PIKE
POLSKA IZBA KOMUNIKACJI
ELEKTRONICZNEJ

Do druku nr 1955

Warszawa, 2 grudnia 2025 roku

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-III.080.368.7.2025
Data wpływu 02.XII.25r.

Sz. Pan

Włodzimierz Czarzasty

Marszałek Sejmu RP

Dotyczy: **Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 1955)**

Szanowny Panie Marszałku!

w imieniu Polskiej Izby Komunikacji Elektronicznej[1] (dalej: „PIKE" lub „Izba"), zwracam się z uprzejmą prośbą o rozważenie modyfikacji obowiązków przedsiębiorców telekomunikacyjnych ujętych w Projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej: „Projekt" lub „uKSC").

Przedstawiona w niniejszym piśmie propozycja to zmiany Projektu zachowujące zasadę proporcjonalności nakładanych obowiązków. Propozycje pozostają w zgodzie z dyrektywą NIS2, którą Projekt transponuje po polskiego prawa. Nie mamy wątpliwości, że zapewnienie odpowiedniego poziomu cyberbezpieczeństwa niesie za sobą koszty, jednak ustawodawca powinien pilnować, aby te koszty były adekwatne i nie prowadziły do konieczności ograniczenia działalności przez najmniejszych przedsiębiorców.

Apelujemy również o wsparcie sektora telekomunikacyjnego w dostosowaniu się do nowych wymogów w Projekcie. Obawiamy się, że wdrożenie nowych wymogów, organizacyjnych i technicznych, będzie oznaczać bardzo wysokie koszty, obciążające w szczególności mikro, małych i średnich przedsiębiorców telekomunikacyjnych.

[1] https://pike.org.pl/o-nas/

1. **Doprecyzowanie rozróżnień pomiędzy podmiotami ważnymi i kluczowymi ze względu na ich wielkość.**

Zwracamy się o doprecyzowanie art. 5 ust. 6 uKSC w taki sposób, aby objął on swym zakresem przedsiębiorców komunikacji elektronicznej. Wydaje się, że brak objęcia ich tym przepisem jest wynikiem przeoczenia.

Zgodnie z art. 5 ust. 1 pkt 1 uKSC podmiotem kluczowym jest m.in. podmiot wskazany w załączniku nr 1, który „przewyższa wymogi dla średniego przedsiębiorstwa". Jednakże przedsiębiorca komunikacji elektronicznej (art. 5 ust. 1 pkt 2 uKSC) będzie uznawany za podmiot kluczowy, gdy „co najmniej spełnia wymogi dla średniego przedsiębiorcy".

Ustalanie wielkości przedsiębiorcy będzie następowało zgodnie z wymogami załącznika I do unijnego rozporządzenia Komisji (UE) nr 651/2014. Zgodnie z tymi zasadami, przy ustalaniu wielkości przedsiębiorcy w oparciu o jego stan zatrudnienia i przychodów, bierze się również pod uwagę jego przedsiębiorstwa powiązane i partnerskie. Są to przedsiębiorstwa, w których dany przedsiębiorca posiada określony poziom udziałów lub to one posiadają odpowiedni poziom udziałów u danego przedsiębiorcy. W uproszczeniu można przyjąć, że ustalając wielkość przedsiębiorcy, do jego pracowników i przychodów należy doliczyć pracowników i przychody przedsiębiorstw z tej samej grupy kapitałowej.

W związku z powyższym przedsiębiorca może być uznany za „przewyższającego wymogi dla średniego przedsiębiorstwa" lub „co najmniej spełniającego wymogi dla średniego przedsiębiorcy" także wówczas, gdy osiąga określone progi w zakresie stanu zatrudnienia i przychodów dopiero po doliczeniu pracowników i przychodów jego przedsiębiorstw powiązanych i partnerskich.

