KRAJOWA IZBA
RADCÓW PRAWNYCH

OŚRODEK BADAŃ, STUDIÓW I LEGISLACJI KRAJOWEJ RADY RADCÓW PRAWNYCH

KRAJOWA IZBA RADCÓW PRAWNYCH | ul. Powązkowska 15, 01-797 Warszawa | tel.: 22 300 86 40 | kirp@kirp.pl | NIP 5261043011

Warszawa, dnia 4 grudnia 2025 r.

Stanowisko Ośrodka Badań, Studiów i Legislacji
Krajowej Rady Radców Prawnych
w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 1955)

W związku z wpłynięciem do Sejmu w dniu 7 listopada 2025 roku projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (druk nr 1955, dalej jako „**projekt nowelizacji UKSC**") Ośrodek Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych (dalej również jako „**KRRP**") jest zainteresowany przedstawieniem swojego stanowiska do projektowanych przepisów.

Ośrodek Badań, Studiów i Legislacji KRRP zauważa potrzebę wyrażenia swojego stanowiska co do projektu nowelizacji UKSC, która ma na celu wdrożenie do polskiego systemu prawnego regulacji wynikających z **dyrektywy NIS 2**[1].

Zgłoszone uwagi dotyczą przy tym zarówno przepisów, które mogą potencjalnie wpływać na świadczenie pomocy prawnej przez radców prawnych, jak i innych istotnych regulacji projektu nowelizacji UKSC.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)

I. Uwagi ogólne

1. Forma i treść projektu nowelizacji.

Projektowane przepisy mają na celu wdrożenie do polskiego systemu prawnego regulacji wynikających z unijnej **dyrektywy NIS 2**. Zgodnie z założeniami autorów projektu, implementacja dyrektywy NIS 2 ma nastąpić poprzez zmianę obowiązującej ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej jako „**UKSC**"). Zdaniem KRRP takie rozwiązanie nie jest jednak najwłaściwsze. Uwzględniając szeroki zakres i dużą ilość modyfikacji, a także mając na uwadze konieczność zapewnienia przejrzystości i dostępności procesu legislacyjnego, bardziej zasadne byłoby opracowanie nowej ustawy.

Za takim podejściem przemawiają nie tylko względy praktyczne, lecz także regulacje Zasad techniki prawodawczej[2], gdzie w § 84 jednoznacznie wskazano, że jeżeli projektowane zmiany są liczne lub ingerują w konstrukcję bądź spójność dotychczasowej ustawy, wówczas właściwym trybem jest przygotowanie projektu nowego aktu prawnego.

2. Pojęcie „świadczonej usługi" i „systemu informacyjnego wykorzystywanego do świadczenia usługi".

Projekt nowelizacji UKSC posługuje się pojęciami **„świadczonej usługi"** oraz **„systemu informacyjnego wykorzystywanego w procesie świadczenia usługi"**.

Pojęcie „usługi" nie zostało jednak nigdzie zdefiniowane i stanowi ono raczej pozostałość po nomenklaturze stosowanej we wciąż obowiązującej UKSC, co w praktyce może budzić istotne wątpliwości interpretacyjne co do zakresu stosowania projektowanej regulacji.

Poważne wątpliwości budzi fakt, że projekt nowelizacji UKSC posługuje się pojęciem systemu wykorzystywanego „**w procesie**" świadczenia usługi – a więc bardzo szerokiego spektrum możliwości. „W procesie" świadczenia usług wykorzystuje się bowiem wiele różnych systemów informacyjnych – jak np. systemy do komunikacji, oprogramowanie biurowe czy programy antywirusowe – które są współcześnie niezbędne do prowadzenia działalności gospodarczej, ale nie są technologicznie powiązane z celem „świadczenia usługi". Analizując brzmienie projektowanych przepisów zachodzi jednak obawa, że również tego rodzaju systemy wykorzystywane jedynie wspomagająco przez organizację do innych celów niż świadczenie usług, przez które dany podmiot jest podmiotem ważnym lub kluczowym stanowić będzie element „procesu" świadczenia usługi, wobec czego również do nich będą się odnosić regulacje projektu nowelizacji UKSC. Natomiast **realizacja wielu obowiązków wynikających**

