wydaje podmiotom, o których mowa w art. 7 ust. 1 zalecenia dotyczące podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności, zwane dalej „zaleceniami".

2. Podmioty, o których mowa w art. 7 ust. 1, mogą wnieść do Szefa AC zastrzeżenia do zaleceń z uwagi na negatywny wpływ rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności w terminie 7 dni od dnia otrzymania zaleceń.

3. Szef AC odnosi się do zastrzeżeń, o których mowa w ust. 2 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania i podtrzymuje lub zmienia zalecenia.

4. Podmioty, które otrzymały zalecenia, w terminie miesiąca od dnia ich otrzymania informują Szefa AC o sposobie i zakresie ich wykonania.

5. Niewykonanie zaleceń przez podmiot sektora administracji publicznej stanowi podstawę do wystąpienia przez Szefa AC do organu sprawującego nadzór nad podmiotem z informacją o niewykonaniu zaleceń lub z wnioskiem o podjęcie działań mających na celu ich wykonanie. W przypadku pozostałych podmiotów, które nie wykonały zaleceń, stosuje się art. 32.

Art. 19. 1. AC może przeprowadzać w podmiotach, o których mowa w art. 7 ust. 1 kontrolę bezpieczeństwa systemów teleinformatycznych, zabezpieczeń danych i sprzętu elektronicznego, zwaną dalej "kontrolą bezpieczeństwa".

2. Kontrole bezpieczeństwa są przeprowadzane zgodnie z rocznym planem przeprowadzania kontroli bezpieczeństwa, opracowywanym w terminie do 30 listopada roku poprzedzającego przez Szefa AC w uzgodnieniu z ministrem właściwym do spraw informatyzacji. W uzasadnionych przypadkach kontrola bezpieczeństwa może zostać przeprowadzona z pominięciem planu.

3. AC informuje podmiot, o którym mowa w art. 7 ust. 1, o włączeniu go do rocznego planu przeprowadzania kontroli bezpieczeństwa.

4. Kontrola bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji podatności, przez które rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływających na integralność, poufność, rozliczalność i dostępność tego systemu.

5. Kontrola bezpieczeństwa powinna być prowadzona z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie teleinformatycznym podlegającym tej ocenie.

6. W celu minimalizacji negatywnych następstw kontroli bezpieczeństwa AC uzgadnia z podmiotem, o którym mowa w ust. 1, ramowe warunki przeprowadzania tej kontroli, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach kontroli bezpieczeństwa testów bezpieczeństwa.

7. AC 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.

8. Używając urządzeń lub programów komputerowych, o których mowa w ust. 7, AC w czasie kontroli bezpieczeństwa 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 teleinformatycznego.

9. Informacje uzyskane przez AC w wyniku przeprowadzania kontroli bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych AC oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Art. 20. 1. Po przeprowadzeniu kontroli bezpieczeństwa AC sporządza i przekazuje podmiotowi, którego system podlegał kontroli bezpieczeństwa, raport

zawierający podsumowanie przeprowadzonych czynności, wskazanie wykrytych podatności systemu teleinformatycznego oraz zalecenia pokontrolne.

2. Jeżeli wykryta podatność może wystąpić w innych systemach teleinformatycznych, AC informuje niezwłocznie Prezesa Rady Ministrów o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach teleinformatycznych.

Art. 21. 1. Szef AC określi, w drodze zarządzenia, rodzaje dokonywanych w ramach kontroli bezpieczeństwa testów bezpieczeństwa, uwzględniając potrzebę kompletności dokonywanej kontroli bezpieczeństwa.

2. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób niszczenia przez Szefa AC materiałów zawierających informacje, o których mowa w art. 19 ust. 9, a także wzory niezbędnych dokumentów, mając na uwadze rodzaj materiałów podlegających zniszczeniu.

3. Rada Ministrów określi, w drodze rozporządzenia, tryb i warunki przeprowadzania kontroli bezpieczeństwa, mając na uwadze określenie czynności niezbędnych do jej przeprowadzenia, w tym dokonywanie uzgodnień, o których mowa w ust. 6.

Art. 22. 1. W celu zapobiegania, przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących podmiotów, o których mowa w art. 4 pkt 2, lub danych w nich przetwarzanych oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, AC wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania", prowadzi go i koordynuje jego funkcjonowanie.

2. Wdrożenie elementów systemu ostrzegania w podmiotach, o których mowa w ust. 1, następuje zgodnie z rocznym planem wdrożenia, opracowywanym przez Szefa AC w terminie do dnia 30 listopada roku poprzedzającego. W uzasadnionych przypadkach, na wniosek podmiotu, wdrożenie elementów systemu ostrzegania może zostać przeprowadzone z pominięciem planu.

3. AC niezwłocznie informuje podmiot, o którym mowa w ust. 1, o jego włączeniu do rocznego planu wdrożenia systemu ostrzegania.

4. Podmiot, o którym mowa w ust. 1, ma obowiązek przystąpić do systemu ostrzegania oraz przekazać AC niezbędne informacje umożliwiające wdrożenie systemu ostrzegania w tym podmiocie.

5. W podmiotach, o których mowa w ust. 1, podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, wdrożenie systemu ostrzegania może nastąpić za zgodą Ministra Obrony Narodowej.

6. Koszty wdrożenia i utrzymania systemu ostrzegania w podmiotach, o których mowa w ust. 1, pokrywa AC.

7. AC, w drodze porozumienia, uzgadnia z podmiotem, o którym mowa w ust. 1, techniczne aspekty uczestnictwa w systemie ostrzegania oraz model konfiguracji systemu.

8. W sytuacji braku możliwości zawarcia porozumienia, o którym mowa w ust. 7, z przyczyn leżących po stronie podmiotu, o którym mowa w ust. 1, AC informuje podmiot go nadzorujący lub Prezesa Rady Ministrów.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w szczególności określi czynności niezbędne do jego uruchomienia i utrzymania oraz wzór porozumienia, o którym mowa w ust. 7, kierując się potrzebą zapewnienia bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa.

Art. 23. 1. W przypadku powzięcia informacji o wystąpieniu zdarzenia o charakterze terrorystycznym dotyczącego systemów lub danych, o których mowa w art. 4 pkt 2, Szef AC może żądać od podmiotów, o których mowa w art. 4 pkt 2, przedstawienia informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych, w tym informacji obejmujących hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemu oraz ich używanie, w celu zapobiegania, reagowania na zdarzenia o charakterze terrorystycznym dotyczące systemów lub danych, o których mowa w art. 4 pkt 2, a

także zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców.

2. Informacje i dane, o których mowa w ust. 1, podlegają ochronie przewidzianej w przepisach o ochronie informacji niejawnych i mogą być udostępniane jedynie funkcjonariuszom AC prowadzącym w danym postępowaniu czynności operacyjno-rozpoznawcze i ich przełożonym, uprawnionym do sprawowania nadzoru nad tymi czynnościami.

3. Skarb Państwa ponosi odpowiedzialność za szkody wyrządzone naruszeniem przepisu ust. 2 na zasadach określonych w Kodeksie cywilnym.

Art. 24. 1. W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa AC, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia, może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym, zwane dalej „blokadą dostępności".

2. Wniosek, o którym mowa w ust. 1, przedstawia się wraz z materiałami uzasadniającymi potrzebę zastosowanie blokady dostępności.

3. Postanowienie, o którym mowa w ust. 1, wydaje Sąd Okręgowy w Warszawie.

4. W przypadkach niecierpiących zwłoki, jeżeli mogłaby ona spowodować zdarzenie o charakterze terrorystycznym, Szef AC, po uzyskaniu pisemnej zgody Prokuratora Generalnego, może zarządzić blokadę dostępności, zwracając się jednocześnie do sądu, o którym mowa w ust. 3, z wnioskiem o wydanie postanowienia w tej sprawie.

5. Usługodawca świadczący usługi drogą elektroniczną jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu żądaniu Szefa AC.

6. Wniosek Szefa AC, o którym mowa w ust. 1, powinien zawierać w szczególności:

1) numer sprawy i jej kryptonim, jeżeli został jej nadany;
2) opis zdarzenia o charakterze terrorystycznym z podaniem, w miarę możliwości, jego kwalifikacji prawnej;
3) okoliczności uzasadniające potrzebę blokady dostępności;
4) szczegółowe określenie rodzaju danych informatycznych lub usług teleinformatycznych mających podlegać zablokowaniu;
5) dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności, ze wskazaniem sposobu jej stosowania;
6) cel i czas prowadzonej blokady dostępności.

7. Blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd, o którym mowa w ust. 3, może, na pisemny wniosek Szefa AC, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia.

8. Do wniosku, o którym mowa w ust. 4 i 7, stosuje się odpowiednio przepisy ust. 2 i 6. Sąd przed wydaniem postanowienia, o którym mowa w ust. 1, 4 i 7, zapoznaje się z materiałami uzasadniającymi wniosek.

9. Wnioski, o których mowa w ust. 1, 4 i 7, sąd rozpoznaje jednoosobowo, przy czym czynności sądu związane z rozpoznawaniem tych wniosków powinny być realizowane w warunkach przewidzianych dla przekazywania, przechowywania i udostępniania informacji niejawnych oraz z odpowiednim zastosowaniem przepisów wydanych na podstawie art. 181 § 2 Kodeksu postępowania karnego. W posiedzeniu sądu może wziąć udział wyłącznie prokurator i Szef AC.

10. Na postanowienia sądu, o których mowa w ust. 1, 4 i 7, przysługuje zażalenie Szefowi AC i Prokuratorowi Generalnemu. Do zażalenia stosuje się odpowiednio przepisy Kodeksu postępowania karnego.

11. Blokady dostępności zaprzestaje się w przypadku:

1) nieudzielenia przez sąd, w terminie 5 dni od złożenia wniosku w trybie ust. 4, zgody na zarządzenie przez Szefa AC blokady dostępności;
2) nieudzielenia przez sąd zgody na przedłużenie blokady dostępności w trybie ust. 7;
3) upływu okresu, na który blokada dostępności została wprowadzona.

12. Sąd, Prokurator Generalny oraz Szef AC prowadzą w formie elektronicznej, z zachowaniem przepisów o ochronie informacji niejawnych, rejestry postanowień, pisemnych zgód, zarządzeń i wniosków dotyczących blokady dostępności.

13. O zastosowaniu blokady dostępności Szef AC powiadamia ministra właściwego do spraw informatyzacji, jeżeli usługodawca świadczący usługi drogą elektroniczną ma siedzibę na terytorium Rzeczypospolitej Polskiej.

14. Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków, uwzględniając potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów.

Art. 25. 1. Szef AC prowadzi rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych, o których mowa w art. 4 pkt 2.

2. Rejestr, o którym mowa w ust. 1, zawiera dane obejmujące:
1) identyfikację podmiotu, na rzecz którego działa system teleinformatyczny, oraz dane administratora systemu;
2) datę i czas wykrycia naruszenia bezpieczeństwa systemu oraz prawdopodobną początkową datę i czas naruszenia bezpieczeństwa systemu;
3) identyfikację źródła zdarzenia naruszającego bezpieczeństwo systemu;
4) opis stwierdzonego zdarzenia naruszającego bezpieczeństwo systemu oraz sposób działania podmiotu powodującego naruszenie bezpieczeństwa;
5) opis szkód w systemie powstałych lub mogących powstać wskutek zdarzenia naruszającego bezpieczeństwo systemu.

3. Dane, o których mowa w ust. 2, przekazuje Szefowi AC administrator systemu teleinformatycznego, o którym mowa w art. 4 pkt 2, niezwłocznie po wykryciu zdarzenia naruszającego bezpieczeństwo tego systemu.

4. Dane z rejestru są udostępniane Prezesowi Rady Ministrów.

Art. 26. 1. Szef AC przedstawia Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji roczną informację o stanie cyberbezpieczeństwa państwa.

Rozdział IV
Pracownicy i funkcjonariusze Agencji Cyberbezpieczeństwa

Art. 27. 1. W ramach AC zatrudnieni są pracownicy i funkcjonariusze.

2. Funkcjonariusze AC pełną służbę w ramach CSIRT GOV.

3. W pozostałych jednostkach AC zatrudnieni są pracownicy AC.

Art. 28. 1. Pracownikiem lub funkcjonariuszem AC może być obywatel polski o nieposzlakowanej opinii, który nie był skazany prawomocnym wyrokiem sądu za przestępstwo lub przestępstwo skarbowe, korzystający z pełni praw publicznych, posiadający wykształcenie wyższe oraz zdolność fizyczną i psychiczną do pracy lub służby w formacjach podległych szczególnej dyscyplinie służbowej, której gotów jest się podporządkować, a także dający rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych.

2. Przyjęcie kandydata do pracy lub służby w AC następuje po przeprowadzeniu postępowania kwalifikacyjnego mającego na celu ustalenie, czy kandydat spełnia warunki zatrudnienia.

3. Postępowanie kwalifikacyjne składa się z etapów:

1) złożenie podania o zatrudnienie, kwestionariusza osobowego kandydata, a także dokumentów stwierdzających wymagane wykształcenie i kwalifikacje zawodowe oraz zawierających dane o uprzednim zatrudnieniu;

2) test wiedzy i umiejętności z zakresu informatyki i nowoczesnych

technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru;

3) badanie psychologiczne;

4) rozmowa kwalifikacyjna;

5) ustalenie zdolności fizycznej i psychicznej do pracy lub służby w AC;

6) sprawdzenie w ewidencjach, rejestrach i kartotekach prawdziwości danych zawartych w kwestionariuszu osobowym kandydata;

7) postępowanie sprawdzające określone w przepisach o ochronie informacji niejawnych.

4. Podczas przeprowadzania etapów, o których mowa w ust. 3 pkt 2-4, kandydatowi zabrania się:

1) korzystania z pomocy innych osób;

2) posługiwania się urządzeniami służącymi do przekazu, odbioru lub zapisu informacji lub korzystania z pomocniczych materiałów, niedopuszczonych do ich wykorzystania;

3) zakłócania ich przebiegu w inny sposób niż określony w pkt 1 i 2.

5. W przypadku wystąpienia zachowań, o których mowa w ust. 5, kandydat otrzymuje odpowiednio negatywny wynik z etapu, o którym mowa w ust. 3 pkt 2-4.

Art. 29. Na podstawie postępowania kwalifikacyjnego Szef AC może podjąć decyzję o powołaniu do służby w CSIRT GOV kandydatów z najwyższymi wynikami postępowania.

Art. 30. Postępowanie kwalifikacyjne zarządza i prowadzi Szef AC.

Art. 31. W zakresie nieregulowanym niniejszą ustawą funkcjonariuszom AC przysługują uprawnienia funkcjonariuszy, o których mowa w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Rozdział V
Przepisy karne

Art. 32. Kto nie wykonuje zaleceń, o których mowa w art. 18, podlega karze grzywny.

Art. 33. Kto nie wykonuje obowiązku, o którym mowa w art. 7 ust. 1, podlega karze grzywny.

Art. 34. 1. Funkcjonariusz AC, który wbrew przepisom ustawy wykorzystuje informacje uzyskane podczas lub w związku z pełnieniem obowiązków służbowych do celów niezwiązanych z pełnieniem obowiązków służbowych
– podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

2. Jeżeli sprawca czynu, o którym mowa w ust. 1, działa w celu osiągnięcia korzyści osobistej lub majątkowej
– podlega karze pozbawienia wolności od lat 2 do lat 12.

Rozdział VI
Przepisy zmieniające

Art. 35. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wprowadza się następujące zmiany:

1) w art. 5 uchyla się pkt 2a;
2) w art. 12:
   a) w ust. 1 pkt 1 in fine dodaje się wyrazy: "Szefa Agencji Cyberbezpieczeństwa",
   b) w ust. 3 po pkt 3a dodaje się pkt 3b w brzmieniu: "3b) Szef Agencji Cyberbezpieczeństwa;";
3) uchyla się art. 32a-32e w całości.

Art. 36. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2020 r. poz. 1856, z 2021 r. poz. 159) wprowadza się następujące zmiany:
1) w art. 5a ust. 2 wyrazy "Pełnomocnik Rządu do spraw Cyberbezpieczeństwa" zastępuje się wyrazami "Szef Agencji Cyberbezpieczeństwa";

2) w art. 8 ust. 3 pkt 15 otrzymuje brzmienie: "15) Szef Agencji Cyberbezpieczeństwa.".

Art. 37. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa wprowadza się następujące zmiany:

1) w art. 2. pkt 1 otrzymuje brzmienie: "1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Cyberbezpieczeństwa;";
2) w art. 4 dotychczasową treść oznacza się jako ust. 1 i dodaje się ust. 2 w brzmieniu: "2. Szef Agencji Cyberbezpieczeństwa koordynuje współpracę między podmiotami, o których mowa w ust. 1.".
3) w art. 36 w ust. 2 oraz w ust. 7 pkt 3 i 5 wyrazy: "Szefa Agencji Bezpieczeństwa Wewnętrznego" zastępuje się wyrazami: "Szefa Agencji Cyberbezpieczeństwa";
4) w art. 37 w ust 2 i 3 wyrazy: "Agencji Bezpieczeństwa Wewnętrznego" zastępuje się wyrazami: "Agencji Cyberbezpieczeństwa";
5) w art. 65 w ust. 1 pkt 2 i 4 wyrazy: "Szefa Agencji Bezpieczeństwa Wewnętrznego" zastępuje się wyrazami: "Szefa Agencji Cyberbezpieczeństwa";
6) w art. 66:
   a) ust. 1 pkt 4 w lit. g kropkę zastępuje się średnikiem i dodaje lit h w brzmieniu: "Szef Agencji Cyberbezpieczeństwa.",
   b) ust. 7 otrzymuje brzmienie: "7. Sekretarz Kolegium organizuje pracę Kolegium i w tym zakresie może występować do Agencji Cyberbezpieczeństwa o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium.";
7) art. 67 otrzymuje brzmienie: "1. Prezes Rady Ministrów w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa może, na podstawie rekomendacji Kolegium, wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania

krajowego systemu cyberbezpieczeństwa, a także żądać informacji i opinii w tym zakresie od Szefa Agencji Cyberbezpieczeństwa.