W sytuacji, gdy mikro lub mały przedsiębiorca telekomunikacyjny, ze względu na funkcjonowanie w grupie kapitałowej, jest traktowany jak duży przedsiębiorca („przewyższający wymogi dla średniego przedsiębiorstwa"), przepisy ogólne wskazują, że jest podmiotem kluczowym. Jednak w przypadku, gdy *„Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy, ponieważ przewyższa kryteria dla średniego przedsiębiorstwa zgodnie z* [przepisami nakazującymi doliczanie stanu zatrudnienia i przychodów przedsiębiorstw z tej samej grupy kapitałowej – wyjaśnienie PIKE] *(...), ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi"* (art. 5 ust 6 uKSC), to nie jest podmiotem kluczowym. Z wyjątku tego nie mogą skorzystać przedsiębiorcy telekomunikacyjni samodzielnie będący samodzielnie mikro lub małymi przedsiębiorcami, a w związku z funkcjonowaniem w grupie kapitałowej, przedsiębiorcami średnimi.

Konieczność doprecyzowania wynika z faktu, że już „średni przedsiębiorcy komunikacji elektronicznej" będą uznawani za podmioty kluczowe. Jednakże art. 5 ust. 6 uKSC pozwala nie doliczać pracowników i przychodów przedsiębiorstw z grupy kapitałowej do stanu zatrudnienia i przychodów danego przedsiębiorcy jedynie wówczas, gdy:

- jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub
- nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi oraz
- dany przedsiębiorca spełnia wymogi dla uznania za kluczowy, ponieważ ze względu na ww. doliczanie pracowników i przychodów dany przedsiębiorca przewyższa kryteria dla średniego przedsiębiorstwa.

Sytuacja, gdy podmiot spełnia wymogi do uznania za kluczowy, ponieważ ze względu na ww. doliczanie dany przedsiębiorca osiągnął (lecz nie przewyższył) próg uznania za przedsiębiorcę średniego, nie została przewidziana w art. 5 ust. 6 uKSC.

Zwracamy się o doprecyzowanie przedmiotowych przepisów i nadanie im następującej treści:

„6. Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy ponieważ:

a) przewyższa kryteria dla średniego przedsiębiorstwa,

b) co najmniej spełnia wymogi dla średniego przedsiębiorcy, w przypadku podmiotów, o których mowa w ust. 1 pkt 2) lub,

c) co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy, w przypadku podmiotów, o których mowa w ust. 1 pkt 3)

- zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem kluczowym."

Analogiczne zmiany należy wprowadzić w art. 5 ust. 7, chociaż nie dotyczą one już bezpośrednio przedsiębiorców komunikacji elektronicznej. Wątpliwości, uzasadniające zmianę, odnoszą się natomiast np. do dostawców usług zarządzanych, będących mikro przedsiębiorcami. Jeżeli dostawca usług zarządzanych, spełnia wymogi dla małego przedsiębiorstwa ze względu na ww. doliczanie, będzie podmiotem kluczowym. Jednocześnie, jeżeli samodzielnie jest mikro przedsiębiorcą, nie będzie mógł skorzystać z wyłączenia, o którym mowa w ust. 7 – ponieważ warunkiem skorzystania z wyłączenia jest bycie co najmniej średnim przedsiębiorcą.

2. Niezależność systemów informacyjnych

Zgodnie z dyrektywą NIS2, w przypadku ustalania wielkości podmiotu, należy brać pod uwagę

> *„niezależność od przedsiębiorstw partnerskich lub powiązanych pod względem sieci i systemów informatycznych, z których korzysta przy świadczeniu usług, a także pod względem świadczonych przez siebie usług"* (motyw 16 preambuły NIS2).

Reguły te zostały wprowadzone do uKSC w art. 5 ust. 6 i 7. Niestety, pojęcie „niezależne systemy informacyjne" pozostawia bardzo duże wątpliwości interpretacyjne. Zwracamy się o wprowadzenie doprecyzowania wskazującego, że regulacja dotyczy systemów informacyjnych wykorzystywanych bezpośrednio do świadczenia usług wspólnie z przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, a nie wszystkich systemów informacyjnych. Jako przykład możemy podać system CRM, który nie jest wykorzystywany bezpośrednio do świadczenia usług i jego wspólne wykorzystanie nie powinno automatycznie implikować wpływu na ustalenie wielkości przedsiębiorstwa.