[2] Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie "Zasad techniki prawodawczej"

z projektu nowelizacji UKSC w kontekście tego rodzaju systemów (np. w zakresie obowiązku audytowego) **może okazać się nieproporcjonalna oraz wręcz niewykonalna** z uwagi na warunki licencyjne narzucane przez międzynarodowych dostawców tych systemów.

Mając powyższe na uwadze **KRRP postuluje uzupełnienie komentowanych przepisów poprzez jednoznaczne wyjaśnienie pojęcia „świadczonej usługi" (lub jego zastąpienie regulacją bardziej oddającą cele dyrektywy NIS 2), a także wskazanie, jakich konkretnie systemów mają dotyczyć obowiązki wynikające z projektu nowelizacji UKSC**.

3. Wiążąca wykładnia przepisów ustawy.

Przepisy projektu nowelizacji UKSC w wielu miejscach są niejasne i posługują się bardzo ogólnymi pojęciami przez co mogą stwarzać liczne wątpliwości interpretacyjne w praktyce stosowania przyszłej regulacji. Będzie to miało szczególne znaczenie już po uchwaleniu przepisów projektu nowelizacji UKSC, gdy wywrą one bezpośredni wpływ na sytuację podmiotów, co do których – nawet tylko potencjalnie – projekt nowelizacji UKSC może mieć zastosowanie. Wątpliwości interpretacyjne mogą zatem pojawić się zarówno na poziomie identyfikacji, czy określony podmiot w ogóle kwalifikuje się do grupy podmiotów kluczowych i ważnych, jak i na poziomie realizacji poszczególnych obowiązków wynikających z projektu nowelizacji UKSC.

Aby przeciwdziałać temu problemowi, **KRRP postuluje wdrożenie rozwiązań, które umożliwią zainteresowanym podmiotom zwrócenie się do ministra właściwego do spraw informatyzacji, odpowiedniego organu nadzoru lub innego właściwego podmiotu z wnioskiem o wydanie prawnie wiążącej interpretacji co do stosowania przepisów znowelizowanej UKSC**.

Tego rodzaju możliwość byłaby szczególnie przydatna w odniesieniu do regulacji z zakresu prawa nowych technologii (w tym cyberbezpieczeństwa), które z uwagi na swój technologiczny charakter stwarzają istotne trudności w praktyce stosowania prawa. **Problem ten został przy tym zauważony przez ustawodawcę m.in. w ramach prac nad projektem ustawy o systemach sztucznej inteligencji**, gdzie wprost przewidziano możliwość zwrócenia się do odpowiedniej komisji z wnioskiem o wydanie opinii indywidualnej w zakresie stosowania przepisów tej ustawy. Ponadto **podobne regulacje już teraz znajdują się w polskim systemie prawnym – przykładowo w przepisach Ordynacji podatkowej**[3] przewidziano możliwość zwrócenia się do Dyrektora Krajowej Informacji Skarbowej z wnioskiem o wydanie indywidualnej interpretacji przepisów prawa podatkowego.

[3] Ustawa z dnia 29 sierpnia 1997 r. Ordynacja podatkowa

KRAJOWA IZBA RADCÓW PRAWNYCH | ul. Powązkowska 15, 01-797 Warszawa | tel.: 22 300 86 40 | kirp@kirp.pl | NIP 5261043011

II. Uwagi dotyczące wpływu na świadczenie pomocy prawnej

W tym zakresie Krajowa Rada Radców Prawnych pragnie zwrócić szczególną uwagę na brzmienie art. 2 pkt 4i) znowelizowanego UKSC[4] i pojęcie *dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa* definiowanego jako:

> osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym obsługę incydentów, testów bezpieczeństwa, audytów systemów informacyjnych, doradztwo.