2. Prezes Rady Ministrów wydaje wiążące wytyczne dla Szefa Agencji Cyberbezpieczeństwa w zakresie obsługi incydentów krytycznych.";

8) w art. 93 uchyla się ust. 7 i 22.

Rozdział VII
Przepisy przejściowe i końcowe

Art. 38. 1. Szef ABW przekaże Szefowi AC w terminie 6 miesięcy od dnia wejścia w życie ustawy zarządzanie CSIRT GOV.

2. Po upływie terminu, o którym mowa w ust. 1, Szef AC staje się dysponentem majątku CSIRT GOV oraz stroną stosunków prawnych zespołu.

3. Wszyscy pracownicy i funkcjonariusze ABW zatrudnieni w ramach CSIRT GOV, po upływie terminu, o którym mowa w ust. 1, stają się pracownikami i funkcjonariuszami AC.

4. Do funkcjonariuszy, o których mowa w ust. 3, stosuje się odpowiednio przepisy rozdziału 4-10 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Art. 39. 1. Maksymalny limit wydatków z budżetu państwa na realizację ustawy wynosi 4.430.000 tys. zł, z tego:

1) w 2022 r. – 117.000 tys. zł;
2) w 2023 r. – 264.000 tys. zł;
3) w 2024 r. – 527.000 tys. zł;
4) w 2025 r. – 765.000 tys. zł;
5) w 2026 r. – 434.000 tys. zł;
6) w 2027 r. – 444.000 tys. zł;
7) w 2028 r. – 454.000 tys. zł;
8) w 2029 r. – 464.000 tys. zł;

9) w 2030 r. – 475.000 tys. zł;

10) w 2031 r. – 486.000 tys. zł.

2. Szef AC monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego półrocza i na koniec każdego roku kalendarzowego oraz w razie konieczności wdraża mechanizm korygujący określony w ust. 3.

3. W przypadku zagrożenia przekroczenia lub przekroczenia w danym roku budżetowym limitu wydatków, o którym mowa w ust. 1, Szef AC wprowadza mechanizm korygujący polegający na zmniejszeniu wydatków budżetu państwa będących skutkiem finansowym niniejszej ustawy.

Art. 40. Ustawa wchodzi w życie z dniem 1 stycznia 2022 r.

Uzasadnienie

1. Cel i potrzeba wydania ustawy, rzeczywisty stan w dziedzinie, która ma zostać unormowana

Zgodnie z założeniami Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieograniczonego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz administracji publicznej. Oznacza to, że liczba potencjalnych zagrożeń rośnie i tylko odpowiednie mechanizmy prewencyjne mogą skutecznie przeciwdziałać zagrożeniom w cyberświecie.

Warto podkreślić, że jeszcze nigdy w historii tak niewyobrażalna liczba danych nie była tak łatwo dostępna dla wszystkich potencjalnych zainteresowanych. Kilkadziesiąt lat temu wrażliwymi danymi dysponowali tylko urzędnicy, lekarze czy prawnicy, a utrzymanie tajemnicy zawodowej było wpisane w zakres obowiązków na wskazanego zawodu. Tymczasem obecnie nasze poufne dane są zapisane w bazach danych różnych instytucji, z których coraz częściej wyciekają do internetu, a następnie są przedmiotem nielegalnego handlu.

Większość społeczeństwa uważa, że rozwój cyfrowych usług, dostępu do Internetu czy przetwarzania danych, zwiększa indywidualne poczucie bezpieczeństwa, przede wszystkim dzięki masowemu dostępowi do wiedzy czy informacji. Niestety, opierając się na faktach i prostej analizie, można stwierdzić, że ten powszechny dostęp do danych stanowi najpoważniejsze zagrożenie bezpieczeństwa wynikające z rozwoju technologicznego. Niemniej jednak tak właśnie przedstawia się nasze poczucie bezpieczeństwa w erze cyfrowej. Ma ono dwa różne wymiary i niestety środki zaradcze często nie nadążają za działaniami przestępczymi – zwykle tworzone są dopiero wtedy, gdy cyberwłamania czy cyberoszustwa stają się powszechne.

Bardzo istotną kwestią jest zatem uwzględnianie bezpieczeństwa informacji i danych już na etapie projektowania systemów i procedur. Niezwykle istotną sprawą

jest także odpowiednie przeszkolenie osób odpowiadających za przechowywanie danych oraz skuteczne egzekwowanie odpowiedzialności za uchybienia w tej dziedzinie. Propozycja powołania Agencji Cyberbezpieczeństwa jest zatem wyjściem naprzeciw nowoczesnym trendom technologicznym. To stworzenie instytucji realizującej zadania edukacyjne, prewencyjne i operacyjne.

Ochrona systemów informacyjnych oraz przetwarzanych w nich informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa. Stworzenie takiej instytucji jak AC, która zbierała będzie wszystkie informacje z całego obszaru administracji publicznej i jednocześnie z sektora prywatnego, pozwoli na szybka analizę danych oraz wdrażanie procedur operacyjnych, które w czasie rzeczywistym będą stawiały czoło zagrożeniom.

Początek trzeciej dekady XXI w. z jednej strony proces globalizacji, a z drugiej nowe doświadczenia cywilizacyjne związane z pandemią. W czasie pandemii COVID-19 przyspieszył proces cyfryzacji i dlatego zintegrowane działania dotyczące zapewnienia cyberbezpieczeństwa powinny stać się kluczowym elementem zapewnienia sprawnego funkcjonowania państwa. Obecnie każde znaczące zakłócenie funkcjonowania cyberprzestrzeni ma wpływ na bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania administracji publicznej, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo państwa. W związku z powyższym celem priorytetowym powinno być powoływanie takich instytucji, które mogą skutecznie realizować zadania w tym obszarze.

Agencja Cyberbezpieczeństwa jako podmiot umiejscowiony w nadzorze Prezesa Rady Ministrów oraz ściśle współpracujący z innymi podmiotami stanowiła będzie kluczową instytucję cywilnej ochrony interesów RP w cyberprzestrzeni.

2. Różnice między dotychczasowym a projektowanym stanem prawnym

W art. 2 wprowadza się kilka definicji ustawowych. Projektodawca zdecydował się nie wprowadzać nowego zbioru definicji ze względu na katalog znajdujący się w przepisach obowiązujących - art. 2 ustawy z dnia 5 lipca 2018 r. o krajowym

systemie cyberbezpieczeństwa. Proponuje się definicję danych na potrzeby ustawy jako dane wytwarzane i dostarczane w postaci cyfrowej. Ponadto określa się właściwości sprzętu elektronicznego - urządzenie umożliwiające przechowywanie lub przetwarzanie danych, którego prawidłowe działanie uzależnione jest od dopływu prądu elektrycznego, obecności pól elektromagnetycznych lub połączenia z innym urządzeniem.

W art. 3. Tworzy się Agencję Cyberbezpieczeństwa (AC), a w art. 4 określa się jej zadania: (1) koordynacja krajowego systemu cyberbezpieczeństwa; (2) rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych 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; (3) prowadzenie działań prewencyjno-edukacyjnych związanych z cyberbezpieczeństwem w sektorze publicznym i prywatnym; (4) budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa; (5) podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego; (6) podejmowanie działań kryptologicznych i ochraniających cybernetyczne zasoby państwa; (7) reagowanie na incydenty związane z bezpieczeństwem cybernetycznym i współpraca operacyjna z innymi służbami specjalnymi w celu likwidacji zagrożeń; (8) koordynowanie i rozwijanie krajowego systemu cyberbezpieczeństwa; (9) wspieranie jednostek nauki i szkolnictwa wyższego w zakresie bezpieczeństwa w cyberprzestrzeni; (10) monitorowanie rozwoju nowoczesnych technologii i ich wpływu na życie człowieka; (11) ocena i zarządzanie ryzykiem cyfrowym; (12) wymiana informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie.

Finansowanie AC zostało określone w art. 5. Zgodnie z przepisem, jego działalność będzie finansowana z odrębnej części budżetu państwa. Dysponentem części zgodnie z przepisami o finansach publicznych, będzie Szef AC Koszty realizacji zadań AC, w zakresie których – ze względu na wyłączenie ich jawności – nie mogą być stosowane przepisy o finansach publicznych, rachunkowości i zamówieniach publicznych, będą finansowane z utworzonego na ten cel funduszu operacyjnego. Zostanie zatem zastosowana procedura analogiczna jak w przypadku innych służb. Fundusz operacyjny nie może przekraczać 20% rocznego budżetu AC, a Szef AC określi w drodze zarządzenia szczegółowe zasady tworzenia i gospodarowania nim.

Następne przepisy regulują relacje AC z innymi podmiotami. Szef AC w zakresie wykonywania swoich zadań koordynuje działania podmiotów krajowego systemu cyberbezpieczeństwa: (1) operatorów usług kluczowych; (2) dostawców usług cyfrowych; (3) CSIRT MON; (4) CSIRT NASK; (5) CSIRT GOV; (6) sektorowych zespołów cyberbezpieczeństwa; (7) jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8, 9,_11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (8) instytutów badawczych; (9) Narodowego Banku Polskiego; (10) Banku Gospodarstwa Krajowego; (11) Urzędu Dozoru Technicznego; (12) Polskiej Agencji Żeglugi Powietrznej; (13) Polskiego Centrum Akredytacji; (14) Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkich funduszów ochrony środowiska i gospodarki wodnej; (15) spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej; (16) podmiotów świadczących usługi z zakresu cyberbezpieczeństwa; (17) organów właściwych do spraw cyberbezpieczeństwa; (18) Pojedynczego Punktu Kontaktowego do spraw cyberbezpieczeństwa. Ponadto w ramach swojej działalności AC będzie współpracować z innymi podmiotami, o których mowa w art. 7 ust. 8 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, tj. z (1) organami właściwymi do spraw cyberbezpieczeństwa; (2) Policją; (3) Żandarmerią Wojskową; (4) Strażą Graniczną; (5) Centralnym Biurem Antykorupcyjnym; (6) Agencją Bezpieczeństwa Wewnętrznego oraz Agencją Wywiadu; (7) Służbą Kontrwywiadu Wojskowego oraz Służbą Wywiadu Wojskowego; (8) sądami; (9) prokuraturą; (10)

organami Krajowej Administracji Skarbowej; (11) dyrektorem Rządowego Centrum Bezpieczeństwa; (12) Służbą Ochrony Państwa.

W art. 7 uregulowano obowiązki innych podmiotów w przedmiocie ustawy. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne są obowiązani, w zakresie swojego działania, do współdziałania z AC. Współdziałanie z AC będzie wiązało się z (1) wdrażaniem zaleceń Szefa AC dotyczących podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności; (2) stosowaniem oprogramowania spełniającego standardy AC; (3) umożliwieniem przeprowadzenia kontroli bezpieczeństwa systemów teleinformatycznych, zabezpieczeń danych i sprzętu elektronicznego; (4) umożliwieniem pracownikom uczestniczenia w szkoleniach AC. W przypadku niewykonywania wybranych obowiązków Szef AC będzie mógł wystąpić z wnioskiem do organu sprawującego nadzór nad podmiotem z informacją o niewykonaniu obowiązków lub z wnioskiem o podjęcie działań mających na celu ich wykonanie (w przypadku podmiotu sektora administracji publicznej. Wobec pozostałych podmiotów zostanie zastosowany przepis karny z możliwą karą grzywny.

Zgodnie z art. 8 na czele AC stoi Szef AC powoływany przez Prezesa Rady Ministrów, po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji. Na wniosek Szefa AC Prezes Rady Ministrów powołuje zastępcę Szefa AC po zasięgnięciu opinii Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji. Wymagania wobec Szefa AC i jego zastępcy są jednakowe: (1) posiadanie wyłączne obywatelstwa polskiego; (2) pełnia praw publicznych; (3) rękojmia należytego wykonywania zadań; (4) wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne"; (5) przynajmniej 5-letnie doświadczenie w zakresie cyberbezpieczeństwa. Szef AC może zostać odwołany w przypadku (1) rezygnacji; (2) zrzeczenia się obywatelstwa polskiego lub nabycia obywatelstwa innego państwa; (3) skazania prawomocnym wyrokiem sądu za popełnione przestępstwo lub przestępstwo

skarbowe; (4) utraty predyspozycji niezbędnych do zajmowania stanowiska; (5) niewykonywania obowiązków z powodu choroby trwającej nieprzerwanie ponad miesiąc. W przypadku zwolnienia stanowiska Szefa AC lub czasowej niemożności sprawowania przez niego funkcji, Prezes Rady Ministrów może powierzyć pełnienie obowiązków Szefa jego zastępcy na czas nie dłuższy niż miesiąc.

Do zadań Szefa AC należy (1) kierowanie pracą AC; (2) reprezentowanie AC w stosunkach prawnych z innymi podmiotami; (3) zarządzanie mieniem AC; (4) przedstawianie rocznej informacji o stanie cyberbezpieczeństwa państwa; (5) wykonywanie innych zadań określonych w ustawie. Szef AC może upoważnić zastępcę Szefa AC do wykonywania powierzonych mu zadań, z wyjątkiem kierowania pracą AC i przedstawiania rocznej informacji o stanie cyberbezpieczeństwa państwa.

Statut AC jest nadawany przez Prezesa Rady Ministrów w drodze zarządzenia. Regulaminy organizacyjne są nadawane przez Szefa AC, który może również tworzyć zespoły o charakterze stałym lub doraźnym, określając ich nazwę, skład osobowy oraz szczegółowy zakres i tryb działania.

Do AC w ramach art. 13 włącza się Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym (CSIRT GOV).

Na podstawie art. 14 Szef AC raz w tygodniu publikuje na stronie internetowej AC raport o stanie cyberbezpieczeństwa, zawierający ogólną ocenę bezpieczeństwa cyfrowego; komunikaty o ostrzeżeniach przed atakami; bieżące zalecenia w zakresie cyberbezpieczeństwa.

Szef AC będzie przekazywać Prezesowi Rady Ministrów informację o bieżącym stanie cyberbezpieczeństwa. Szczegółowy zakres informacji oraz tryb jej przekazywania określi Prezes Rady Ministrów w drodze zarządzenia.

AC przeprowadzać będzie szkolenia z zakresu cyberbezpieczeństwa. Szkolenia obowiązkowe dla organów administracji rządowej, organów samorządu terytorialnego, instytucji państwowych oraz przedsiębiorców wykorzystujących środki publiczne są nieodpłatne. Opłata za uczestnictwo w szkoleniu dla pracowników pozostałych podmiotów od osoby wynosi nie więcej niż 1/10 minimalnego miesięcznego wynagrodzenia za pracę, ustalanego na podstawie przepisów odrębnych. Wpływy z opłaty stanowią dochód AC.

Szef AC publikuje standardy oprogramowania i zarządzania bezpieczeństwem informacji, tworzone są na podstawie norm międzynarodowych oraz bieżących zaleceń Szefa AC dotyczących podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności.

Szef AC na podstawie analizy zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych wydaje organom administracji rządowej, organom samorządu terytorialnego, instytucjom państwowym oraz przedsiębiorcom wykorzystujących środki publiczne zalecenia dotyczące podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności. Wskazane podmioty mogą wnieść do Szefa AC zastrzeżenia do zaleceń z uwagi na negatywny wpływ rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności w terminie 7 dni od dnia otrzymania zaleceń. Szef AC odnosi się do zastrzeżeń niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania i podtrzymuje lub zmienia zalecenia. Podmioty, które otrzymały zalecenia, w terminie miesiąca od dnia ich otrzymania informują Szefa AC o sposobie i zakresie ich wykonania. Niewykonanie zaleceń przez podmiot sektora administracji publicznej stanowi podstawę do wystąpienia przez Szefa AC do organu sprawującego nadzór nad podmiotem z informacją o niewykonaniu zaleceń lub z wnioskiem o podjęcie działań mających na celu ich wykonanie. W przypadku pozostałych podmiotów, które nie wykonały zaleceń, stosuje się przepis karny.

AC może przeprowadzać w organach administracji rządowej, organach samorządu terytorialnego, instytucjach państwowym oraz przedsiębiorstwach wykorzystujących środki kontrolę bezpieczeństwa systemów teleinformatycznych, zabezpieczeń danych i sprzętu elektronicznego. Kontrole bezpieczeństwa są przeprowadzane zgodnie z rocznym planem przeprowadzania kontroli bezpieczeństwa, opracowywanym w terminie do 30 listopada każdego roku. Szefa AC uzgadnia plan z ministrem właściwym do spraw informatyzacji. Szef AC po sporządzeniu listy informuje właściwe podmioty o wpisaniu ich do planu. W

uzasadnionych przypadkach kontrola bezpieczeństwa może zostać przeprowadzona z pominięciem planu.

Kontrola bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu teleinformatycznego w celu identyfikacji podatności, przez które rozumie się słabość zasobu lub zabezpieczenia systemu teleinformatycznego, która może zostać wykorzystana przez zagrożenie, wpływających na integralność, poufność, rozliczalność i dostępność tego systemu.