Zwracamy się o nadanie art. 5 ust. 6 uKSC *in fine* następującego brzmienia:

> *„(...) ale jego system informacyjny wykorzystywany bezpośrednio do świadczenia usług jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem kluczowym."*

Analogiczna zmiana powinna zostać wprowadzona w art. 5 ust. 7 uKSC.

3. Nierówne traktowanie podmiotów prywatnych oraz podmiotów publicznych.

Przepisy uKSC nierówno traktują podmioty publiczne i niepubliczne. Podmioty niepubliczne, będące podmiotami ważnymi, mają znacząco większe obowiązki niż podmioty publiczne, również będące podmiotami ważnymi. Ta nierówność znacząco uderzy w sektor telekomunikacyjny – niemal 4 tysiące przedsiębiorców telekomunikacyjnych wkrótce będzie podmiotami regulowanymi w uKSC.

Jawi się pytanie, **czy naruszenie cyberbezpieczeństwa w podmiotach niepublicznych niesie większe zagrożenia niż naruszenie cyberbezpieczeństwa w podmiotach publicznych?**

Odpowiedź na to pytanie jest o tyle istotna, że NIS2 nie różnicuje obowiązków podmiotów niepublicznych oraz publicznych.

Postulujemy zrównanie obowiązków podmiotów tych dwóch kategorii. Zwracamy się o wprowadzenie następującej zmiany:

- Art. 8 ust. 1 uKSC

„Podmiot kluczowy ~~lub podmiot ważny~~ wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

(...)" (konieczne są również odpowiadające zmiany w pkt 2 lit. e, pkt 5 lit. d)

- Art. 8 ust. 2 uKSC

„Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. e, podmiot kluczowy ~~i podmiot ważny~~ uwzględnia:

(...)"

- Art. 8 ust. 3 uKSC

„Podmiot ważny ~~będący podmiotem publicznym~~ nie stosuje przepisu ust. 1. Podmiot ważny ~~będący podmiotem publicznym~~ opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy."

Ewentualnie, w przypadku nieuwzględnienia powyższego postulatu, zwracamy się o wprowadzenie regulacji uwzględniających zasadę proporcjonalności dla najmniejszych przedsiębiorców telekomunikacyjnych. Z uKSC wynika, że wszyscy przedsiębiorcy telekomunikacyjni wejdą do krajowego systemu cyberbezpieczeństwa – również ci najmniejsi. Zwracamy się o nałożenie na mikro- i małych przedsiębiorców telekomunikacyjnych, którzy będą podmiotami ważnymi, regulacji odpowiadających regulacjom podmiotów ważnych będących podmiotami publicznymi. Zwracamy się o wprowadzenie następującej zmiany w art. 8 ust. 3 uKSC:

„Podmiot ważny będący:

a) podmiotem publicznym

b) mikro- lub małym przedsiębiorcą telekomunikacyjnym

- nie stosuje przepisu ust. 1. Podmiot ważny będący podmiotem publicznym lub mikro- lub małym przedsiębiorcą telekomunikacyjnym opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy."

4. Dostosowanie maksymalnej kary pieniężnej do poziomu określonego w NIS2

Zwracamy się o modyfikację maksymalnego wymiaru kary do poziomu ustalonego w przepisach europejskich. Polski ustawodawca podwyższył wymiar maksymalnej kary względem określonego w NIS2. Zgodnie z art. 34 ust. 4 NIS2 maksymalna kara pieniężna nakładana na podmioty ważne powinna wynosić maksymalnie 7 milionów euro, zaś na podmioty kluczowe – 10 milionów euro (lub wyższe, uwzględniając odpowiedni poziom przychodów).

Tymczasem w projekcie uKSC przewiduje się maksymalną karę w wysokości aż 100 milionów złotych, niezależnie od przychodów przedsiębiorstwa. Jest to zagrożenie nieproporcjonalne i nie mieszczące się w przygotowaniu racjonalnego modelu sankcji za naruszenie przepisów cyberbezpieczeństwa. Czy mikro przedsiębiorca telekomunikacyjny powinien być zagrożony karą 100 milionów złotych?

Zwracamy się o wykreślenie art. 73 ust. 5 uKSC.