W konsekwencji takiego sformułowania definicji *dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa* **istnieje ryzyko, że pojęcie to może być wykładane w ten sposób, że w jego zakres mogą także wchodzić osoby świadczące pomoc prawną, które doradzają od strony prawnej w kwestii regulacji UKSC** (a więc również radcowie prawni) np. w zakresie prawidłowego wdrożenia wymogów wynikających z projektu nowelizacji UKSC lub w zakresie wsparcia w zgłaszaniu incydentów do organów nadzorczych.

Jednocześnie zgodnie z art. 2 pkt 4h) znowelizowanego UKSC każdy *dostawca usług zarządzanych w zakresie cyberbezpieczeństwa*, który stanowi co najmniej małe przedsiębiorstwo (tj. zatrudnia co najmniej 10 pracowników lub jego roczny obrót lub suma bilansowa przekracza 2 mln euro), będzie uznawany za podmiot kluczowy. Jeżeli więc wskazana wyżej interpretacja byłaby zgodna z wolą ustawodawcy, **istniałoby ryzyko nieproporcjonalnego i niezamierzonego przez unijnego prawodawcę włączenia w krąg podmiotów kluczowych również podmiotów świadczących usługi doradcze, ale niemające charakteru technicznego – a więc również radców prawnych**.

Należy bowiem zauważyć, że **pojęcie do*stawcy usług zarządzanych w zakresie cyberbezpieczeństwa* w rozumieniu projektu nowelizacji UKSC nie jest spójne z rozumieniem tego pojęcia na gruncie przepisów dyrektywy NIS 2**. Zgodnie z art. 6 pkt 39 i 40 dyrektywy NIS 2, pod pojęciem *dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa* rozumie się:

> podmiot, który świadczy usługi związane z **instalacją, eksploatacją lub konserwacją produktów, sieci, infrastruktury, aplikacji ICT lub innych sieci i systemów informatycznych lub z zarządzaniem nimi**, poprzez pomoc lub aktywną administrację prowadzoną u klientów lub zdalnie, który prowadzi działania związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań.

[4] Odwołania do przepisów „znowelizowanego UKSC" odnoszą się do jednostek redakcyjnych, które otrzymałyby przepisy UKSC po uchwaleniu i wejściu w życie projektu nowelizacji UKSC

Oznacza to, że **przepisy dyrektywy NIS 2 jednoznacznie wiążą pojęcie *dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa* z instalacją, eksploatacją, konserwacją lub zarządzaniem produktami, sieciami, infrastrukturą, aplikacjami ICT lub innymi sieciami i systemami informatycznych. Pod pojęciem tym nie mieszczą się tym samym usługi o charakterze doradczym, które nie mają technicznego charakteru**.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje zmianę definicji *dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa* poprzez jednoznacznie powiązanie tego pojęcia ze świadczeniem usług związanych z instalacją, eksploatacją, konserwacją lub zarządzaniem produktami, sieciami, infrastrukturą, aplikacjami ICT lub innymi sieciami i systemami informatycznymi** – tak jak ma to miejsce na gruncie przepisów dyrektywy NIS 2.

III. Uwagi szczegółowe.

1. Zakres podmiotowy regulacji, problemy definicyjne.

Definiując rodzaje podmiotów operujących w ramach sektorów „cyfrowych" projekt nowelizacji UKSC w wielu miejscach wykracza poza ramy wyznaczone przez dyrektywę NIS 2. Część pojęć została w nim ujęta w sposób niejasny, a niektóre nie zostały zdefiniowane w ogóle. Skutkuje to rozbieżnością pomiędzy projektem nowelizacji UKSC a dyrektywą NIS 2 w jednym z najistotniejszych obszarów, jakim jest zakres podmiotowy projektowanej regulacji.