Kontrola bezpieczeństwa powinna być prowadzona z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie teleinformatycznym podlegającym tej ocenie. W celu minimalizacji negatywnych następstw kontroli bezpieczeństwa AC uzgadnia z podmiotem ramowe warunki przeprowadzania tej kontroli, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach kontroli bezpieczeństwa testów bezpieczeństwa.

Tak jak obecnie w podobnych procedurach AC będzie mogło 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. AC w czasie kontroli bezpieczeństwa 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 teleinformatycznego. Informacje uzyskane przez AC w wyniku przeprowadzania kontroli bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych AC oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Po przeprowadzeniu kontroli bezpieczeństwa AC sporządza i przekazuje podmiotowi, którego system podlegał kontroli bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych czynności, wskazanie wykrytych podatności systemu teleinformatycznego oraz zalecenia pokontrolne. Jeżeli wykryta podatność

może wystąpić w innych systemach teleinformatycznych, AC informuje niezwłocznie Prezesa Rady Ministrów o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach teleinformatycznych.

Zgodnie z art. 22 w celu zapobiegania, przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących podmiotów krajowego systemu cyberbezpieczeństwa lub danych w nich przetwarzanych oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, AC wdraża w tych podmiotach, zgodnie z planem rocznym, system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet. Koszty wdrożenia i utrzymania systemu ostrzegania pokrywa AC. AC, w drodze porozumienia, uzgadnia z podmiotem techniczne aspekty uczestnictwa w systemie ostrzegania oraz model konfiguracji systemu.

W przypadku powzięcia informacji o wystąpieniu zdarzenia o charakterze terrorystycznym żądać od podmiotów krajowego systemu cyberbezpieczeństwa przedstawienia informacji o budowie, funkcjonowaniu oraz zasadach eksploatacji posiadanych systemów teleinformatycznych, w tym informacji obejmujących hasła komputerowe, kody dostępu i inne dane umożliwiające dostęp do systemu oraz ich używanie, w celu zapobiegania, reagowania na zdarzenia o charakterze terrorystycznym, a także zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców. Informacje i dane podlegają ochronie przewidzianej w przepisach o ochronie informacji niejawnych i mogą być udostępniane jedynie funkcjonariuszom AC prowadzącym w danym postępowaniu czynności operacyjno-rozpoznawcze i ich przełożonym, uprawnionym do sprawowania nadzoru nad tymi czynnościami.

W celu zapobiegania, przeciwdziałania i wykrywania przestępstw o charakterze terrorystycznym oraz ścigania ich sprawców sąd, na pisemny wniosek Szefa AC, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, w drodze postanowienia, może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym określonych danych informatycznych mających związek ze zdarzeniem o charakterze terrorystycznym lub określonych usług teleinformatycznych służących lub

wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym. Postanowienie wydaje Sąd Okręgowy w Warszawie.

W przypadkach niecierpiących zwłoki, jeżeli mogłaby ona spowodować zdarzenie o charakterze terrorystycznym, Szef AC, po uzyskaniu pisemnej zgody Prokuratora Generalnego, może zarządzić blokadę dostępności, zwracając się jednocześnie do sądu z wnioskiem o wydanie postanowienia w tej sprawie. Usługodawca świadczący usługi drogą elektroniczną jest obowiązany do natychmiastowego dokonania czynności określonych w postanowieniu sądu lub przekazanym mu żądaniu Szefa AC. Blokadę dostępności zarządza się na okres nie dłuższy niż 30 dni. Sąd może na pisemny wniosek Szefa AC, złożony po uzyskaniu pisemnej zgody Prokuratora Generalnego, wydać postanowienie o jednorazowym przedłużeniu blokady dostępności na okres nie dłuższy niż 3 miesiące, jeżeli nie ustały przyczyny jej zarządzenia.

Blokady dostępności zaprzestaje się w przypadku:(1) nieudzielenia przez sąd w terminie 5 dni od złożenia wniosku zgody na zarządzenie przez Szefa AC blokady dostępności; (2) nieudzielenia przez sąd zgody na przedłużenie blokady dostępności; (3) upływu okresu, na który blokada dostępności została wprowadzona.

Szef AC prowadzi rejestr zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych. Rejestr zawiera w szczególności opis stwierdzonego zdarzenia naruszającego bezpieczeństwo systemu oraz sposób działania podmiotu powodującego naruszenie bezpieczeństwa oraz opis szkód w systemie powstałych lub mogących powstać wskutek zdarzenia naruszającego bezpieczeństwo systemu. Dane przekazuje Szefowi AC administrator systemu teleinformatycznego, o którym mowa po wykryciu zdarzenia naruszającego bezpieczeństwo tego systemu. Dane z rejestru są udostępniane Prezesowi Rady Ministrów.

Szef AC przedstawia Sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji roczną informację o stanie cyberbezpieczeństwa państwa.

W ramach AC zatrudnieni są pracownicy i funkcjonariusze. Funkcjonariusze AC pełną służbę w ramach CSIRT GOV. Funkcjonariuszom AC przysługują uprawnienia funkcjonariuszy, o których mowa w ustawie z dnia 24 maja 2002 r. o Agencji

Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Pracownikiem lub funkcjonariuszem AC może być obywatel polski o nieposzlakowanej opinii, który nie był skazany prawomocnym wyrokiem sądu za przestępstwo lub przestępstwo skarbowe, korzystający z pełni praw publicznych, posiadający wykształcenie wyższe oraz zdolność fizyczną i psychiczną do pracy lub służby w formacjach podległych szczególnej dyscyplinie służbowej, której gotów jest się podporządkować, a także dający rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych. Przyjęcie kandydata do pracy lub służby w AC następuje po przeprowadzeniu postępowania kwalifikacyjnego mającego na celu ustalenie, czy kandydat spełnia warunki zatrudnienia.

Postępowanie kwalifikacyjne rozpoczyna się od złożenia podania o zatrudnienie, kwestionariusza osobowego kandydata, a także dokumentów stwierdzających wymagane wykształcenie i kwalifikacje zawodowe oraz zawierających dane o uprzednim zatrudnieniu. Następnie kandydaci wypełniają test wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru. Po wypełnieniu testu przechodzą badanie psychologiczne i uczestniczą w rozmowie kwalifikacyjnej. Po rozmowie komisja na podstawie wcześniejszych procedur ustala zdolność fizyczną i psychiczną do pracy lub służby w AC; sprawdza w ewidencjach, rejestrach i kartotekach prawdziwość danych zawartych w kwestionariuszu osobowym kandydata i przeprowadza wraz z innymi służbami postępowanie sprawdzające określone w przepisach o ochronie informacji niejawnych.

Podczas przeprowadzania postępowania kandydaci nie mogą korzystać z pomocy innych osób; posługiwać się urządzeniami służącymi do przekazu, odbioru lub zapisu informacji lub korzystania z pomocniczych materiałów, niedopuszczonych do ich wykorzystania; zakłócania przebiegu etapów postępowania kwalifikacyjnego. Kandydaci z najwyższymi wynikami postępowania mają szansę na pełnienie służby w CSIRT GOV.

Art. 32-33 stanowią przepisy karne związane z niewykonywaniem zaleceń i obowiązków opisanych wyżej. Zgodnie z nimi za popełnienia takiego zaniechanie grozi grzywna. Funkcjonariusz AC, który wbrew przepisom ustawy wykorzystuje

informacje uzyskane podczas lub w związku z pełnieniem obowiązków służbowych do celów niezwiązanych ze pełnieniem obowiązków służbowych podlega karze pozbawienia wolności od 6 miesięcy do lat 8. W postaci kwalifikowanej działania w celu osiągnięcia korzyści osobistej lub majątkowej kara pozbawienia wolności może wynosić od lat 2 do lat 12.

W przepisach zmieniających dokonuje się nowelizacji ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu; ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2020 r. poz. 1856, z 2021 r. poz. 159) oraz ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. W zakresie zmiany z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu przenosi się funkcjonowanie CSIRT GOV spod Agencji Bezpieczeństwa Wewnętrznego pod kierownictwo AC.

Jak uregulowano w przepisach przejściowych, Szef ABW przekaże Szefowi AC w terminie 6 miesięcy od dnia wejścia w życie ustawy zarządzanie CSIRT GOV. W tym momencie Szef AC stanie się dysponentem majątku CSIRT GOV oraz stroną stosunków prawnych zespołu. Wszyscy pracownicy i funkcjonariusze ABW zatrudnieni w ramach CSIRT GOV, po upływie terminu, o którym mowa w ust. 1, stają się pracownikami i funkcjonariuszami AC.

Proponuje się wejście ustawy w życie z dniem 1 stycznia 2022 r.

3. Przewidywane skutki społeczne, gospodarcze, finansowe i prawne

Działanie Agencji Cyberbezpieczeństwa pozwoli na szybką analizę danych oraz wdrażanie procedur operacyjnych, które w czasie rzeczywistym będą stawiały czoło zagrożeniom. Przedsiębiorcy będą mieli zapewnione lepsze zabezpieczenie swoich działalności gospodarczych, a obywatele - swoich danych osobowych. Dzięki koordynacji systemu w ramach Agencji Cyberbezpieczeństwa reakcje na ataki będzie szybsza i sprawniejsza niż obecnie. To z kolei może zachęcić nowe inwestorów zagranicznych. Wprowadzenie proponowanej ustawy stworzy szansę na większą stabilność dla prowadzenia działalności gospodarczej i szybszy wzrost gospodarczy w następnych latach. To także lepsze zabezpieczenie infrastruktury krytycznej.

Innym ważnym skutkiem społecznym będą szkolenia z zakresu cyberbezpieczeństwa, które z czasem mogą zbudować świadomość społeczną na temat bezpieczeństwa cyfrowego.

Z punktu widzenia systemu prawnego krajowy system bezpieczeństwa zyska instytucję koordynującą. Wszystkie działania operacyjne podejmowane przez CSIRT GOV są dzisiaj implementowane na podstawie ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Nie ma zatem niebezpieczeństwa braku przygotowania infrastrukturalnego lub systemowego - proponowane procedury już funkcjonują, tylko w ramach innych podmiotów.

Maksymalne wydatki związane z wykonaniem proponowanej ustawy zostały określone w art 39:

1) w 2022 r. – 117.000 tys. zł;
2) w 2023 r. – 264.000 tys. zł;
3) w 2024 r. – 527.000 tys. zł;
4) w 2025 r. – 765.000 tys. zł;
5) w 2026 r. – 434.000 tys. zł;
6) w 2027 r. – 444.000 tys. zł;
7) w 2028 r. – 454.000 tys. zł;
8) w 2029 r. – 464.000 tys. zł;
9) w 2030 r. – 475.000 tys. zł;
10) w 2031 r. – 486.000 tys. zł.

Wydatki związane będą z wydatkami bieżącymi (wynagrodzenia, koszty bieżące funkcjonowania) oraz w szczególności w pierwszych latach z inwestycjami. Inwestycje mają zbudować potencjał infrastrukturalny Agencji Cyberbezpieczeństwa i są konieczne do prawidłowego wykonywania powierzonych jej zadań.

4. Źródła finansowania

Zgodnie z art. 5 wydatki wskazane powyżej finansowane będą z odrębnej części budżetu państwa. Koszty realizacji zadań AC, w zakresie których – ze względu na wyłączenie ich jawności – nie mogą być stosowane przepisy o finansach

publicznych, rachunkowości i zamówieniach publicznych, są finansowane z utworzonego na ten cel funduszu operacyjnego. Fundusz operacyjny nie będzie przekraczać 20% rocznego budżetu AC.

5. Założenia podstawowych aktów wykonawczych

Art. 21 ust. 2. Rozporządzenie Prezesa Rady Ministrów sposób niszczenia materiałów z kontroli bezpieczeństwa Agencji Cyberbezpieczeństwa.

Prezes Rady Ministrów wskaże, że informacje uzyskane przez Agencję Cyberbezpieczeństwa w wyniku przeprowadzania kontroli bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych Agencji Cyberbezpieczeństwa oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Prezes Rady Ministrów określi procedure zniszczenia, sposób ustalania składu komisji, w której będą przedstawiciele podmiotu, którego dane są niszczone, oraz wzór protokołu zniszczenia, mając na uwadze rodzaj materiałów podlegających zniszczeniu.

Art. 21 ust. 3. Rozporządzenie Rady Ministrów w sprawie określenia trybu i warunków przeprowadzania kontroli bezpieczeństwa Agencji Cyberbezpieczeństwa

Rada Ministrów określi czynności niezbędne do przeprowadzenia kontroli bezpieczeństwa. w szczególności zobowiąże Agencję Cyberbezpieczeństwa do uzgodnienia z podmiotem kontrolowanym ramowych warunki przeprowadzenia kontroli, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach kontroli bezpieczeństwa testów bezpieczeństwa. Rada Ministrów w szczególności weźmie pod uwagę minimalizację zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności.

Art. 22 ust. 9. Rozporządzenie Prezesa Rady Ministrów warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania w zakresie cyberbezpieczeństwa

Prezes Rady Ministrów określi warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w szczególności określi czynności niezbędne do jego uruchomienia i utrzymania oraz wzór porozumienia między Agencją Cyberbezpieczeństwa a podmiotem objętym systemem w sprawie technicznych aspektów uczestnictwa w systemie ostrzegania oraz modelu konfiguracji systemu. Prezes Rady Ministrów będzie kierował się potrzebą zapewnienia bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa.

Art. 24 ust. 14. Rozporządzenie Prezesa Rady Ministrów sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania dokumentów

Prezes Rady Ministrów określi sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków. Prezes Rady Ministrów uwzględni w szczególności potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów, a także przejrzystość procedury dla zainteresowanych stron.

6. Wpływ na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców

Proponowana ustawa pozytywnie wpłynie na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców poprzez zwiększenie poziom cyberbezpieczeństwa systemów teleinformatycznych oraz podniesienie kompetencji pracowników w zakresie cyberbezpieczeństwa.

7. Oświadczenie o zgodności projektu ustawy z prawem Unii Europejskiej albo oświadczenie, że przedmiot projektowanej regulacji nie jest objęty prawem Unii Europejskiej

Projektowana ustawa jest zgodna z prawem Unii Europejskiej. Projekt ustawy nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji lub uzgodnienia.

8. Oświadczenie o zgodności projektu ustawy z Konstytucją RP

W ocenie wnioskodawcy proponowany projekt jest zgodny z Konstytucją RP.

9. Konsultacje społeczne

Projekt nie był poddany konsultacjom społecznym.

Warszawa, 18 października 2021 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (przedstawiciel wnioskodawców: poseł Krzysztof Gawkowski)

Na podstawie art. 34 ust. 9 uchwały Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 roku – Regulamin Sejmu Rzeczypospolitej Polskiej (Monitor Polski z 2021 r. poz. 483 i 607) sporządza się następującą opinię:

1. Przedmiot projektu ustawy

W projekcie ustawy przewiduje się utworzenie Agencji Cyberbezpieczeństwa, zwanej dalej „Agencją" lub „AC". Proponowana ustawa określa zakres i zasady działania oraz strukturę Agencji. Zaproponowany katalog zadań AC obejmuje m.in.: koordynację krajowego systemu cyberbezpieczeństwa; podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego; reagowanie na incydenty związane z bezpieczeństwem cybernetycznym i współpracę operacyjną z innymi służbami specjalnymi w celu likwidacji zagrożeń; ocenę i zarządzanie ryzykiem cyfrowym; wymianę informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami i podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie. Działalność AC byłaby finansowana z odrębnej części budżetu państwa. Szef AC w zakresie wykonywania swoich zadań koordynowałby działania podmiotów krajowego systemu cyberbezpieczeństwa, określonych w art. 4 punkty 1–18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], a także współpracował z innymi podmiotami określonymi w art. 7 ust. 8 tej ustawy. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne byliby obowiązani, w zakresie swojego działania, do współdziałania z AC w sposób określony proponowaną

[1] Dz. U. z 2020 r. poz. 1369.

regulacją. Pozostałe przepisy regulują strukturę i organizację Agencji, szczegółowe zasady działalności AC oraz zasady i tryb zatrudniania pracowników i funkcjonariuszy Agencji. Projekt zawiera przepisy karne.

Projektodawcy proponują zmianę ustaw: z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2], z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3] oraz z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projekt zawiera postanowienia przejściowe. Projektowana ustawa ma wejść w życie z dniem 1 stycznia 2022 r.

2. Stan prawa Unii Europejskiej w materii objętej projektem ustawy

Z uwagi na przedmiot projektu ustawy należy uwzględnić:

- art. 45 Traktatu o funkcjonowaniu Unii Europejskiej (dalej: TfUE), ustanawiający swobodę przepływu pracowników wewnątrz Unii;

- 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[4], dalej jako „dyrektywa (UE) 2016/1148" lub „dyrektywa".

Dyrektywa (UE) 2016/1148 ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego (art. 1 ust. 1). Jednocześnie 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 (art. 1 ust. 6).

3. Analiza przepisów projektu ustawy pod kątem ustalonego stanu prawa Unii Europejskiej

3. Opiniowany projekt ustawy wymaga oceny zgodności z prawem Unii Europejskiej w dwóch kwestiach: 1) zgodności z zasadą swobodnego przepływu pracowników wewnątrz Unii (art. 45 TfUE), oraz 2) zgodności z dyrektywą (UE) 2016/1148.

3.1. W art. 8 ust. 4 projektu ustanowiono wymóg posiadania wyłącznie obywatelstwa polskiego w odniesieniu do osoby powoływanej na stanowisko Szefa lub zastępcy Szefa AC. Wymóg obywatelstwa polskiego przewidziano także w odniesieniu do pracowników i funkcjonariuszy AC (art. 28 ust. 1 projektu). Oznacza to, że Szefem lub zastępcą Szefa AC, funkcjonariuszem lub

[2] Dz. U. z 2020 r. poz. 27 i 2320.