5. Dodatkowe kary, niewymagane przez NIS2

Projekt uKSC zawiera nadmiarowe, względem wymogów NIS2, sankcje karne. Dodatkowe możliwości nałożenia kary oznaczają większe ryzyko prowadzenia działalności, co w oczywisty sposób przekłada się na wyższy koszt prowadzenia działalności. Zagrożenie karą pieniężną polskich przedsiębiorców, w sytuacji w której konkurenci z innych Państw Członkowskich UE nie będą taką karą zagrożeni, w oczywisty sposób stawia ich w gorszej pozycji konkurencyjnej – z inicjatywy Ministra Cyfryzacji!

NIS2 nie przewiduje sankcji za każdy dzień nierealizowania nakazów organu właściwego do spraw cyberbezpieczeństwa (art. 53 ust 5 w zw z art. 76b uKSC). Za naruszenie przepisów ustawy przewidziane są kary w określonej w przepisach maksymalnej wysokości, nakładane z uwzględnieniem przesłanek wskazanych w uKSC. Tymczasem projekt przewiduje (dodatkowe!) kary okresowe za każdy dzień nierealizowania określonych kategorii decyzji.

Zwracamy się o wykreślenie art. 76b uKSC.

Ewentualnie, zwracamy się o uzupełnienie art. 76b uKSC o katalog przesłanek, jakie organ właściwy do spraw cyberbezpieczeństwa bierze pod uwagę nakładając karę, jak również widełek kary powiązanych z poziomem przychodów (lub wielkością) przedsiębiorcy. Obecnie, zgodnie z projektem, organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę 100 000 złotych za dzień opóźnienia wykonania decyzji nawet na mikroprzedsiębiorcę!

6. Kary pieniężne pod rygorem natychmiastowej wykonalności.

Generalną regułą nakładania kar pieniężnych jest nienadawanie decyzjom nakładającym kary rygoru natychmiastowej wykonalności.

Jako przykład można wskazać art. 446 ust. 1 zdanie 2 ustawy Prawo komunikacji elektronicznej (z 2024 roku!): *„Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.”.*

Tymczasem w uKSC umożliwiono organom właściwym do spraw cyberbezpieczeństwa do nakładania rygoru natychmiastowej wykonalności na decyzje nakładające kary pieniężne. Co więcej, projektodawca planuje znacząco złagodzić przesłanki nakładania rygoru na tę kategorię decyzji administracyjnych względem ogólnych reguł określonych w Kodeksie postępowania administracyjnego.

Zwracamy się o nienakładanie na decyzje nakładające kary rygoru natychmiastowej wykonalności. Spełnienie wszystkich nowych obowiązków przewidzianych w uKSC będzie wiązało się z ponoszeniem regularnych wydatków. Gdy określony podmiot nie wykona tych obowiązków prawidłowo, w pierwszej kolejności powinien mieć możliwość przeznaczenia środków finansowych na jak najszybsze naprawienie swoich błędów, zamiast tracić je na karę finansową, na którą nałożono rygor natychmiastowej wykonalności. Wnosimy o nadanie art. 74 ust. 4 uKSC następującego brzmienia:

> *~~„Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub ust. 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego.~~ Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.”.*

7. Długość obowiązywania polecenia zabezpieczającego

Jedną z kluczowych instytucji nowego krajowego systemu cyberbezpieczeństwa jest „polecenie zabezpieczające”. Na podstawie polecenia zabezpieczającego, minister właściwy do spraw informatyzacji, w przypadku wystąpienia incydentu krytycznego, może m.in. nakazać szczególną konfigurację produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności lub zakazać korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego (art. 67g ust. 9 uKSC).

Polecenie zabezpieczające podlega natychmiastowej wykonalności. Zgodnie z uKSC (art. 67g ust. 12 i 13), polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.

Ze względu na dużą uciążliwość techniczną i organizacyjną polecenia zabezpieczającego, zwracamy się o modyfikację przepisów dot. długości trwania polecenia zabezpieczającego. Wnosimy, aby termin obowiązywania polecenia zabezpieczającego pokrywał się z terminem koordynacji obsługi incydentu krytycznego i termin ten mógł wynosić co najwyżej dwa lata. Innymi słowy, nie powinno być możliwości ustalenia „z góry" obowiązywania polecenia zabezpieczającego na dwa lata, niezależnie od trwania koordynacji obsługi incydentu krytycznego.