W związku z tym KRRP pragnie zwrócić uwagę na:

1. **Niezrozumiałą definicję pojęcia *dostawców chmury obliczeniowej*, które umożliwia potencjalnie bardzo szeroką interpretację tego pojęcia.**

   Zgodnie z projektem nowelizacji UKSC praktycznie każda usługa świadczona w modelu SaaS (Software as a Service) może być rozumiana jako usługa chmury obliczeniowej, nawet jeśli stanowi ona jedynie nieznaczną działalność danego podmiotu, co w ocenie KRRP należy uznać za działanie niecelowe i nieproporcjonalne.

2. **Brak ograniczenia zakresu działalności *dostawców usług zarządzanych* oraz *dostawców usług zarządzanych w zakresie cyberbezpieczeństwa* do usług świadczonych wyłącznie w modelu B2B (między przedsiębiorcami).**

   Choć w załączniku nr 1 do dyrektywy NIS 2 wprost wskazano, że o zarządzaniu usługami ICT jest mowa wyłącznie w relacjach między przedsiębiorcami, to projekt nowelizacji UKSC nie zawiera takiego ograniczenia. Ponadto w samych definicjach pojęcia *dostawców usług zarządzanych* oraz *dostawców usług zarządzanych w zakresie cyberbezpieczeństwa* wskazano, że do zakresu tego pojęcia zaliczają się również osoby fizyczne.

3. **Włączenie w zakres sektora infrastruktury cyfrowej *podmiotów świadczących usługi rejestracji nazw domen***.

   W myśl dyrektywy NIS 2 *podmioty świadczące usługi rejestracji nazw domen* stanowią autonomiczną grupę podmiotów, odrębną od podmiotów kluczowych oraz ważnych.

4. **Wadliwie zdefiniowane pojęcie *dostawcy sieci dostarczania treści*.**

   Za dostawcę sieci dostarczania treści uważa się „*osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe **do** sieci rozproszonych geograficznie serwerów (…)*”.

   Definicja ta zawiera jednak bardzo istotną różnicę w stosunku do dyrektywy NIS 2. Zgodnie z logiką dyrektywy NIS 2 dostarczanie treści i usług cyfrowych powinno się odbywać **„w ramach” – a nie „do”** – sieci rozproszonych geograficznie serwerów. W przeciwnym razie praktycznie każda aktywność użytkownika w sieci mogłaby zostać potencjalnie powiązana z tym pojęciem.

5. **Brak zdefiniowania pojęcia *dostawcy punktu wymiany ruchu internetowego*.**

   Projekt nowelizacji UKSC nie definiuje pojęcia *dostawców punktu wymiany ruchu internetowego*, mimo że tego rodzaju podmioty zostały uwzględnione w ramach sektorów kluczowych.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. wprowadzenie jasnych i czytelnych przesłanek, które umożliwią rozgraniczenie, którzy *dostawcy chmury obliczeniowej* – zwłaszcza w kontekście usług świadczonych w modelu SaaS – będą regulowani przepisami projektowanej regulacji;
2. ograniczenie zakresu działalności *dostawców usług zarządzanych* oraz *dostawców usług zarządzanych w zakresie cyberbezpieczeństwa* do usług świadczonych wyłącznie w modelu B2B (między przedsiębiorcami);
3. wykreślenie *podmiotów świadczących usługi rejestracji nazw domen* z załącznika nr 1 do projektu nowelizacji UKSC;
4. modyfikację pojęcia *dostawców sieci dostarczania treści*;
5. zdefiniowania pojęcia *dostawców punktu wymiany ruchu internetowego*.