[3] Dz. U. z 2020 r. poz. 1856 oraz z 2021 r. poz. 159.

[4] Dz. Urz. UE L 194 z 19.7.2016 r., str. 1.

pracownikiem AC nie będzie mogła być osoba, która nie jest obywatelem polskim. Pełnienie funkcji Szefa lub zastępcy AC, jak również posiadanie statusu funkcjonariusza lub pracownika AC, byłoby więc wykluczone w odniesieniu do obywateli innych niż RP państw członkowskich UE. Proponowane przepisy należy ocenić pod kątem zgodności z zasadą swobody przepływu pracowników w rozumieniu art. 45 TfUE.

Zasada swobodnego przepływu pracowników wewnątrz Unii obejmuje zniesienie wszelkiej dyskryminacji ze względu na przynależność państwową między pracownikami państw członkowskich w zakresie zatrudnienia (art. 45 ust. 1 i 2 TfUE). Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (dalej: Trybunał) swoboda przepływu pracowników oznacza zniesienie także barier o charakterze niedyskryminującym. Za sprzeczne z art. 45 TfUE Trybunał uznaje regulacje krajowe, które uniemożliwiają lub zniechęcają pracownika – obywatela UE do skorzystania ze swobody przemieszczania się do innego państwa członkowskiego. Postanowienia art. 45 TfUE nie mają jednak zastosowania do zatrudnienia w administracji publicznej (art. 45 ust. 4 TfUE). Wyłączenie to ma charakter wyjątku, nie można więc traktować go rozszerzająco. Jego treść, wraz z pojęciem „administracja publiczna", jest przedmiotem orzecznictwa Trybunału.[5]

Trybunał stwierdził, że pojęcie administracji publicznej w rozumieniu przepisów TfUE należy interpretować i stosować jednolicie w całej Unii i w związku z tym nie może być w pełni pozostawione uznaniu państw członkowskich. Zgodnie z orzecznictwem Trybunału art. 45 ust. 4 TfUE będzie miał zastosowanie tylko do stanowisk, które są związane z bezpośrednim lub pośrednim udziałem w wykonywaniu władzy powierzonej przez prawo publiczne oraz funkcji, które mają na celu ochronę ogólnych interesów państwa lub władz publicznych i wymagają zatem od osób dysponujących tymi uprawnieniami istnienia szczególnego relacji solidarności z państwem oraz wzajemności praw i obowiązków leżących u podstaw więzów obywatelstwa. Trybunał stoi na stanowisku, że art. 45 ust. 4 TfUE może być zastosowany wówczas, gdy wykonywanie uprawnień przyznanych przez prawo publiczne odbywa się regularnie oraz nie jest bardzo niewielką częścią prowadzonej aktywności. Wyłączenia określonego w art. 45 ust. 4 TFUE nie stosuje się natomiast do stanowisk, które podlegają wprawdzie państwu lub innym podmiotom prawa

---

[5] Zob. m.in. wyrok Trybunału z 17 grudnia 1980 r. w sprawie Komisja przeciwko Belgii, 149/79, ECLI:EU:C:1980:297, punkty 10, 12, 18 i 19, wyrok Trybunału z 16 czerwca 1987 r. w sprawie Komisja przeciwko Włochom, 225/85, ECLI:EU:C:1987:284, pkt 7, wyrok Trybunału z dnia 2 lipca 1996 r. w sprawie Komisja przeciwko Grecji, C-290/94, ECLI:EU:C:1996:265, pkt 2, wyrok Trybunału z dnia 30 września 2003 r. w sprawie Colegio de Oficiales de la Marina Mercante Española, C-405/01, ECLI:EU:C:2003:515, pkt 40, wyrok Trybunału z 30 września 2003 r. w sprawie Anker i inni, C-47/02, ECLI:EU:C:2003:516, punkty 57–60, wyrok Trybunału z 10 września 2014 r. w sprawie Haralambidis, C-270/13, ECLI:EU:C:2014:2185, punkty 42–45, wyrok Trybunału z 6 października 2015 r. w sprawie Brouillard, C-298/14, ECLI:EU:C:2015:652, punkty 30–32, wyrok Trybunału z 22 czerwca 2017 r. w sprawie Bechtel, C-20/16, punkty 34 i 35.

publicznego, jednak nie wiążą się ze współdziałaniem przy wykonywaniu zadań należących do administracji publicznej we właściwym znaczeniu.

Dodatkową wskazówką interpretacyjną może być treść komunikatu Komisji z 11 grudnia 2002 r. dotyczącego swobody przepływu pracowników[6] oraz komunikatu Komisji z 13 lipca 2010 r. do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Potwierdzenie zasady swobodnego przepływu pracowników: prawa oraz główne zmiany*[7]. Komisja Europejska uważa, że wyjątek dotyczący administracji publicznej odnosi się przede wszystkim do sił zbrojnych, policji, wymiaru sprawiedliwości, administracji skarbowej oraz dyplomacji[8]. Może odnosić się do stanowisk w administracji publicznej szczebla centralnego lub lokalnego, których sprawowanie zakłada wykonywanie władzy państwowej, w związku z procesem tworzenia lub stosowania prawa oraz nadzoru nad jednostkami podporządkowanymi. Zgodnie z orzecznictwem Trybunału Komisja podkreśla, że art. 45 ust. 4 TfUE ma charakter wyjątku, który należy interpretować w sposób zawężający, a kryteria kwalifikujące do skorzystania z wyjątku należy rozpatrywać indywidualnie.

Na gruncie przepisów projektu powstaje pytanie, czy w odniesieniu do stanowisk Szefa i zastępcy Szefa AC oraz statusów funkcjonariusza i pracownika Agencji ma zastosowanie wyjątek określony w art. 45 ust. 4 TfUE, a więc czy są one wyłączone ze swobody przepływu pracowników wewnątrz Unii.

Zgodnie z projektem zarówno Szefa AC, jak i zastępcę Szefa AC (na wniosek Szefa AC) powoływałby Prezes Rady Ministrów, po zasięgnięciu opinii sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji (art. 8 ust. 2 i 3). Szefem AC lub zastępcą Szefa AC mogłaby zostać osoba, która m.in. spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne" (art. 8 ust. 4 pkt 4). Szef AC przekazywałby Prezesowi Rady Ministrów informację o bieżącym stanie cyberbezpieczeństwa (art. 15). Szef AC przedstawiałby sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji roczną informację o stanie bezpieczeństwa państwa (art. 26).

Biorąc pod uwagę przewidziane w projekcie ustawy kompetencje, zakres zadań oraz szczególną pozycję ustrojową Szefa AC i zastępcy Szefa AC należy uznać, że sprawowanie tego urzędu będzie wymagało istnienia szczególnych relacji w stosunku do państwa, wynikających z więzów obywatelstwa. Pełnienie funkcji Szefa AC (zastępcy Szefa AC) byłoby więc zatrudnieniem w administracji publicznej, spełniającym kryterium wyjątku przewidzianego w art. 45 ust. 4 TfUE. Należy uznać, że w omawianym przypadku wymóg obywatelstwa

---

[6] *Communication from the Commission "Free movement of workers – achieving the full benefits and potential"* (COM(2002) 694 final). Dokument niedostępny w języku polskim.

[7] KOM(2010) 373 wersja ostateczna.

[8] Jednocześnie Komisja Europejska wyraźnie zastrzega, że nie wszystkie stanowiska w wymienionych przez nią dziedzinach administracji publicznej wiążą się z wykonywaniem władzy publicznej i odpowiedzialnością za ochronę ogólnych interesów państwa.

polskiego jest usprawiedliwiony, zasada swobody przepływu pracowników nie ma zastosowania, a projektowany przepis nie jest sprzeczny z prawem UE.

Analizy wymaga ponadto przewidziany przez projektodawców wymóg obywatelstwa polskiego w odniesieniu do pracowników i funkcjonariuszy AC (art. 28 ust. 1 projektu). Zgodnie z projektowana regulacją w ramach AC zatrudniani byliby pracownicy i funkcjonariusze, przy czym funkcjonariusze AC pełniliby służbę w ramach CSIRT GOV, natomiast w pozostałych jednostkach AC zatrudnieni byliby pracownicy AC (art. 27). Pracownikiem lub funkcjonariuszem AC mogłaby być osoba m.in. posiadająca zdolność fizyczną i psychiczną do pracy lub służby w formacjach podległych szczególnej dyscyplinie służbowej, której gotów jest się podporządkować, a także dająca rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych (art. 28 ust. 1). Na podstawie postępowania kwalifikacyjnego Szef AC będzie mógł podjąć decyzję o powołaniu do służby w CSIRT GOV kandydatów z najwyższymi wynikami postępowania (art. 29). W zakresie nieregulowanym proponowaną ustawą funkcjonariuszom AC przysługiwałyby uprawnienia funkcjonariuszy określone w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (art. 31).

Biorąc pod uwagę proponowane przyznanie funkcjonariuszom AC uprawnień funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu należy uznać, że pełnienie służby w charakterze funkcjonariusza AC będzie wymagało istnienia szczególnych relacji w stosunku do państwa, wynikających z więzów obywatelstwa. Pełnienie służby w charakterze funkcjonariusza AC byłoby więc zatrudnieniem w administracji publicznej, spełniającym kryterium wyjątku przewidzianego w art. 45 ust. 4 TfUE. Przewidziany w art. 28 ust. 1 projektu wymóg obywatelstwa polskiego w odniesieniu do funkcjonariuszy AC należy więc uznać za usprawiedliwiony. Projektowany przepis nie jest w omawianym zakresie sprzeczny z prawem UE.

Wątpliwości z punktu widzenia prawa UE budzi natomiast wymóg obywatelstwa polskiego w odniesieniu do pracowników AC. W proponowanej regulacji nie określono zakresu zadań realizowanych przez poszczególne grupy pracowników Agencji ani przysługujących im uprawnień. Przyjęcie proponowanej ustawy w obecnym kształcie mogłoby prowadzić do sytuacji, że nie wszystkie stanowiska, na których byliby zatrudnieni pracownicy Agencji, wiązałyby się z wykonywaniem władzy publicznej i odpowiedzialnością za ochronę ogólnych interesów państwa. Należy zatem uznać, że posiadanie jedynie ogólnie określonego statusu pracownika Agencji nie stanowi zatrudnienia w administracji publicznej w rozumieniu art. 45 ust. 4 TfUE. Przewidziany w art. 28 ust. 1 projektu wymóg obywatelstwa polskiego w odniesieniu do wszystkich pracowników AC nie jest usprawiedliwiony. Projektowany przepis w omawianym zakresie jest sprzeczny z prawem UE.

3.2. Zgodnie z proponowaną ustawą do zadań tworzonej Agencji ma należeć koordynacja krajowego systemu cyberbezpieczeństwa (art. 4 pkt 1 projektu). W zakresie wykonywania tego zadania Szef AC koordynowałby działania podmiotów wchodzących w skład krajowego systemu

cyberbezpieczeństwa, określonych w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa[9]. Należy zauważyć, że ustawa ta w zakresie swojej regulacji wdraża dyrektywę (UE) 2016/1148. Ze względu na przedmiot projektu ustawy można w szczególności wskazać implementowane przez ustawę o krajowym systemie cyberbezpieczeństwa postanowienia dyrektywy dotyczące wyznaczenia właściwego organu krajowego ds. bezpieczeństwa sieci i systemów informatycznych lub większej ich liczby (zwanych dalej „właściwym organem"), które są obowiązane do monitorowania stosowania dyrektywy na poziomie krajowym (art. 8), jak również dotyczące współpracy między właściwym organem, pojedynczym punktem kontaktowym i CSIRT w zakresie wypełnienia obowiązków określonych w dyrektywie (art. 9). Należy uznać, że proponowana ustawa, zakładająca powołanie Agencji koordynującej działalność podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, nie narusza postanowień dyrektywy (UE) 2016/1148.

4. Konkluzja

Artykuł 28 ust. 1 projektu ustawy o Agencji Cyberbezpieczeństwa – w zakresie, w jakim ustanawia wymóg obywatelstwa w odniesieniu do pracowników Agencji Cyberbezpieczeństwa (punkt 3.1 *in fine* niniejszej opinii) – jest sprzeczny z prawem UE.

W pozostałym zakresie projekt ustawy nie narusza prawa Unii Europejskiej.

Autor:
Marcin Fryźlewicz
ekspert ds. legislacji
w Biurze Analiz Sejmowych

Akceptował:
Dyrektor
Biura Analiz Sejmowych
Sobolewski
Przemysław Sobolewski

[9] Zgodnie z art. 6 ust. 1 projektu oraz art. 37 pkt 2 (dotyczącym zmiany art. 4 ustawy o krajowym systemie cyberbezpieczeństwa).

SEJM
RZECZYPOSPOLITEJ POLSKIEJ

BIURO ANALIZ SEJMOWYCH
KANCELARII SEJMU

Warszawa, 18 października 2021 r.

BAS-WAPM-2457/21

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie stwierdzenia – w trybie art. 95a ust. 3 regulaminu Sejmu – czy poselski projekt ustawy o Agencji Cyberbezpieczeństwa (przedstawiciel wnioskodawców: poseł Krzysztof Gawkowski) jest projektem ustawy wykonującej prawo Unii Europejskiej

W projekcie ustawy przewiduje się utworzenie Agencji Cyberbezpieczeństwa, zwanej dalej „Agencją" lub „AC". Proponowana ustawa określa zakres i zasady działania oraz strukturę Agencji. Zaproponowany katalog zadań AC obejmuje m.in.: koordynację krajowego systemu cyberbezpieczeństwa; podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego; reagowanie na incydenty związane z bezpieczeństwem cybernetycznym i współpracę operacyjną z innymi służbami specjalnymi w celu likwidacji zagrożeń; ocenę i zarządzanie ryzykiem cyfrowym; wymianę informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami i podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie. Działalność AC byłaby finansowana z odrębnej części budżetu państwa. Szef AC w zakresie wykonywania swoich zadań koordynowałby działania podmiotów krajowego systemu cyberbezpieczeństwa, określonych w art. 4 punkty 1–18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], a także współpracował z innymi podmiotami określonymi w art. 7 ust. 8 tej ustawy. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne byliby obowiązani, w zakresie swojego działania, do współdziałania z AC w sposób określony proponowaną regulacją. Pozostałe przepisy regulują strukturę i organizację Agencji, szczegółowe zasady działalności AC oraz zasady i tryb zatrudniania pracowników i funkcjonariuszy Agencji. Projekt zawiera przepisy karne i postanowienia przejściowe. Projektodawcy proponują zmianę ustaw: z dnia 24 maja 2002 r.

[1] Dz. U. z 2020 r. poz. 1369.

o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2], z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3] oraz z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projekt nie zawiera przepisów mających na celu wykonanie prawa UE.

Projekt ustawy o Agencji Cyberbezpieczeństwa **nie jest projektem ustawy wykonującej** prawo Unii Europejskiej.

Autor:
Marcin Fryźlewicz
ekspert ds. legislacji
w Biurze Analiz Sejmowych

Akceptował:
Dyrektor
Biura Analiz Sejmowych
Sobolewski
Przemysław Sobolewski

[2] Dz. U. z 2020 r. poz. 27 i 2320.
[3] Dz. U. z 2020 r. poz. 1856 oraz z 2021 r. poz. 159.

Krzysztof Gawkowski

Przewodniczący Koalicyjnego Klubu Parlamentarnego Lewicy

Warszawa, 15 listopada 2021 r.

Szanowna Pani
Elżbieta Witek
Marszałek Sejmu RP

Szanowna Pani Marszałek,

Na podstawie art. 36 ust 1a Regulaminu Sejmu Rzeczypospolitej Polskiej jako przedstawiciel wnioskodawców wnoszę

autopoprawkę do poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (EW-020-674/21).

Autopoprawkę przekazuję w załączeniu.

Z poważaniem

Krzysztof Gawkowski

Autopoprawka do poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (EW-020-674/21).

Pkt. 5 uzasadnienia nadać brzmienie:

„5. Założenia podstawowych aktów wykonawczych

Art. 21 ust. 2. Rozporządzenie Prezesa Rady Ministrów sposób niszczenia materiałów z kontroli bezpieczeństwa Agencji Cyberbezpieczeństwa.

Prezes Rady Ministrów wskaże, że informacje uzyskane przez Agencję Cyberbezpieczeństwa w wyniku przeprowadzania kontroli bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych Agencji Cyberbezpieczeństwa oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu. Prezes Rady Ministrów określi procedurę zniszczenia, sposób ustalania składu komisji, w której będą przedstawiciele podmiotu, którego dane są niszczone, oraz wzór protokołu zniszczenia, mając na uwadze rodzaj materiałów podlegających zniszczeniu.

Procedura niszczenia będzie obejmować bezpowrotne usunięcie informacji zapisanych na nośnikach cyfrowych oraz usunięcie informacji zapisanych na nośnikach fizycznych w sposób uniemożliwiający odczytanie informacji.

W skład komisji wchodzić będzie przedstawiciel Agencji Cyberbezpieczeństwa, przedstawiciel podmiotu, którego dane są niszczone, a także – na wniosek tego podmiotu – przedstawiciel organizacji pozarządowej.

Protokół zniszczenia obejmuje opisanie nośnika, na którym znajdowały się zapisane dane, sposób zniszczenia i wskazanie czy dane zostały skutecznie zniszczone. Pod protokołem widnieją podpisy wszystkich członków komisji. Protokół sporządzany jest w dwóch jednobrzmiących egzemplarzach – dla AC oraz podmiotu, którego dane zostały zniszczone.