Zwracamy się o nadanie art. 67g ust. 12 uKSC następującego brzmienia:

> *„12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego ~~lub na czas oznaczony, nie dłużej niż na dwa lata~~.*
>
> *13. Polecenie zabezpieczające wygasa:*
>
> *1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, oraz ~~lub~~*
>
> *2) ~~po upływie czasu, na który zostało wydane~~ nie później niż po dwóch latach."*

8. Rezygnacja z natychmiastowego zamykania prowadzonej działalności.

Wśród uprawnień organu właściwego do spraw cyberbezpieczeństwa są m.in. (art. 53 ust. 9 uKSC):

- wstrzymanie koncesji (art. 53 ust. 9 pkt 1 uKSC),
- wstrzymanie w całości albo w części działalność podmiotu ważnego kluczowego wpisanego do rejestru działalności regulowanej (art. 53 ust. 9 pkt 2 uKSC),
- wstrzymanie zezwolenie na prowadzenie działalności gospodarczej wydane podmiotowi ważnemu kluczowemu (art. 53 ust. 9 pkt 3 uKSC),
- wstrzymanie w całości albo w części działalności (art. 53 ust. 9 pkt 4 uKSC),
- zakazanie pełnienia w podmiocie ważnym lub kluczowym funkcji zarządczych przez kierownika podmiotu (art. 53 ust. 9 pkt 6 uKSC).

Decyzja w której organ właściwy do spraw cyberbezpieczeństwa stosuje powyższe środki jest wykonalna z dniem jej doręczenia (art. 53e ust. 9 uKSC). Postępowanie administracyjne jest jednoinstancyjne (art. 53e ust. 10 uKSC). Należy docenić zmianę projektu i wprowadzenie możliwości zaskarżenia decyzji do sądu administracyjnego (art. 53e ust. 10 uKSC). Co jednak istotne, decyzja jest wykonalna już od momentu jej doręczenia, a nie upływu czasu na złożenie skargi. Co więcej, złożenie skargi do sądu administracyjnego nie wstrzymuje jej wykonania.

Wnosimy o modyfikację powyższych przepisów w ten sposób, aby złożenie skargi do sądu administracyjnego, ze względu na szczególną dolegliwość ww. uprawnień względem przedsiębiorców, powodowało wstrzymanie ich wykonalności do czasu rozstrzygnięcia sprawy przez sąd. Aktualny projekt zakłada, że wniesienie skargi do sądu na mniej uciążliwe środki nadzorcze, przewidziane w art. 53 ust. 5 uKSC, powoduje wstrzymanie wykonania środków z art. 53 ust. 9 uKSC. Jednakże wniesienie skargi na same środki z art. 53 ust. 9 uKSC już nie powoduje wstrzymania ich wykonania.

Zwracamy się o nadanie art. 53e ust. 10 uKSC następującego brzmienia:

> *„10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3–5, podmiot kluczowy może wnieść skargę do sądu administracyjnego. Wniesienie skargi do sądu administracyjnego wstrzymuje wykonanie decyzji."*

[PODSUMOWANIE]

Stosowanie uKSC przez wszystkich przedsiębiorców objętych jej przepisami, w szczególności mikro- i małych przedsiębiorców, nie powinno rodzić wątpliwości interpretacyjnych. Nakładane obowiązki nie powinny prowadzić do nieproporcjonalnych ryzyk prowadzenia działalności gospodarczej.

Proponowane w niniejszym piśmie zmiany w uKSC wpisują się w konieczność zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w Polsce. Jednocześnie racjonalizują obowiązki przedsiębiorców lub doprecyzowują postanowienia projektu. Zwracamy się o wprowadzenie opisanych zmian w projekcie ustawy nowelizującej ustawę o krajowym systemie cyberbezpieczeństwa.

PIKE deklaruje pełną gotowość do współpracy i udzielenia ewentualnych dalszych wyjaśnień w zakresie przedstawionych propozycji.

B. Łaga

Bogdan Łaga
Prezes Zarządu Polskiej Izby Komunikacji Elektronicznej