2. Działanie w ramach grupy kapitałowej.

W projekcie nowelizacji UKSC przewidziano regulację, zgodnie z którą podmiot ujęty w załączniku nr 1 lub 2 do projektu, spełniający kryteria dla co najmniej średniego przedsiębiorcy, lecz posiadający system informacyjny „niezależny" od systemów jego przedsiębiorstw powiązanych lub partnerskich lub niewykonujący usług „wspólnie" z tymi przedsiębiorstwami, nie zostanie zaliczony do kategorii podmiotów kluczowych ani ważnych. **Jednocześnie projektodawca nie doprecyzował, jak należy rozumieć „niezależność" systemu informacyjnego ani czym jest „wspólne" świadczenie usług**.

Jednocześnie, w ocenie KRRP, w przywołanym przepisie **błędnie użyto spójnika „lub" zamiast „oraz"** przy określaniu relacji pomiędzy kryterium niezależności systemu a wspólnym świadczeniem usług. Ponadto **projektowane wyłączenie obejmuje jedynie podmioty kwalifikujące się co najmniej jako przedsiębiorcy średniej wielkości**. W efekcie, jeżeli dany podmiot zostałby uznany za podmiot kluczowy lub ważny na innej podstawie niż art. 5 ust. 1 pkt 1 albo art. 5 ust. 2 pkt 1 i 2 znowelizowanego UKSC, to nie mógłby skorzystać z omawianego wyłączenia. Powstaje więc pytanie, czy rzeczywiście taki był intencjonalny zamysł ustawodawcy.

Warto także zauważyć, że projekt nowelizacji UKSC **nie przewiduje żadnych wyłączeń dla podmiotów należących do grup kapitałowych, które świadczą usługi wyłącznie na rzecz innych spółek z grupy**. W wielu grupach funkcjonują wyspecjalizowane podmioty – informatyczne centra usług wspólnych (CUW) – obsługujące wyłącznie podmioty powiązane lub partnerskie. Taki model organizacyjny umożliwia rozwijanie wyspecjalizowanych zespołów oraz efektywną organizację usług IT w ramach grupy. Jeżeli centra te nie świadczą usług poza strukturą grupy kapitałowej, brak jest uzasadnienia, aby ich działalność była kwalifikowana jako świadczenie usług zarządzanych (w tym usług zarządzanych w zakresie cyberbezpieczeństwa) objętych reżimem dyrektywy NIS 2 i projektu nowelizacji UKSC. Obecne brzmienie projektu nie przewiduje jednak takiego wyłączenia, co – w ocenie KRRP – uzasadnia potrzebę jego jednoznacznego wprowadzenia.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. wyjaśnienie pojęcia „niezależnego" systemu informacyjnego oraz „wspólnego" świadczenia usług;
2. zastąpienie w omawianym przepisie spójnika „lub" spójnikiem „oraz";
3. objęcie analizowanym wyłączeniem wszystkich podmiotów bez względu na ich wielkość;
4. wyłączenie spod regulacji projektu nowelizacji UKSC podmiotów, które świadczą usługi wyłącznie na rzecz podmiotów wchodzących w skład własnej grupy kapitałowej.

3. Zakres stosowania przepisów do podmiotów zagranicznych.

Projekt nowelizacji UKSC posługuje się **nieprecyzyjnymi i niejednoznacznymi określeniami**, takimi jak „kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji" czy „realizowanie zadań związanych z systemem zarządzania bezpieczeństwem informacji". Tak niedookreślona terminologia rodzi liczne możliwości interpretacyjne, utrudniając spójne i przewidywalne stosowanie przepisów.

Projektowana regulacja nie odnosi się również do sytuacji podmiotów, które – mimo że posiadają spółkę zarejestrowaną w Polsce i uczestniczą w procesie świadczenia usług na terytorium RP – **nie mają realnego wpływu na sposób wykonywania usług i ich bezpieczeństwo**.

Problem ten dotyczy m.in. dostawców usług chmury obliczeniowej, którzy w Polsce pełnią funkcję „pośrednika" dla spółki zarejestrowanej w innym państwie UE. Podmioty te mają jednostki organizacyjne na terytorium RP oraz zarządzają własnym systemem bezpieczeństwa informacji, ale jednocześnie nie posiadają w Polsce osoby odpowiedzialnej za bezpieczeństwo faktycznie świadczonych usług chmurowych.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje doprecyzowania analizowanego przepisu tak, aby umożliwiał jednoznaczne ustalenie, do jakich podmiotów ma on zastosowanie**.