Art. 21 ust. 3. Rozporządzenie Rady Ministrów w sprawie określenia trybu i warunków przeprowadzania kontroli bezpieczeństwa Agencji Cyberbezpieczeństwa

Rada Ministrów określi czynności niezbędne do przeprowadzenia kontroli bezpieczeństwa. w szczególności zobowiąże Agencję Cyberbezpieczeństwa do uzgodnienia z podmiotem kontrolowanym ramowych warunki przeprowadzenia kontroli, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach kontroli bezpieczeństwa testów bezpieczeństwa. Rada Ministrów w szczególności weźmie pod uwagę minimalizację zakłócenia pracy systemu teleinformatycznego lub ograniczenia jego dostępności.

Przed przystąpieniem do czynności kontrolnych funkcjonariusz przeprowadzający kontrolę okazuje kontrolowanemu legitymację służbową oraz imienne upoważnienie do przeprowadzenia kontroli. Funkcjonariusz w porozumieniu z kontrolowanym może poinformować pracowników kontrolowanego o rozpoczęciu kontroli i temacie kontroli. W celu udokumentowania przebiegu i wyników czynności kontrolnych funkcjonariusz zakłada i prowadzi akta kontroli. Kontrola kończy się sporządzeniem protokołu kontroli w dwóch jednobrzmiących egzemplarzach oraz doręczeniem go kontrolowanemu podmiotowi celem zapoznania i podpisania.

Art. 22 ust. 9. Rozporządzenie Prezesa Rady Ministrów w sprawie określenia warunków i trybu prowadzenia, koordynacji i wdrażania systemu ostrzegania w zakresie cyberbezpieczeństwa

Prezes Rady Ministrów określi warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w szczególności określi czynności niezbędne do jego uruchomienia i utrzymania oraz wzór porozumienia między Agencją Cyberbezpieczeństwa a podmiotem objętym systemem w sprawie technicznych aspektów uczestnictwa w systemie ostrzegania oraz modelu konfiguracji systemu.

Prezes Rady Ministrów będzie kierował się potrzebą zapewnienia bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa.

Prezes Rady Ministrów będzie kierować się przepisami rozporządzenia Prezesa Rady Ministrów z dnia 2 stycznia 2020 r. w sprawie warunków i trybu prowadzenia, koordynacji i wdrażania systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet (Dz.U. poz. 54).

W ramach porozumienia uczestnik będzie zobowiązany oświadczyć, iż na dzień podpisania porozumienia spełnia wszystkie aspekty techniczne niezbędne do wdrożenia systemu ostrzegania, w szczególności jego uruchomienia. Strony rozstrzygną, czy AC dostarczy uczestnikowi platformy sprzętowej, czy też uczestnik zorganizuje ja we własnym zakresie. W porozumieniu wskazane zostaną dane kontaktowe koordynatorów wyznaczonych przez strony. Po przeprowadzeniu wdrożenia systemu ostrzegania AC poinformuje uczestnika o zakończeniu wdrożenia tego systemu oraz o jego uruchomieniu i sprawdzeniu poprawności działania systemu ostrzegania. Uczestnik będzie mieć prawo dostępu do informacji przetwarzanych w systemie ostrzegania dotyczących tego uczestnika, w tym raportów wygenerowanych przez system ostrzegania. Raporty będą informować o wykrytych nieprawidłowościach w ruchu sieciowym, agregując dostępne dane na potrzeby analizy zdarzeń.

Art. 24 ust. 14. Rozporządzenie Prezesa Rady Ministrów sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania dokumentów

Prezes Rady Ministrów określi sposób dokumentowania blokady dostępności oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków. Prezes Rady Ministrów uwzględni w szczególności potrzebę zapewnienia niejawnego charakteru podejmowanych czynności i uzyskanych materiałów, a także przejrzystość procedury dla zainteresowanych stron.

Prezes Rady Ministrów będzie kierować się obecnie obowiązującymi przepisami rozporządzenia z dnia 18 lipca 2016 r. w sprawie sposobu dokumentowania blokady

dostępności określonych danych informatycznych lub usług teleinformatycznych w systemie teleinformatycznym oraz przechowywania i przekazywania postanowień, pisemnych zgód, zarządzeń i wniosków (Dz.U. poz. 1056). Dokumentację blokady dostępności będą stanowić:

1) wniosek Szefa AC do Sądu Okręgowego w Warszawie, zwanego dalej "Sądem", o zarządzenie lub przedłużenie blokady dostępności;
2) postanowienie Prokuratora Generalnego w sprawie wystąpienia przez Szefa AC z wnioskiem o zarządzenie lub przedłużenie przez Sąd blokady dostępności;
3) postanowienie Sądu w sprawie zarządzenia lub przedłużenia blokady dostępności;
4) wniosek Szefa AC do Prokuratora Generalnego o wyrażenie zgody na zarządzenie blokady dostępności w przypadkach niecierpiących zwłoki;
5) postanowienie Prokuratora Generalnego w sprawie zarządzenia przez Szefa AC blokady dostępności w przypadkach niecierpiących zwłoki;
6) zarządzenie przez Szefa AC blokady dostępności w przypadkach niecierpiących zwłoki;
7) wniosek Szefa AC do Sądu w sprawie zatwierdzenia zarządzenia przez Szefa AC blokady dostępności w przypadkach niecierpiących zwłoki;
8) postanowienie Sądu w sprawie zatwierdzenia zarządzenia przez Szefa AC blokady dostępności w przypadkach niecierpiących zwłoki;
9) wniosek Szefa AC do Sądu o wyrażenie zgody na przedłużenie blokady dostępności zarządzonej przez Szefa AC w przypadkach niecierpiących zwłoki;
10) postanowienie Prokuratora Generalnego w sprawie wyrażenia zgody na wystąpienie przez Szefa AC z wnioskiem do Sądu o przedłużenie zarządzonej przez Szefa AC blokady dostępności w przypadkach niecierpiących zwłoki;
11) postanowienie Sądu w sprawie wyrażenia zgody na przedłużenie blokady dostępności zarządzonej przez Szefa AC w przypadkach niecierpiących zwłoki;
12) zażalenie Szefa AC lub Prokuratora Generalnego na postanowienie Sądu w sprawie blokady dostępności;

13) zawiadomienie ministra właściwego do spraw informatyzacji o zarządzeniu blokady dostępności.

W ramach dokumentacji określone zostaną m.in. przesłanki podjęcia czynności, zakres blokady, okres blokady, uzasadnienie, kryptonim sprawy, dane kontaktowe koordynatora sprawy.

Prezes Rady Ministrów określi również wzór rejestru wskazanych dokumentów, który będzie ustalony w formie tabelarycznej z wykazem danych koniecznych do właściwego zidentyfikowania sprawy."

Krzysztof Gawkowski

Poseł na Sejm RP

Warszawa, 24 stycznia 2022 r.

Szanowna Pani
Elżbieta Witek
Marszałek Sejmu RP

Szanowna Pani Marszałek,

Na podstawie art. 36 ust 1a Regulaminu Sejmu Rzeczypospolitej Polskiej, jako przedstawiciel wnioskodawców wnoszę

autopoprawkę do poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (EW-020-674/21).

Autopoprawkę przekazuję w załączeniu.

Z poważaniem

Krzysztof Gawkowski

Autopoprawka do poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (EW-020-674/21)

W art. 28:

a) ust. 1 nadać brzmienie:

„1. Pracownikiem lub funkcjonariuszem AC może być osoba o nieposzlakowanej opinii, która nie była skazana prawomocnym wyrokiem sądu za przestępstwo lub przestępstwo skarbowe, korzystająca z pełni praw publicznych, posiadająca wykształcenie wyższe oraz zdolność fizyczną i psychiczną do pracy lub służby w formacjach podległych szczególnej dyscyplinie służbowej, której gotowa jest się podporządkować, a także dająca rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych."

b) po ust. 1 dodać ust. 1a w brzmieniu:

„1a. Funkcjonariuszem AC może zostać osoba, która spełnia warunki, o których mowa w ust. 1, i posiada wyłącznie obywatelstwo polskie."

Uzasadnienie

Projektodawca zgodnie z brzmieniem autopoprawki proponuje wykreślenie z art. 28 ust. 1 warunku posiadania wyłącznie polskiego obywatelstwa. Warunek ten wprowadzany jest z przepisie szczególnym (ust. 1a), zgodnie z którym warunek posiadanie wyłącznie obywatelstwa polskiego będzie dotyczyć tylko funkcjonariuszy AC. Autopoprawka jest odpowiedzią na opinię w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa z dnia 18 października 2021 roku (BAS-WAPM-2452/21) i stanowi realizację zasady swobody przepływu pracowników w rozumieniu art. 45 TfUE oraz przepisów 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. Jednocześnie projektodawca pragnie podziękować Panu Marcinowi Fryźlewiczowi oraz Panu Dyrektorowi Przemysławowi Sobolewskiemu za pracę włożoną w stworzenie opinii.

SEJM RZECZYPOSPOLITEJ POLSKIEJ

BIURO ANALIZ SEJMOWYCH
KANCELARII SEJMU

Warszawa, 2 lutego 2022 r.

BAS-WAPEiM-166/22

DS. 1120.54.2022
3.02.2022

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie zgodności z prawem Unii Europejskiej poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa (przedstawiciel wnioskodawców: poseł Krzysztof Gawkowski) w wersji uwzględniającej autopoprawkę z dnia 25 stycznia 2022 r.

Na podstawie art. 34 ust. 9 uchwały Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 roku – Regulamin Sejmu Rzeczypospolitej Polskiej (Monitor Polski z 2021 r. poz. 483, ze zmianami) sporządza się następującą opinię:

1. Przedmiot projektu ustawy

W projekcie ustawy przewiduje się utworzenie Agencji Cyberbezpieczeństwa, zwanej dalej „Agencją" lub „AC". Proponowana ustawa określa zakres i zasady działania oraz strukturę Agencji. Zaproponowany katalog zadań AC obejmuje m.in.: koordynację krajowego systemu cyberbezpieczeństwa; podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego; reagowanie na incydenty związane z bezpieczeństwem cybernetycznym; współpracę operacyjną z innymi służbami specjalnymi w celu likwidacji zagrożeń; ocenę i zarządzanie ryzykiem cyfrowym; wymianę informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami i podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie. Działalność AC byłaby finansowana z odrębnej części budżetu państwa. Szef AC w zakresie wykonywania swoich zadań koordynowałby działania podmiotów krajowego systemu cyberbezpieczeństwa, określonych w art. 4 punkty 1–18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], a także współpracował z innymi podmiotami określonymi w art. 7 ust. 8 tej ustawy. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne byliby obowiązani, w zakresie

[1] Dz. U. z 2020 r. poz. 1369, ze zmianami.

swojego działania, do współdziałania z AC w sposób określony proponowaną regulacją. Pozostałe przepisy regulują strukturę i organizację Agencji, szczegółowe zasady działalności AC oraz zasady i tryb zatrudniania pracowników i funkcjonariuszy Agencji. Projekt zawiera przepisy karne.

Projektodawcy proponują zmianę ustaw: z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2], z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3] oraz z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projekt zawiera postanowienia przejściowe. Projektowana ustawa ma wejść w życie z dniem 1 stycznia 2022 r.

2. Stan prawa Unii Europejskiej w materii objętej projektem ustawy

Z uwagi na przedmiot projektu ustawy należy uwzględnić:

- art. 45 Traktatu o funkcjonowaniu Unii Europejskiej (dalej: TfUE), ustanawiający swobodę przepływu pracowników wewnątrz Unii;

- 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[4], dalej jako „dyrektywa (UE) 2016/1148" lub „dyrektywa".

Dyrektywa (UE) 2016/1148 ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego (art. 1 ust. 1). Jednocześnie 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 (art. 1 ust. 6).

3. Analiza przepisów projektu ustawy pod kątem ustalonego stanu prawa Unii Europejskiej

3. Opiniowany projekt ustawy wymaga oceny zgodności z prawem Unii Europejskiej w dwóch kwestiach: 1) zgodności z zasadą swobodnego przepływu pracowników wewnątrz Unii (art. 45 TfUE), oraz 2) zgodności z dyrektywą (UE) 2016/1148.

3.1. W art. 8 ust. 4 projektu ustanowiono wymóg posiadania wyłącznie obywatelstwa polskiego w odniesieniu do osoby powoływanej na stanowisko Szefa lub zastępcy Szefa AC. Wymóg obywatelstwa polskiego przewidziano także w odniesieniu do funkcjonariuszy AC (art. 28 ust. 1 projektu). Oznacza to,

---

[2] Dz. U. z 2020 r. poz. 27, ze zmianami.

[3] Dz. U. z 2020 r. poz. 1856 oraz z 2021 r. poz. 159.

[4] Dz. Urz. UE L 194 z 19.7.2016 r., str. 1.

że Szefem lub zastępcą Szefa AC oraz funkcjonariuszem AC nie będzie mogła być osoba, która nie jest obywatelem polskim. Pełnienie funkcji Szefa lub zastępcy AC, jak również posiadanie statusu funkcjonariusza AC, byłoby więc wykluczone w odniesieniu do obywateli innych niż RP państw członkowskich UE. Proponowane przepisy należy ocenić pod kątem zgodności z zasadą swobody przepływu pracowników w rozumieniu art. 45 TfUE.

Zasada swobodnego przepływu pracowników wewnątrz Unii obejmuje zniesienie wszelkiej dyskryminacji ze względu na przynależność państwową między pracownikami państw członkowskich w zakresie zatrudnienia (art. 45 ust. 1 i 2 TfUE). Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej (dalej: Trybunał) swoboda przepływu pracowników oznacza zniesienie także barier o charakterze niedyskryminującym. Za sprzeczne z art. 45 TfUE Trybunał uznaje regulacje krajowe, które uniemożliwiają lub zniechęcają pracownika – obywatela UE do skorzystania ze swobody przemieszczania się do innego państwa członkowskiego. Postanowienia art. 45 TfUE nie mają jednak zastosowania do zatrudnienia w administracji publicznej (art. 45 ust. 4 TfUE). Wyłączenie to ma charakter wyjątku, nie można więc traktować go rozszerzająco. Jego treść, wraz z pojęciem „administracja publiczna", jest przedmiotem orzecznictwa Trybunału.[5]

Trybunał stwierdził, że pojęcie administracji publicznej w rozumieniu przepisów TfUE należy interpretować i stosować jednolicie w całej Unii i w związku z tym nie może być w pełni pozostawione uznaniu państw członkowskich. Zgodnie z orzecznictwem Trybunału art. 45 ust. 4 TfUE będzie miał zastosowanie tylko do stanowisk, które są związane z bezpośrednim lub pośrednim udziałem w wykonywaniu władzy powierzonej przez prawo publiczne oraz funkcji, które mają na celu ochronę ogólnych interesów państwa lub władz publicznych i wymagają zatem od osób dysponujących tymi uprawnieniami istnienia szczególnego relacji solidarności z państwem oraz wzajemności praw i obowiązków leżących u podstaw więzów obywatelstwa. Trybunał stoi na stanowisku, że art. 45 ust. 4 TfUE może być zastosowany wówczas, gdy wykonywanie uprawnień przyznanych przez prawo publiczne odbywa się regularnie oraz nie jest bardzo niewielką częścią prowadzonej aktywności. Wyłączenia określonego w art. 45 ust. 4 TFUE nie stosuje się natomiast do stanowisk, które podlegają wprawdzie państwu lub innym podmiotom prawa

---

[5] Zob. m.in. wyrok Trybunału z 17 grudnia 1980 r. w sprawie Komisja przeciwko Belgii, 149/79, ECLI:EU:C:1980:297, punkty 10, 12, 18 i 19, wyrok Trybunału z 16 czerwca 1987 r. w sprawie Komisja przeciwko Włochom, 225/85, ECLI:EU:C:1987:284, pkt 7, wyrok Trybunału z dnia 2 lipca 1996 r. w sprawie Komisja przeciwko Grecji, C-290/94, ECLI:EU:C:1996:265, pkt 2, wyrok Trybunału z dnia 30 września 2003 r. w sprawie Colegio de Oficiales de la Marina Mercante Española, C-405/01, ECLI:EU:C:2003:515, pkt 40, wyrok Trybunału z 30 września 2003 r. w sprawie Anker i inni, C-47/02, ECLI:EU:C:2003:516, punkty 57–60, wyrok Trybunału z 10 września 2014 r. w sprawie Haralambidis, C-270/13, ECLI:EU:C:2014:2185, punkty 42–45, wyrok Trybunału z 6 października 2015 r. w sprawie Brouillard, C-298/14, ECLI:EU:C:2015:652, punkty 30–32, wyrok Trybunału z 22 czerwca 2017 r. w sprawie Bechtel, C-20/16, punkty 34 i 35.

publicznego, jednak nie wiążą się ze współdziałaniem przy wykonywaniu zadań należących do administracji publicznej we właściwym znaczeniu.

Dodatkową wskazówką interpretacyjną może być treść komunikatu Komisji z 11 grudnia 2002 r. dotyczącego swobody przepływu pracowników[6] oraz komunikatu Komisji z 13 lipca 2010 r. do Rady, Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Potwierdzenie zasady swobodnego przepływu pracowników: prawa oraz główne zmiany*[7]. Komisja Europejska uważa, że wyjątek dotyczący administracji publicznej odnosi się przede wszystkim do sił zbrojnych, policji, wymiaru sprawiedliwości, administracji skarbowej oraz dyplomacji[8]. Może odnosić się do stanowisk w administracji publicznej szczebla centralnego lub lokalnego, których sprawowanie zakłada wykonywanie władzy państwowej, w związku z procesem tworzenia lub stosowania prawa oraz nadzoru nad jednostkami podporządkowanymi. Zgodnie z orzecznictwem Trybunału Komisja podkreśla, że art. 45 ust. 4 TfUE ma charakter wyjątku, który należy interpretować w sposób zawężający, a kryteria kwalifikujące do skorzystania z wyjątku należy rozpatrywać indywidualnie.