4. Rozporządzenia Rady Ministrów określające szczegółowe wymagania dla systemów zarządzania bezpieczeństwem informacji.

W projekcie nowelizacji UKSC przewidziano upoważnienie dla Rady Ministrów do wydawania – w formie rozporządzeń – szczegółowych wymagań dotyczących systemów zarządzania bezpieczeństwem informacji, przy czym regulacje te mają być zróżnicowane w zależności od rodzaju działalności prowadzonej przez podmioty kluczowe oraz ważne.

Projekt nowelizacji UKSC **nie przewiduje jednak żadnego okresu przejściowego**, który umożliwiłby podmiotom kluczowym i ważnym dostosowanie się do nowych wymagań określonych w przyszłych rozporządzeniach. Jest to szczególnie istotne w przypadku aktów wykonawczych, które zwykle podlegają krótszym i mniej szczegółowym konsultacjom publicznym.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. ustanowienie na poziomie ustawowym obowiązku przeprowadzenia konsultacji publicznych przed przyjęciem tych rozporządzeń;
2. ustanowienie na poziomie ustawowym minimalnego sześciomiesięcznego vacatio legis – bądź innego adekwatnego okresu – umożliwiającego dostosowanie się do nowych wymogów regulacyjnych.

5. Badanie produktów, usług i procesów ICT w celu identyfikacji podatności.

Projekt nowelizacji UKSC w istotnym zakresie rozszerza dotychczasowe kompetencje zespołów CSIRT w obszarze badania produktów, usług i procesów ICT w celu identyfikacji podatności. Zgodnie z proponowanymi regulacjami właściwe zespoły CSIRT będą mogły wykorzystywać techniki obejmujące m.in. obserwację oraz analizę działania urządzeń i oprogramowania, pozyskiwanie dostępu do danych, odtwarzanie postaci źródłowej oprogramowania, kopiowanie kodu programistycznego oraz dokonywanie jego translacji.

Co istotne, w trakcie prowadzenia takich badań **zespoły CSIRT nie będą związane warunkami umownymi – w szczególności postanowieniami licencyjnymi** – dotyczącymi produktów, usług lub procesów ICT, jeżeli ograniczałyby one możliwość przeprowadzenia badania. **Przepisy nie przewidują również konieczności uzyskania zgody licencjodawcy bądź dysponenta** produktu, usługi lub procesu ICT.

Zdaniem KRRP tak daleko idące uprawnienia **mogą w sposób nieproporcjonalny ingerować w prawa dostawców oraz użytkowników produktów, usług i procesów ICT, stwarzając istotne ryzyko naruszenia praw własności intelektualnej**. W konsekwencji przyjęcie analizowanych rozwiązań może skutkować ograniczeniem gotowości zagranicznych dostawców do oferowania swoich usług i rozwiązań na rynku polskim, ze względu na obawy przed naruszeniem przysługujących im praw.

Dodatkowo projektowane przepisy **nie określają kryteriów kwalifikowania produktów, usług czy procesów ICT do przeprowadzenia badania**, a samo badanie miałoby być realizowane bez wiedzy dostawców czy użytkowników. **Ustawa nie przewiduje również obowiązku zachowania poufności** przez osoby przeprowadzające badanie, nie uznaje pozyskanych informacji za prawnie chronione ani nie nakłada obowiązku ich niezwłocznego zniszczenia.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje usunięcie art. 33 ust. 1c – 1f znowelizowanego UKSC lub w braku decyzji o całkowitym usunięciu tych przepisów:**

1. ustanowienie jasnych zasad kwalifikowania produktów, usług i procesów ICT do badania;
2. ustanowienie obowiązku uprzedniego poinformowania co najmniej dostawcy o zamiarze przeprowadzenia badania;
3. ustanowienie obowiązku poinformowania dostawcy o przeprowadzeniu badania – najpóźniej w terminie 7 dni od jego zakończenia;
4. zobowiązanie osób prowadzących badanie do zachowania poufności, uznanie pozyskanych informacji za informacje prawnie chronione oraz nałożenie obowiązku ich niezwłocznego zniszczenia.

6. Ocena bezpieczeństwa.

W projekcie nowelizacji UKSC określono zasady przeprowadzania przez właściwe zespoły CSIRT oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.

Projektowane przepisy **nie przewidują jednak żadnych kryteriów kwalifikowania podmiotów do objęcia oceną bezpieczeństwa. Brakuje także regulacji określających maksymalny czas trwania takiej oceny, jak również wyłączeń dla podmiotów, które samodzielnie i regularnie przeprowadzają testy bezpieczeństwa swoich systemów**.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. jednoznaczne określenie zasad kwalifikowania podmiotów kluczowych i ważnych do przeprowadzenia oceny bezpieczeństwa;
2. wskazanie maksymalnego czasu trwania oceny na poziomie 5 dni roboczych;
3. wyłączenie stosowania tych przepisów dla podmiotów, które we własnym zakresie systematycznie realizują ocenę bezpieczeństwa.

7. Organy właściwe do sprawowania nadzoru.

Projekt nowelizacji UKSC **nie zawiera przepisów właściwie regulujących możliwości wystąpienia sporu kompetencyjnego w sytuacji, gdy określony podmiot będzie podmiotem kluczowym lub ważnym jednocześnie w kilku sektorach gospodarki**.

Choć w uzasadnieniu do projektu nowelizacji UKSC wskazano, że organ właściwy może stosować środki nadzorcze tylko w zakresie obejmującym sektor, który został mu przypisany, a w sytuacji zbiegu nadzoru będzie możliwość stworzenia przez organy właściwe wspólnych metodyk nadzoru, to **metodyki te będą najprawdopodobniej rozwiązaniem wtórnym, niemożliwym do zastosowania w momencie wystąpienia sporu**. Tym samym projektowane przepisy nie przewidują trwałej i jednoznacznej metody rozwiązywania sporów kompetencyjnych, **co w praktyce może naruszać interesy podmiotów nadzorowanych z uwagi na brak określoności prawa w tym zakresie**.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje wprowadzenie przepisów jednoznacznie regulujących zasady wykonywania nadzoru nad podmiotem kluczowym lub ważnym, który jednocześnie działa w kilku sektorach gospodarki, w stosunku do których zostały wyznaczone różne organy właściwe** (np. poprzez wyznaczanie wiodącego organu nadzoru w momencie wpisania podmiotu do wykazu podmiotów kluczowych i ważnych).

8. Dostawcy wysokiego ryzyka.

W projekcie nowelizacji UKSC przewidziano wprowadzenie procedury pozwalającej na uznanie dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, co z kolei będzie skutkowało zakazem stosowania (oraz nakazem wycofania z użytku) określonych typów produktów, usług lub procesów ICT przez podmioty kluczowe i ważne.

Mechanizm ten nie wynika z przepisów dyrektywy NIS 2, ani innych unijnych regulacji**. Abstrahując od oceny zasadności wprowadzenia tego rodzaju instytucji** KRRP pragnie zwrócić uwagę na konsekwencje oraz sposób jej wdrożenia.