Na gruncie przepisów projektu powstaje pytanie, czy w odniesieniu do stanowisk Szefa i zastępcy Szefa AC oraz statusu funkcjonariusza Agencji ma zastosowanie wyjątek określony w art. 45 ust. 4 TfUE, a więc czy są one wyłączone ze swobody przepływu pracowników wewnątrz Unii.

Zgodnie z projektem zarówno Szefa AC, jak i zastępcę Szefa AC (na wniosek Szefa AC) powoływałby Prezes Rady Ministrów, po zasięgnięciu opinii sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji (art. 8 ust. 2 i 3). Szefem AC lub zastępcą Szefa AC mogłaby zostać osoba, która m.in. spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności „ściśle tajne" (art. 8 ust. 4 pkt 4). Szef AC przekazywałby Prezesowi Rady Ministrów informację o bieżącym stanie cyberbezpieczeństwa (art. 15). Szef AC przedstawiałby sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji roczną informację o stanie bezpieczeństwa państwa (art. 26).

Biorąc pod uwagę przewidziane w projekcie ustawy kompetencje, zakres zadań oraz szczególną pozycję ustrojową Szefa AC i zastępcy Szefa AC należy uznać, że sprawowanie tego urzędu będzie wymagało istnienia szczególnych relacji w stosunku do państwa, wynikających z więzów obywatelstwa. Pełnienie funkcji Szefa AC (zastępcy Szefa AC) byłoby więc zatrudnieniem w administracji publicznej, spełniającym kryterium wyjątku przewidzianego w art. 45 ust. 4 TfUE. Należy uznać, że w omawianym przypadku wymóg obywatelstwa

---

[6] *Communication from the Commission "Free movement of workers – achieving the full benefits and potential"* (COM(2002) 694 final). Dokument niedostępny w języku polskim.

[7] KOM(2010) 373 wersja ostateczna.

[8] Jednocześnie Komisja Europejska wyraźnie zastrzega, że nie wszystkie stanowiska w wymienionych przez nią dziedzinach administracji publicznej wiążą się z wykonywaniem władzy publicznej i odpowiedzialnością za ochronę ogólnych interesów państwa.

polskiego jest usprawiedliwiony, zasada swobody przepływu pracowników nie ma zastosowania, a projektowany przepis nie jest sprzeczny z prawem UE.

Analizy wymaga ponadto przewidziany przez projektodawców wymóg obywatelstwa polskiego w odniesieniu do funkcjonariuszy AC (art. 28 ust. 1a projektu). Zgodnie z projektowaną regulacją w ramach AC zatrudniani byliby pracownicy i funkcjonariusze, przy czym funkcjonariusze AC pełniliby służbę w ramach CSIRT GOV (art. 27). Funkcjonariuszem AC mogłaby być osoba m.in. posiadająca zdolność fizyczną i psychiczną do pracy lub służby w formacjach podległych szczególnej dyscyplinie służbowej, której gotów jest się podporządkować, a także dająca rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych (art. 28 ust. 1). Na podstawie postępowania kwalifikacyjnego Szef AC będzie mógł podjąć decyzję o powołaniu do służby w CSIRT GOV kandydatów z najwyższymi wynikami postępowania (art. 29). W zakresie nieregulowanym proponowaną ustawą funkcjonariuszom AC przysługiwałyby uprawnienia funkcjonariuszy określone w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (art. 31).

Biorąc pod uwagę proponowane przyznanie funkcjonariuszom AC uprawnień funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu należy uznać, że pełnienie służby w charakterze funkcjonariusza AC będzie wymagało istnienia szczególnych relacji w stosunku do państwa, wynikających z więzów obywatelstwa. Pełnienie służby w charakterze funkcjonariusza AC byłoby więc zatrudnieniem w administracji publicznej, spełniającym kryterium wyjątku przewidzianego w art. 45 ust. 4 TfUE. Przewidziany w art. 28 ust. 1a projektu wymóg obywatelstwa polskiego w odniesieniu do funkcjonariuszy AC należy więc uznać za usprawiedliwiony. Projektowany przepis nie jest sprzeczny z prawem UE.

3.2. Zgodnie z proponowaną ustawą do zadań tworzonej Agencji ma należeć koordynacja krajowego systemu cyberbezpieczeństwa (art. 4 pkt 1 projektu). W zakresie wykonywania tego zadania Szef AC koordynowałby działania podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, określonych w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa[9]. Należy zauważyć, że ustawa ta w zakresie swojej regulacji wdraża dyrektywę (UE) 2016/1148. Ze względu na przedmiot projektu ustawy można w szczególności wskazać implementowane przez ustawę o krajowym systemie cyberbezpieczeństwa postanowienia dyrektywy dotyczące wyznaczenia właściwego organu krajowego ds. bezpieczeństwa sieci i systemów informatycznych lub większej ich liczby (zwanych dalej „właściwym organem"), które są obowiązane do monitorowania stosowania dyrektywy na poziomie krajowym (art. 8), jak również dotyczące współpracy między właściwym organem, pojedynczym punktem kontaktowym i CSIRT w zakresie wypełnienia obowiązków określonych w dyrektywie (art. 9). Należy uznać, że proponowana

[9] Zgodnie z art. 6 ust. 1 projektu oraz art. 37 pkt 2 (dotyczącym zmiany art. 4 ustawy o krajowym systemie cyberbezpieczeństwa).

ustawa, zakładająca powołanie Agencji koordynującej działalność podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, nie narusza postanowień dyrektywy (UE) 2016/1148.

4. Konkluzja

Projekt ustawy o Agencji Cyberbezpieczeństwa w wersji uwzględniającej autopoprawkę z dnia 25 stycznia 2022 r. nie jest sprzeczny z prawem UE.

Autor:
Marcin Fryźlewicz
ekspert ds. legislacji
w Biurze Analiz Sejmowych

Akceptował:
Dyrektor
Biura Analiz Sejmowych
Sobolewski
Przemysław Sobolewski

SEJM RZECZYPOSPOLITEJ POLSKIEJ

BIURO ANALIZ SEJMOWYCH
KANCELARII SEJMU

Warszawa, 2 lutego 2022 r.

BAS-WAPEiM-167/22

DS. 1120.54.2022 (2)
3.02.2022 r.

Pani
Elżbieta Witek
Marszałek Sejmu
Rzeczypospolitej Polskiej

Opinia w sprawie stwierdzenia – w trybie art. 95a ust. 3 regulaminu Sejmu – czy poselski projekt ustawy o Agencji Cyberbezpieczeństwa (przedstawiciel wnioskodawców: poseł Krzysztof Gawkowski) w wersji uwzględniającej autopoprawkę z dnia 25 stycznia 2022 r. jest projektem ustawy wykonującej prawo Unii Europejskiej

W projekcie ustawy przewiduje się utworzenie Agencji Cyberbezpieczeństwa, zwanej dalej „Agencją" lub „AC". Proponowana ustawa określa zakres i zasady działania oraz strukturę Agencji. Zaproponowany katalog zadań AC obejmuje m.in.: koordynację krajowego systemu cyberbezpieczeństwa; podnoszenie poziomu odporności systemów informatyczno-informacyjnych administracji publicznej i sektora prywatnego; reagowanie na incydenty związane z bezpieczeństwem cybernetycznym; współpracę operacyjną z innymi służbami specjalnymi w celu likwidacji zagrożeń; ocenę i zarządzanie ryzykiem cyfrowym; wymianę informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami i podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie. Działalność AC byłaby finansowana z odrębnej części budżetu państwa. Szef AC w zakresie wykonywania swoich zadań koordynowałby działania podmiotów krajowego systemu cyberbezpieczeństwa, określonych w art. 4 punkty 1–18 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[1], a także współpracował z innymi podmiotami określonymi w art. 7 ust. 8 tej ustawy. Organy administracji rządowej, organy samorządu terytorialnego, instytucje państwowe oraz przedsiębiorcy wykorzystujący środki publiczne byliby obowiązani, w zakresie swojego działania, do współdziałania z AC w sposób określony proponowaną regulacją. Pozostałe przepisy regulują strukturę i organizację Agencji, szczegółowe zasady działalności AC oraz zasady i tryb zatrudniania pracowników i funkcjonariuszy Agencji. Projekt zawiera przepisy karne i postanowienia

[1] Dz. U. z 2020 r. poz. 1369, ze zmianami.

przejściowe. Projektodawcy proponują zmianę ustaw: z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[2], z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3] oraz z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projekt nie zawiera przepisów mających na celu wykonanie prawa UE.

Projekt ustawy o Agencji Cyberbezpieczeństwa w wersji uwzględniającej autopoprawkę z dnia 25 stycznia 2022 r. **nie jest projektem ustawy wykonującej** prawo Unii Europejskiej.

Autor:
Marcin Fryźlewicz
ekspert ds. legislacji
w Biurze Analiz Sejmowych

Akceptował:
Dyrektor
Biura Analiz Sejmowych
Sobolewski
Przemysław Sobolewski

[2] Dz. U. z 2020 r. poz. 27, ze zmianami.
[3] Dz. U. z 2020 r. poz. 1856 oraz z 2021 r. poz. 159.

Warszawa, 15 lutego 2022 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
Komisja Ustawodawcza
UST.00. 34 .2022

SEKRETARIAT MARSZAŁKA SEJMU RP
WPŁYNĘŁO
16. 02. 2022
EW.020.64.21(4)

Pani
Elżbieta WITEK
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowna Pani Marszałek

Przekazuję – przyjęte na posiedzeniu w dniu 15 lutego 2022 r. – opinie Komisji Ustawodawczej:

– o poselskim projekcie ustawy o Agencji Cyberbezpieczeństwa wraz z autopoprawką (przedstawiciel wnioskodawców poseł Krzysztof Gawkowski);

– o poselskim projekcie ustawy – Tanie paliwo (przedstawiciel wnioskodawców poseł Artur Dziambor).

Z poważaniem

Przewodniczący Komisji

Arkadiusz Myrcha

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L.dz. SPS-WP.020.313.26.2021
Data wpływu 16.02.2022r.

OPINIA nr 189

Komisji Ustawodawczej

w sprawie poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa wraz z autopoprawką

przyjęta na posiedzeniu
w dniu 15 lutego 2022 r.

dla Marszałka Sejmu

Komisja Ustawodawcza, na posiedzeniu w dniu 15 lutego 2022 r., rozpatrzyła skierowany przez Marszałka Sejmu – w trybie art. 34 ust. 8 regulaminu Sejmu, celem wyrażenia opinii w świetle zgłoszonych wątpliwości w sprawie zgodności projektu z prawem Unii Europejskiej – poselski projekt ustawy o Agencji Cyberbezpieczeństwa wraz z autopoprawką.

Komisja, po przedstawieniu projektu i wysłuchaniu ekspertów, przeprowadziła dyskusję. W wyniku głosowania Komisja

- **uznała ten projekt za dopuszczalny.**

Przewodniczący Komisji

Arkadiusz Myrcha

Pan
Dariusz Salomończyk
Zastępca Szefa Kancelarii Sejmu

SEKRETARIAT Z-CY SZEFA KS
Ldz. DS. 175. 727.21
Data wpływu 22. 10. 2021 r.
WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-WP. 020.313.8.2021
Data wpływu 25. 10. 2021

Szanowny Panie Ministrze,

w odpowiedzi na pismo z dnia 14 października br. o nr EW-020-674/21, w sprawie przedłożenia opinii do **poselskiego projektu ustawy – o Agencji Cyberbezpieczeństwa,** Związek Województw RP przekazuje uwagi otrzymane z województw: lubelskiego, mazowieckiego i zachodniopomorskiego.

Z wyrazami szacunku,
Lidia Sztramska
Koordynator Komisji i
Organów Opiniodawczo-Doradczych

Związek Województw RP
ul. Świętojerska 5/7, 00-236 Warszawa
Phone +48 (22) 831 14 41
Mobile +48 511 271 869
www.polskieregiony.pl

POLSKIE REGIONY

URZĄD MARSZAŁKOWSKI
WOJEWÓDZTWA LUBELSKIEGO
w Lublinie
Biuro Bezpieczeństwa
20-029 Lublin, ul. Artura Grottgera 4
BB.0221.32.2021.PBŁ

Lublin, 21 października 2021 r.

MARSZAŁEK WOJEWÓDZTWA
Jarosław Stawiarski

Pani
Katarzyna Janiszewska
Dyrektor
Kancelarii Marszałka
w miejscu

Szanowna Pani Dyrektor

W odpowiedzi na korespondencję mailową z dnia 15.10.2021 r. dotyczącej poselskiego projektu (KP Lewica) ustawy o Agencji Cyberbezpieczeństwa informuje, że Biuro Bezpieczeństwa tut. Urzędu proponuje rozważanie możliwości nietworzenia nowej odrębnej agencji jako niezależnej formacji, natomiast zadania oraz prawa i obowiązki nowej spec jednostki, zawarte w załączonym projekcie włączyć do istniejących służb mundurowych tj. ABW i Policji. Tworzenie nowej Agencji spowoduje powielenie struktur zajmujących się cyberbezpieczeństwiem w już istniejących służbach.

Proponowany projekt ustawy w obecnym stadium wymagałby dopracowania pod względem prawno-merytorycznym.

Z poważaniem

DYREKTOR
Biura Bezpieczeństwa
Szymanek

Informacja o projekcie:

Tytuł	Ustawa o Agencji Cyberbezpieczeństwa
Projekt z dnia	8 października 2021 r.

Informacje o zgłaszającym uwagi:

Urząd	Urząd Marszałkowski Województwa Mazowieckiego za pośrednictwem Biura Związku Województw RP
Organizacja samorządowa	Związek Województw RP

Uwagi:

Lp.	Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)	Treść uwagi (propozycja zmian)	Uzasadnienie uwagi
1.	art. 4 pkt 10	Proponuje się doprecyzować art. 4 pkt 10 projektu poprzez wskazanie jakie konkretnie technologie mają wpływ na życie człowieka.	Art. 4 punkt 10 projektu jest zbyt ogólny. Nie wszystkie nowoczesne technologie opierają się na danych lub sprzęcie elektronicznym, o których mowa w projekcie ustawy. Niezrozumiałe jest w jaki sposób wpływ rozwoju nowoczesnej technologii na życie człowieka odnosi się do cyberbezpieczeństwa.
2.	art. 7 ust. 2 pkt 2	Brak wskazania w tym przepisie o jakim dokładnie oprogramowaniu mowa. Proponuje się doprecyzować jakiego rodzaju oprogramowanie spełnia standardy AC.	Obecne brzmienie art. 7 ust. 2 projektu powoduje uznaniowość przy decydowaniu czy dane oprogramowanie spełnia standardy AC. Prywatny przedsiębiorca, który korzysta z licencji na oprogramowanie, które pozwala mu uzyskiwać dochód, a które nie spełni uznaniowych standardów AC, traci możliwość uzyskiwania tegoż dochodu. Jest to zjawisko potencjalnie umożliwiające wykluczenie pewnych podmiotów z korzystania ze środków publicznych, poprzez wyznaczenie niemożliwych do osiągnięcia standardów.
3.	art. 28 ust. 3 pkt 2	Proponuje się zmienić brzmienie pkt 2 na następujące: „2) test wiedzy, umiejętności oraz znajomości języka obcego z zakresu informatyki i nowoczesnych technologii teleinformatycznych".	Z obecnego brzmienia przepisu nie wynika o jaki język obcy w tym kontekście chodzi.

4.	Art. 4 pkt 5	Proponuje się doprecyzować przepis poprzez wskazanie jaki sposób AC może mieć fizyczny wpływ na podniesienie poziomu odporności systemów informatyczno – informacyjny administracji publicznej i sektora prywatnego.	Obecne brzmienie przepisu projektu ustawy może zostać zinterpretowane tak, że AC będzie wprowadzać gruntowne zmiany w kodzie oprogramowania w celu podniesienia jego bezpieczeństwa.
5.	Art. 8 ust. 4	Proponuje się zmianę brzmienia art. 8 ust. 4 projektu ustawy poprzez dodanie po punkcie 5 punktów 6, 7, 8 i 9 o następującej treści: „6) posiada wyższe wykształcenie kierunkowe; 7) posiada co najmniej 5 letni staż pracy ogółem; 8) posiada doświadczenie w realizacji zadań z zakresu przepisów ustawy o krajowym systemie cyberbezpieczeństwa; 9) posiada doświadczenie w nadzorowaniu i koordynowaniu pracy Pracowników".	Kompetencje do powołania szefa AC może mieć osoba bezpośrednio po studiach zarządzanie cyberbezpieczeństwem. W projekcie nie wskazano wymagań co do doświadczenia zawodowego ogółem oraz co do doświadczenia w zarządzaniu. Z uwagi na doniosłość stanowiska, w projekcie należy uwzględnić powyższe kryteria dotyczące wyboru kandydata na Szefa AC lub zastępcy Szefa AC.
6.	Art. 9	Brak kadencyjności Szefa AC i zastępcy Szefa AC oraz zbyt ogólna treść art. 9 pkt 4 projektu ustawy. Proponuje się wprowadzić kadencyjność Szefa AC i zastępcy Szefa AC oraz doprecyzować art. 9 pkt 4 projektu poprzez zdefiniowanie „predyspozycji niezbędnych do zajmowania stanowiska".	Z uwagi na to, że treść pkt 4 jest ogólna, utrata rzeczywistej „predyspozycji" w praktyce będzie trudna do udowodnienia. Wprowadzenie kadencyjności stanowiska Szefa AC zapobiegnie nieprawidłowościom w sprawowaniu funkcji.

Grzegorz Jaworski

Kierownik Wydziału ds. Legislacji i Koordynacji Pomocy Prawnej

/- podpisano elektronicznie/

Informacja o projekcie:

Tytuł	Poselski projekt ustawy o Agencji Cyberbezpieczeństwa.
Projekt z dnia	8 października 2021r.

Informacje o zgłaszającym uwagi:

Urząd	Urząd Marszałkowski Województwa Zachodniopomorskiego za pośrednictwem Biura Związku Województw RP
Organizacja samorządowa	Związek Województw RP

Uwagi:

Lp.	Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)	Treść uwagi (propozycja zmian)	Uzasadnienie uwagi
1.	Art.1. Pkt 2)	Usunąć wyrazy „przechowywanie lub".	Przetwarzanie danych zawiera w swoim zakresie przechowywanie danych. Tak jest to zdefiniowane w literaturze specjalistycznej i definiowane w aktach prawnych.
2.	Art. 18. Ust 2.	Proponuje się wydłużyć czas wniesienia zastrzeżeń podmiotu do zaleceń Szefa AC do 30 dni.	Tego typu analizy bywają pracochłonne i kosztowne. Waga zaś problemu jest znaczna. W przypadkach nieoczywistych trudno będzie zgłosić zastrzeżenia w ciągu 7 dni od dnia otrzymania zaleceń. Jednocześnie warto utrzymać równowagę między terminami przypisanymi obu stronom; Szef AC – podmiot publiczny i wyrównać czas reakcji obu podmiotom.
3.	Art. 19 Ust 4.	W zakończeniu zdania zamienić „... wpływających na integralność, poufność, rozliczalność i dostępność tego systemu." na „...wpływających na integralność, poufność, rozliczalność i dostępność informacji."	W zakresie wpływania na integralność, poufność, rozliczalność i dostępność ustawodawcy zapewne chodzi o informacje.
4.	Uwaga ogólna	Zachodzi ryzyko konfliktu zakresu działania Pełnomocnika Rządu ds. Cyberbezpieczeństwa (o którym mowa w art. 60 ustawy o KSC) z zakresem działania Agencji Cyberbezpieczeństwa	Ustawa o KSC powierza Pełnomocnikowi koordynowanie i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP. Wg projektu ustawy o AC – postulowany zakres działania AC pokrywa się z zakresem Pełnomocnika.
5.	Uwaga ogólna	Uzasadnienie do projektu ustawy o AC zawiera Rozdział 2. Różnice między dotychczasowym a projektowanym stanem prawnym. Niestety nie wskazano tych różnic, opisując tylko językiem niespecjalistycznym zawartość projektu ustawy. Należy wyraźnie wskazać na czym polega zmiana i jaki przyniesie efekt w zakresie poprawy cyberbezpieczeństwa RP.	Opiniujący powinni mieć realną wiedzę co się zmienia w systemie cyberbezpieczeństwa państwa i dlaczego. Tym bardziej, że koszt tej zmiany konsumuje około pół miliarda złotych środków publicznych rocznie.

SEKRETARIAT Z-CY SZEFA KS
L.dz. DS. 175.89.2021
Data wpływu 11.02.2022

Pan
Dariusz Salomończyk
Zastępca Szefa w Kancelarii Sejmu

Szanowny Panie Ministrze,
w odpowiedzi na pismo z dnia 01 lutego br. nr EW.020.673/22, w sprawie przedłożenia opinii do autopoprawki do poselskiego projektu ustawy – **O Agencji Cyberbepieczeństwa (KP Lewica),** Związek Województw, w załączeniu przesyła opinię otrzymaną z województw: mazowieckiego i zachodniopomorskiego .

Jednocześnie informujemy, że województwo lubelskie pozytywnie zaopiniowało przedmiotowy projekt.

Z wyrazami szacunku,

Lidia Sztramska
Koordynator Komisji i
Organów Opiniodawczo-Doradczych
.....
Związek Województw RP
ul. Świętojerska 5/7, 00-236 Warszawa
Phone +48 (22) 831 14 41
Mobile +48 511 271 869
www.polskieregiony.pl

POLSKIE REGIONY

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L.dz. BKS-WP.020.313.2.2021
Data wpływu 11.02.2022

Informacja o projekcie:

Tytuł	Ustawa o Agencji Cyberbezpieczeństwa
Projekt z dnia	luty 2022 r.

Informacje o zgłaszającym uwagi:

Urząd	Urząd Marszałkowski Województwa Mazowieckiego w Warszawie za pośrednictwem Biura Związku Województw RP
Organizacja samorządowa	Związek Województw RP

Uwagi:

Lp.	Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)	Treść uwagi (propozycja zmian)	Uzasadnienie uwagi
1.	art. 9 pkt. 4	Wątpliwości budzi fakt, jakie cechy czy umiejętności oznaczają predyspozycje, o których mowa w art. 9 pkt. 4, których utrata staje się przesłanką do odwołania szefa AC. Proponuje się uszczegółowić o te wytyczne lub ich określenie w drodze aktu wykonawczego do ustawy (porównaj: § 30 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 12 stycznia 2022 r. w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji lub § 8 ust. 4 rozporządzenia Ministra Sprawiedliwości z dnia 29 lipca 2010 r. w sprawie określenia trybu przeprowadzania procedury określającej predyspozycje funkcjonariuszy do służby na określonych stanowiskach lub w określonych komórkach organizacyjnych w Służbie Więziennej).	Brak wskazania nawet orientacyjnego katalogu cech i umiejętności określanych jako „predyspozycje niezbędne do zajmowania stanowiska" stwarza wysokie ryzyko nadużyć w obszarze odwołania Szefa AC na podstawie art. 9 pkt. 4 ustawy. Ryzyko to wpływa na stabilność kadrową i organizacyjną, co zagraża właściwemu funkcjonowaniu AC jako kluczowej jednostki koordynującej krajowy system cyberbezpieczeństwa.
2.	art. 18 ust. 2	Art. 18 ust. 2 ustawy nie przewiduje innych okoliczności uniemożliwiających realizację zaleceń szefa AC niż „negatywny wpływ rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności", podczas gdy w danej sytuacji wykonanie zaleceń może okazać się niemożliwe na przykład technicznie, organizacyjnie lub wykraczać poza posiadany budżet danej jednostki, co uniemożliwia realizację zaleceń we wskazanym terminie. Brak uwzględnienia takich okoliczności w treści przepisu art. 18 ust. 2 wiązać się będzie z objęciem podmiotu karą grzywny mimo faktycznego braku możliwości wykonania zaleceń nie wynikających ze złej woli i nie objętych przesłankami art. 18 ust. 2. Proponuje się uzupełnienie przesłanek art. 18 ust. 2 dotyczących możliwości wniesienia zastrzeżeń do zaleceń Szefa AC o okoliczności inne niż wyłącznie „negatywny wpływ rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności", jeżeli okoliczności te są uzasadnione, niezależne od podmiotów, o których mowa w art. 7 ust. 1 i niemożliwe do zapobieżenia przez te podmioty, a jednocześnie wykluczają realizację zaleceń szefa AC w zakresie i terminie w nich określonych.	Zawężenie katalogu przypadków, w których podmiot może wnieść zastrzeżenia do zaleceń szefa AC wyłączenie do „negatywnego wpływu rekomendowanych działań na funkcjonalność systemu lub powstanie nowych podatności" uniemożliwia zastosowanie trybu odwoławczego, a w konsekwencji nakłada na podmiot kontrolowany karę grzywny na podstawie art. 32, nawet w przypadkach, w których ograniczenia techniczne, organizacyjne czy finansowe albo zdarzenia losowe wykluczają możliwość wykonania zaleceń w zakresie i terminie wskazanych przez szefa AC. Rozwiązanie takie w sposób niesprawiedliwy ogranicza możliwości składania wyjaśnień i przedstawiania okoliczności, które mają wpływ na rozstrzygnięcie, a mogły nie być znane szefowi AC w dacie wydania zaleceń.

3.	art. 27 ust. 2	Proponuje się w ust. 2 wyraz „pełną" zastąpić wyrazem „pełnią".	korekta redakcyjna
4.	art. 32	Przepis art. 32. „Kto nie wykonuje zaleceń, o których mowa w art. 18, podlega karze grzywny", wymaga szczegółowego wyjaśnienia, jakiej grzywnie podlegać będą organy samorządu terytorialnego.	Szczegółowe wyjaśnienia oraz przepisy regulujące wysokość kary grzywny, o której mowa w art. 32.
5.	art. 33	Pojawia się wątpliwość jakiej grzywnie podlegać będą organy samorządu terytorialnego, o którym mowa w art. 33 „Kto nie wykonuje obowiązku, o którym mowa w art. 7 ust. 1, podlega karze grzywny".	W związku z tym, że przepis budzi duże wątpliwości należałoby szczegółowo wyjaśnić oraz wskazać przepisy regulujące wysokość kary grzywny, o której mowa w art. 33.

Grzegorz Jaworski

Kierownik Wydziału ds. Legislacji i Koordynacji Pomocy Prawnej

/- podpisano elektronicznie/

Informacja o projekcie:

Tytuł	Poselski projekt ustawy o Agencji Cyberbezpieczeństwa.
Projekt z dnia	1 lutego 2022r. po autopoprawce

Informacje o zgłaszającym uwagi:

Urząd	Urząd Marszałkowski Województwa Zachodniopomorskiego za pośrednictwem Biura Związku Województw RP
Organizacja samorządowa	Związek Województw RP

Uwagi:

Lp.	Część dokumentu, do którego odnosi się uwaga (np. art., nr str., rozdział)	Treść uwagi (propozycja zmian)	Uzasadnienie uwagi
1.	Art.2. Pkt 2)	Usunąć wyrazy „przechowywanie lub".	Przetwarzanie danych zawiera w swoim zakresie przechowywanie danych. Tak jest to zdefiniowane w literaturze specjalistycznej i definiowane w aktach prawnych.
2.	Art. 18. Ust 2.	Proponuje się wydłużyć czas wniesienia zastrzeżeń podmiotu do zaleceń Szefa AC do 30 dni.	Tego typu analizy bywają pracochłonne i kosztowne, a waga problemu znaczna. W przypadkach nieoczywistych trudno będzie zgłosić zastrzeżenia w ciągu 7 dni od dnia otrzymania zaleceń. Jednocześnie warto zachować równowagę pomiędzy terminami przypisanymi obu stronom: Szefowi AC i podmiotom publicznym i wyrównać czas reakcji obu stron.
3.	Art. 19 Ust 4.	W zakończeniu zdania zamienić „... wpływających na integralność, poufność, rozliczalność i dostępność tego systemu." na „...wpływających na integralność, poufność, rozliczalność i dostępność informacji."	W zakresie wpływania na integralność, poufność, rozliczalność i dostępność głównie chodzi o informacje.
4.	Uwaga ogólna	Zachodzi ryzyko konfliktu zakresu działania Pełnomocnika Rządu ds. Cyberbezpieczeństwa (o którym mowa w art. 60 ustawy o KSC) z zakresem działania Agencji Cyberbezpieczeństwa	Ustawa o KSC powierza Pełnomocnikowi koordynowanie i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP. Wg projektu ustawy o AC – postulowany zakres działania AC pokrywa się z zakresem Pełnomocnika.
5.	Uwaga ogólna	Uzasadnienie do projektu ustawy o AC zawiera Rozdział 2 pt. *Różnice między dotychczasowym a projektowanym stanem prawnym*. Niestety nie wskazano tych różnic, opisując tylko językiem niespecjalistycznym zawartość projektu ustawy. Należy wyraźnie wskazać na czym polega zmiana i jaki przyniesie efekt w zakresie poprawy cyberbezpieczeństwa RP.	Opiniujący powinni mieć realną wiedzę co się zmienia w systemie cyberbezpieczeństwa państwa i dlaczego. Tym bardziej, że koszt tej zmiany konsumuje około pół miliarda złotych środków publicznych rocznie.

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

Warszawa, *03-11-2021*

DOL.401.514.2021.WL.PM

DS. 175.747.21
8.11.2021 r.

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu RP
ul. Wiejska 4/6/8
00-902 Warszawa
elektroniczna skrzynka podawcza ePUAP
/KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w związku z korespondencją z dnia 14 października 2021 r. (znak: SPS-WP.020.313.5.2021) i przedłożeniem do zaopiniowania poselskiego projektu **ustawy o Agencji Cyberbezpieczeństwa** organ nadzorczy, z punktu widzenia przepisów *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 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.), dalej: rozporządzenie 2016/679, zgłasza następujące kwestie.

Projektowana ustawa w znacznej mierze powiela rozwiązania zawarte w art. 32a-32e *ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. z 2020 r. poz. 27, z późn. zm.) wprowadzone do niej *ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych* (Dz. U. z 2019 r. poz. 796, z późn. zm.). Tym niemniej, jako że projekt przewiduje, iż Agencja Cyberbezpieczeństwa miałaby przejąć uprawnienia ABW określone w art. 32a-32e *ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* zasadnym jest przeprowadzenie oceny tych przepisów z punktu widzenia zapewnienia stosowania przepisów rozporządzenia 2016/679 oraz *dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych*

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-07-20
www.uodo.gov.pl

przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz. U. UE. L. z 2016 r. Nr 119, str. 89 z późn. zm.) dalej dyrektywa: 2016/680. Ocenie pod kątem zgodności z dyrektywą 2016/680 powinny podlegać uprawnienia Agencji Cyberbezieczeństwa związane z dostępem do danych osobowych w ramach postepowań związanych z wykrywaniem zdarzeń o charakterze terrorystycznym jak również dotyczących innych czynów zabronionych.

Aspekty projektowanej regulacji takie jak powołanie nowej służby specjalnej – Agencji Cyberbezpieczeństwa i przyznanie jej szeregu uprawnień w obszarze bezpieczeństwa teleinformatycznego, w tym m.in. uprawnienia do ustalania standardów w tym obszarze jak również prowadzenia kontroli związanych z cyberbezpieczeństwem determinuje zasadność projektowania ochrony danych osobowych w procesie tworzenia prawa (art. 25 ust.1 rozporządzenia[1]), w tym przeprowadzenia oceny skutków dla ochrony danych, o której mowa w art. 35 ust. 1[2] rozporządzenia 2016/679 na etapie tworzenia projektowanego aktu prawnego, zgodnie z art. 35 ust. 10[3] rozporządzenia 2016/679. Wymaga tego wzgląd na to, że projektowane jest przyjęcie rozwiązań i rodzajów przetwarzania – w szczególności z użyciem nowych technologii – które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Przeprowadzenie takiej oceny, uwzględnienie jej wyników w treści projektowanych przepisów prawa oraz zawarcie informacji o jej wynikach w ocenie skutków projektowanej regulacji lub w uzasadnieniu do projektowanej ustawy jest niezwykle

---

[1] Zgodnie z w art. 25 ust. 1 rozporządzenia 2016/ Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania –wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

[2] Zgodnie z w art. 35 ust. 1 rozporządzenia 2016/679 jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

[3] Zgodnie z art. 35 ust. 10 rozporządzenia 2016/679 ust. 1–7 nie mają zastosowania, jeżeli przetwarzanie na mocy art. 6 ust. 1 lit. c) lub e) ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej – chyba że państwa członkowskie uznają za niezbędne, by przed podjęciem czynności przetwarzania dokonać oceny skutków dla ochrony danych.

pomocne, zarówno dla Projektodawcy, celem stworzenia przepisów zapewniających stosowanie przepisów projektowanej ustawy i dających odpowiednie gwarancje zgodności z rozporządzeniem 2016/679 wykonawcom norm, jak i dla organu nadzorczego, celem oceny zaproponowanych uregulowań. Właściwe wywarzenie aspektów przetwarzania danych osobowych, w tym zapewnienie poszanowania zasad dotyczących przetwarzania danych osobowych (art. 5 rozporządzenia 2016/679) jest istotne zarówno dla przyszłych wykonawców tych norm, jak i dla osób, których dane osobowe będą przetwarzane.

Poniżej uwagi szczegółowe do projektu ustawy.

1. W **art. 2 pkt 2** projektu ustawy proponuje się przyjęcie regulacji w brzmieniu: *Ilekroć w ustawie mowa o: (...) sprzęcie elektronicznym – rozumie się przez to urządzenie umożliwiające przechowywanie lub przetwarzanie danych, którego prawidłowe działanie uzależnione jest od dopływu prądu elektrycznego, obecności pól elektromagnetycznych lub połączenia z innym urządzeniem.* Zgodnie z art. 4 pkt 2[4] rozporządzenia 2016/679 przechowywanie danych osobowych jest również przetwarzaniem. Z dalszych przepisów projektowanej ustawy wynika, że projektodawca poprzez „dane" rozumie również dane osobowe, dlatego też art. 2 pkt 2 projektu ustawy nie odpowiada definicji danych osobowych. Tym samym projektowany przepis generuje ryzyko przyjęcia rozwiązań godzących w zasadę zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679[5]).
2. W **art. 7 ust. 2 pkt 2** projektu ustawy proponuje się aby: *Podmioty, o których mowa w ust. 1, w ramach współdziałania są zobowiązane do: (...) stosowania oprogramowania spełniającego standardy AC.* Przepisy rozporządzenia 2016/679 statuują m.in. zasadę neutralności technologicznej w odniesieniu do bezpieczeństwa przetwarzania danych osobowych. Kształtując tego rodzaju przepisy należałoby zatem wziąć pod uwagę treść motywu 15[6] rozporządzenia 2016/679 zawierającego postulat

[4]Zgodnie z art. 4 pkt 2 rozporządzenia 2016/679 „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

[5] Zgodnie z zasadą zgodności z prawem, rzetelności i przejrzystości dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą.

[6] Zgodnie z motywem 15 rozporządzenia 2016/679 Aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego

neutralności ochrony osób fizycznych pod względem technicznym i nieuzależniania jej od stosowanych technik oraz wynikający z art. 32 ust. 1[7] rozporządzenia 2016/679 obowiązek wdrażania i stosowania środków technicznych odpowiednich dla zapewnienia stopnia bezpieczeństwa przetwarzania danych odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia. Dlatego projektodawca powinien przeanalizować potencjalny wpływ wprowadzenia rozwiązania przewidywanego w art. 7 ust. 2 pkt 2 projektu ustawy, w szczególności w aspekcie ryzyka wprowadzenia nieadekwatnych standardów, które mogłyby obniżyć poziom bezpieczeństwa przetwarzania danych osobowych. Jest to istotne również o tyle, że standard ten ustalany byłby poleceniem szefa służby specjalnej – Szefa AC – nie zaś przepisem powszechnie obowiązującego prawa. Odpowiednimi miejscem dla takiej analizy jest jak już wyżej wskazano ocena skutków dla ochrony danych, o której mowa w art. 35 ust 1 rozporządzenia 2016/679, dokonana w trakcie projektowania ochrony danych w procesie tworzenia prawa.

3. W **art. 8 ust. 4 pkt 3** projektu ustawy zakłada się, że *Szefem AC lub zastępcą Szefa AC może zostać osoba, która: (...) daje rękojmię należytego wykonywania zadań.* Z projektowanych przepisów nie wynika jednak na podstawie jakich kryteriów ustalane będzie czy osoba kandydata na to stanowisko daje rękojmię należytego wykonywania zadań, w szczególności jakie informacje i z jakich źródeł będą pozyskiwane, jakie osoby/podmioty i z jakich zasobów mają obowiązek takich informacji udzielić, jak długo przetwarzane będą informacje związane z weryfikacją ww. przesłanki, w szczególności potwierdzające brak rękojmi należytego wykonywania zadań. Powyższe kwestie wymagają wyjaśnienia i doprecyzowania dla zachowania zgodności projektowanego przepisu z zasadami dotyczącymi przetwarzania danych osobowych: zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a rozporządzenia 2016/679), ograniczenia celu (art. 5 ust. 1 lit. b rozporządzenia 2016/679[8]), minimalizacji danych (art. 5 ust. 1 lit. c rozporządzenia

---

przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia.

[7] „Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: (...).

[8] Zgodnie z zasadą ograniczenia celu dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów

2016/679[9]), ograniczenia przechowywania (art. 5 ust. 1 lit e rozporządzenia 2016/679 [10]) i rozliczalności (art. 5 ust. 2 rozporządzenia 2016/679[11]).

4. W art. **18 ust. 1** projektu ustawy proponuje się aby: *Szef AC na podstawie analizy zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych wydaje podmiotom, o których mowa w art. 7 ust. 1 zalecenia dotyczące podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności, zwane dalej „zaleceniami"*. Należy zwrócić uwagę na konieczność uwzględnienia w treści tego przepisu rozbieżności pojęciowej pomiędzy projektowanym przepisem a art. 32 ust. 1 lit b[12] rozporządzenia 2016/679, który w odniesieniu do usług przetwarzania wskazuje na *zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania.*

   Uwaga odnosi się analogicznie do art. 19 ust. 4 projektu ustawy.

   Dodatkowo należy wskazać, że zgodnie z art. 58 ust. 2 lit. e rozporządzenia 2016/679 Prezesowi Urzędu Ochrony Danych Osobowych jako organowi nadzorczemu w rozumieniu rozporządzenia 2016/679 przysługuje uprawnienie naprawcze – nakazanie administratorowi lub podmiotowi przetwarzającemu dostosowania operacji przetwarzania do przepisów niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu. Uzasadnionym jest by wyeliminowany został w odpowiedniej regulacji przyjmowanego projektu potencjalny konflikt pomiędzy zaleceniami Szefa AC a zaleceniami Prezesa UODO (organu nadzorczego), o ile byłyby wydawane w tym samym stanie faktycznym, w związku naruszeniem

---

archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami.

[9] Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

[10] Zgodnie z zasadą ograniczenia przechowywania dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

[11] Zgodnie z art. 5 ust. 2 rozporządzenia 2016/679Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie

[12] Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku: (...) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

bezpieczeństwa przetwarzania danych osobowych. Odpowiednim miejscem dla takiej analizy jest również ocena skutków dla ochrony danych, o której mowa w art. 35 ust 1 rozporządzenia 2016/679, dokonana w trakcie projektowania ochrony danych w procesie tworzenia prawa.

5. **Art. 19 ust. 5** projektu ustawy – dotyczący warunków przeprowadzenia kontroli bezpieczeństwa - powinien wskazywać, że kontrola taka nie może prowadzić do naruszenia zasad wyrażonych w rozporządzeniu 2016/679 dla zachowania zgodności z zasadą zgodności z prawem, rzetelności i przejrzystości.
6. **Art. 21 ust. 2** projektu ustawy przewiduje, że *Prezes Rady Ministrów określi, w drodze rozporządzenia, sposób niszczenia przez Szefa AC materiałów zawierających informacje, o których mowa w art. 19 ust. 9, a także wzory niezbędnych dokumentów, mając na uwadze rodzaj materiałów podlegających zniszczeniu.* Z projektowanego przepisu nie wynika, jakie dokumenty projektodawca uznaje za „niezbędne", tym samym projektowany przepis ma charakter blankietowy. Dodatkowo, zważywszy na fakt, że procedurze niszczenia będą podlegały również dane osobowe to zakres danych zawartych w dokumentach, o których mowa w art. 21 ust. 2 projektu ustawy powinien przynajmniej na poziomie ogólnym wynikać z przepisów projektowanej ustawy. Odpowiadałoby to w sposób pełniejszy zasadzie zgodności z prawem, rzetelności i przejrzystości.
7. **Art. 21 ust. 3** projektu ustawy przewiduje, że *Rada Ministrów określi, w drodze rozporządzenia, tryb i warunki przeprowadzania kontroli bezpieczeństwa, mając na uwadze określenie czynności niezbędnych do jej przeprowadzenia, w tym dokonywanie uzgodnień, o których mowa w ust. 6.* Z uwagi na fakt, że kontrola ta będzie dotyczyć warunków przetwarzania danych osobowych przez danego administratora, zarówno tryb jak i warunki przeprowadzania tej kontroli powinny – jako stanowiące prawa i obowiązki - uregulowane powinny zostać w przepisach rangi ustawy, zaś akt wykonawczy może je jedynie uszczegóławiać. Odpowiadałoby to w sposób pełniejszy zasadzie zgodności z prawem, rzetelności i przejrzystości.
8. **Art. 22 ust. 4** projektu ustawy przewiduje, że *Podmiot, o którym mowa w ust. 1, ma obowiązek przystąpić do systemu ostrzegania oraz przekazać AC niezbędne informacje umożliwiające wdrożenie systemu ostrzegania w tym podmiocie.* Pojęcie „niezbędne informacje" ma charakter nieostry - z projektowanego przepisu powinno jasno wynikać jakie informacje o charakterze danych osobowych mają być

przekazywane do Agencji Cyberbezpieczeństwa dla zapewnienia zgodności z zasadą zgodności z prawem, rzetelności i przejrzystości oraz zasadą minimalizacji danych.

9. W **art. 23 ust. 1** projektu ustawy przewiduje się, że *w przypadku powzięcia informacji o wystąpieniu zdarzenia o charakterze terrorystycznym dotyczącego systemów lub danych, szef AC może żądać m.in. „innych danych" umożliwiających dostęp do systemu.* Zasada legalizmu – wskazująca konieczność działania na podstawie i w granicach oraz mająca znaczenie dla wyznaczenia kompetencji organów - wymaga wyznaczenia jakie inne dane umożliwiające dostęp do systemów będzie mógł przetwarzać szef AC. Dodatkowo, jeśli będą to również dane biometryczne[13] używane do logowań do systemów teleinformatycznych, to z projektowanego przepisu powinno wprost wynikać, że chodzi o te dane. Przyjęcie komentowanego rozwiązania oznacza, iż dotyczy ono również przetwarzania innych danych sensytywnych - z art. 9 ust. 1[14] regulującego przetwarzanie szczególnych kategorii danych oraz art. 10 rozporządzenia 2016/679 regulującego przetwarzanie przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa. Taka redakcja przepisu powinna być zgodna z zasadami zgodności z prawem, rzetelności i przejrzystości oraz minimalizacji danych.
10. **Art. 24 ust. 6 pkt 5** projektu ustawy przewiduje, że *Wniosek Szefa AC, o którym mowa w ust. 1, powinien zawierać w szczególności: (...) dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie blokada dostępności, ze wskazaniem sposobu jej stosowania.* Określenie „dane pozwalające na jednoznaczne określenie podmiotu", jest pojęciem nieostrym, celem wypełniania zasady legalizmu przepis powinien wprost wymieniać dane osobowe jakie będzie zawierał wniosek Szefa AC. Użyte w ust. 6 sformułowanie „w szczególności" również jest nieprecyzyjne i tworzy otwarty katalog danych osobowych. Tym samym projektowany przepis nie odpowiada zasadom zgodności z prawem, rzetelności i przejrzystości oraz minimalizacji danych.

---

[13] Zgodnie z art. 4 pkt 14 rozporządzenia 2016/679 dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

[14] Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

11. Projektowany **art. 25 ust. 3** ustawy zakłada, że *Dane, o których mowa w ust. 2, przekazuje Szefowi AC administrator systemu teleinformatycznego, o którym mowa w art. 4 pkt 2, niezwłocznie po wykryciu zdarzenia naruszającego bezpieczeństwo tego systemu.* Projektowane przepisy nie definiują pojęcia „administrator systemu", a rozporządzenie 2016/679 nie posługuje się takim terminem, pod pojęciem administratora rozumie zaś *osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (...)* (art. 4 pkt 7 rozporządzenia 2016/679). Projektowany przepis powinien zostać więc przeredagowany tak, aby nie budził wątpliwości interpretacyjnych i odpowiadał zasadzie zgodności z prawem, rzetelności i przejrzystości.
12. **Art. 28 ust. 1** projektu ustawy przewiduje, że *aby móc zostać pracownikiem lub funkcjonariuszem AC należy m.in. wykazywać się nieposzlakowaną opinią oraz odpowiednią zdolnością fizyczną i psychiczną.* Dalsze przepisy projektowanej ustawy nie określają w jaki sposób będzie weryfikowane kryterium nieposzlakowanej opinii, na podstawie jakich kryteriów ustalana będzie czy dana osoba ma nieposzlakowaną opinię, w szczególności jakie informacje i z jakich źródeł będą pozyskiwane, jakie osoby/podmioty i z jakich zasobów mają obowiązek takich informacji udzielić, jak długo przetwarzane będą informacje związane z weryfikacją ww. przesłanki, w tym potwierdzające brak nieposzlakowanej opinii. W odniesieniu do *kryterium odpowiedniej zdolności fizycznej i psychicznej*, tylko art. 28 ust. 3 pkt 5 projektu ustawy odnosi się do tego, że w ramach postępowania kwalifikacyjnego odbywa się „ustalenie zdolności fizycznej i psychicznej do pracy lub służby w AC", bez określenia formy ani trybu tego ustalania. Powyższe kwestie wymagają wyjaśnienia i doprecyzowania dla zachowania zgodności projektowanego przepisu z zasadą zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych , ograniczenia przechowywania.
13. W **art. 28 ust. 3 pkt 1** projektowanej ustawy planuje się, że *Postępowanie kwalifikacyjne składa się z etapów: (...) złożenie podania o zatrudnienie, kwestionariusza osobowego kandydata, a także dokumentów stwierdzających wymagane wykształcenie i kwalifikacje zawodowe oraz zawierających dane o uprzednim zatrudnieniu.* Projektowany przepis nie określa jednak jakie dane mają być zawarte w wymienionym w nim *dokumentach, podaniu o zatrudnienie* oraz *kwestionariuszu osobowym kandydata*. Przepis nie precyzuje również jakie dokumenty

wchodzą w zakres pojęcia „dokumentów stwierdzających wymagane wykształcenie i kwalifikacje zawodowe oraz zawierających dane o uprzednim zatrudnieniu", w szczególności wątpliwości budzi wymaganie od kandydatów „dokumentów zawierających dane o uprzednim zatrudnieniu" bez wyraźnego wskazanie jakie to miałyby być dokumenty oraz jakie dane miałyby zawierać. Powyższe kwestie wymagają wyjaśnienia i doprecyzowania dla zachowania zgodności projektowanego przepisu z zasadą zgodności z prawem, rzetelności i przejrzystości, ograniczenia celu, minimalizacji danych.

Z wyrazami szacunku,

Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

Warszawa, *10-02-2022*

PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Jan Nowak

DOL.401.514.2021.WL.PM

SEKRETARIAT Z-CY SZEFA KS
L.dz. DS.HS.98.2022
Data wpływu 11.02.2022

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu RP
ul. Wiejska 4/6/8
00-902 Warszawa
elektroniczna skrzynka podawcza ePUAP
/KSRP/SkrytkaESP

Szanowny Panie Ministrze,

w związku z korespondencją z dnia 31 stycznia 2022 r. (znak: SPS-WP.020.313.16.20.2021) i przedłożeniem do zaopiniowania autopoprawki do poselskiego projektu **ustawy o Agencji Cyberbezpieczeństwa** organ nadzorczy, z punktu widzenia przepisów *rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietna 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.), zgłasza następującą kwestię.

Organ nadzorczy podtrzymuje uwagę do **art. 28 ust. 1** projektu ustawy, zgłoszoną pismem do Kancelarii Sejmu z dnia 3 listopada 2021 r. (znak: DOL.401.514.2021.WL.PM). Treść autopoprawki nie wpływa na aktualność ww. uwagi.

Z wyrazami szacunku,

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L.dz. SPS-WP.020.313.24.2021
Data wpływu 11.02.2022

Prezes Urzędu Ochrony Danych Osobowych
Jan Nowak

/ - dokument w postaci elektronicznej podpisany kwalifikowanym podpisem elektronicznym/

Urząd Ochrony
Danych Osobowych
ul. Stawki 2
00-193 Warszawa

tel. 22 531-07-20
www.uodo.gov.pl

Biuro Rzecznika
Małych i Średnich Przedsiębiorców

WPL.849.2021.GG

Warszawa, 12 listopada 2021 r.

SEKRETARIAT Z-CY SZEFA KS
L. dz. DS.175.458.2021
Data wpływu 17.11.2021

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-WP.020.313.14.2021
Data wpływu 18. 11. 2021

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu
Kancelaria Sejmu
ul. Wiejska 4/6/8
00-902 Warszawa

Szanowny Panie Ministrze

w odpowiedzi na pismo z dnia 14 października 2021 r., (SPS-WP.020.313.5.2021) w związku z wniesieniem do Sejmu Rzeczypospolitej Polskiej Poselskiego Projektu ustawy o Agencji Cyberbezpieczeństwa[1], na podstawie art. 8 pkt 1 ustawy z dnia 6 marca 2018 r. o Rzeczniku Małych i Średnich Przedsiębiorców[2], który stanowi, że do zadań Rzecznika MŚP należy opiniowanie projektów aktów normatywnych dotyczących interesów przedsiębiorców oraz zasad podejmowania, wykonywania lub zakończenia działalności gospodarczej na terytorium Rzeczypospolitej Polskiej, proszę o przyjęcie poniższej uwagi.

Zagadnienia poruszone w Projekcie mogą być objęte zakresami: projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne (pierwotny tytuł: projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych)[3] i projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości[4].

Biorąc pod uwagę powyższe, należy rozważyć skierowanie Projektu do prac w ramach procedowania ww. projektów ustaw.

z up. Rzecznika Małych i Średnich Przedsiębiorców
Dyrektor Generalny
Dr n. pr. Marek Woch

[1] Znak: EW-020-674/21, dalej: „Projekt".
[2] Dz. U. z 2018 r. poz. 648, dalej: Rzecznik MŚP".
[3] Numer wykazu: UD68.
[4] Wpłynął do Sejmu: 12-11-2021.

Biuro Rzecznika Małych i Średnich Przedsiębiorców
ul. Wilcza 46, 00-679 Warszawa
tel.: +48 22 123 70 70, fax: +48 22 123 70 71, e-mail: biuro@rzecznikmsp.gov.pl, www.rzecznikmsp.gov.pl, NIP: 7010832846, REGON: 380779546

RZECZPOSPOLITA POLSKA

PIERWSZY ZASTĘPCA
PROKURATORA GENERALNEGO
PROKURATOR KRAJOWY

Warszawa, dnia 06.12. 2021 r.

1001-1.0280.70.2021

SEKRETARIAT Z-CY SZEFA KS
L.dz. DS.175.840.21
Data wpływu 13.12.2021

Pan
Dariusz Salamończyk
Zastępca Szefa Kancelarii Sejmu

Szanowny Panie Ministrze

W odpowiedzi na pismo z dnia 14 października 2021 roku nr SPS-WP.020.315.5.2021, dotyczące *poselskiego projektu ustawy o Agencji Cyberbezpieczeństwa*, przekazanego Prokuratorowi Generalnemu do wyrażenia opinii w trybie art. 3 § 1 pkt 12 ustawy z dnia 28 stycznia 2016 roku – *Prawo o prokuraturze*, uprzejmie informuję, że o *projekcie* opinii nie przedstawiam.

z poważaniem

Bogdan Święczkowski

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L.dz. BS-WP.020.313.15.2021
Data wpływu 13.12.2021