Fakt wszczęcia odpowiedniego postępowania oraz poinformowania o tym opinii publicznej **może prowadzić do powstania efektu mrożącego wobec podmiotów, które takiemu postępowaniu podlegają**. Wystarczy bowiem sama informacja o wszczęciu procedury – jeszcze przed jakimkolwiek merytorycznym rozstrzygnięciem – aby podmioty kluczowe i ważne zrezygnowały z relacji gospodarczych z potencjalnym dostawcą, obawiając się przyszłego obowiązku wycofania jego sprzętu lub oprogramowania. Natomiast gdy sama

decyzja zostanie już wydana, to przepisy projektu nowelizacji UKSC **nie przewidują obowiązku bezpośredniego informowania podmiotów kluczowych i ważnych o wydaniu takiej decyzji**, mimo że podmioty te w praktyce muszą się do niej stosować.

Odnosząc się natomiast do uwag natury proceduralnej, na decyzję o uznaniu podmiotu za dostawcę wysokiego ma być nakładany **rygor natychmiastowej wykonalności**, a projekt nowelizacji UKSC **wyłącza możliwość złożenia wniosku o ponowne rozpatrzenie sprawy**.

Projektowane przepisy **nie przewidują również możliwości podjęcia działań naprawczych** przez dostawcę, wobec którego prowadzone jest postępowanie, **ani mechanizmu okresowej weryfikacji**, czy podmiot uznany za dostawcę wysokiego ryzyka nadal spełnia przesłanki do takiej kwalifikacji.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. wykreślenie przepisów przewidujących natychmiastową wykonalność decyzji;
2. wprowadzenie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy;
3. umożliwienie dostawcy podjęcia działań naprawczych przed wydaniem decyzji;
4. wprowadzenie obowiązku bezpośredniego informowania podmiotów kluczowych i ważnych o wydaniu decyzji (np. za pośrednictwem systemu S46);
5. ustanowienie procedury przeglądowej zapewniającej okresową weryfikację zasadności utrzymywania statusu dostawcy wysokiego ryzyka.

9. Polecenie zabezpieczające.

W projekcie nowelizacji UKSC wprowadzono instytucję polecenia zabezpieczającego, wydawanego w celu skoordynowania reakcji na incydent krytyczny. Rozwiązanie to **nie wynika z przepisów dyrektywy NIS 2** i – podobnie jak ma to miejsce w przypadku procedury uznania za dostawcę wysokiego ryzyka – **nie zabezpiecza w pełni praw podmiotów, których może ono dotyczyć**.

Przede wszystkim należy zauważyć, że polecenie zabezpieczające będzie **podlegało natychmiastowemu wykonaniu i nie będzie przysługiwał od niego wniosek o ponowne rozpatrzenie sprawy**. Co więcej, projekt nowelizacji UKSC **nie wprowadza żadnego minimalnego okresu na dostosowanie się przez podmioty kluczowe i ważne do jego treści**, mimo że polecenie zabezpieczające uznaje się za doręczone z chwilą jego ogłoszenia w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Jednocześnie warto zauważyć, że podmioty kluczowe i ważne **nie zostaną bezpośrednio poinformowane**

o wydaniu takiego polecenia, mimo że byłoby to techniczne wykonalne bez nadmiarowych obciążeń administracyjnych.

Propozycja KRRP:

Mając powyższe na uwadze KRRP postuluje:

1. wykreślenie przepisów przewidujących natychmiastową wykonalność decyzji;
2. wprowadzenie możliwości złożenia wniosku o ponowne rozpatrzenie sprawy;
3. wprowadzenie obowiązku bezpośredniego poinformowania podmiotów kluczowych i ważnych o wydaniu decyzji (choćby za pośrednictwem systemu S46);
4. wprowadzenie na poziomie ustawowym minimalnego okresu na dostosowanie się przez podmioty kluczowe i ważne do treści polecenia zabezpieczającego – wynoszącego co najmniej 14 dni roboczych.

10. Kara pieniężna w wysokości do 100 mln zł.

W projekcie nowelizacji UKSC wprowadzono możliwość nałożenia na podmiot kluczowy lub ważny kary pieniężnej w wysokości do 100 mln zł, jeżeli taki podmiot naruszy przepisy ustawy, powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi; lub 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług.

Taka regulacja **nie znajduje swojego odpowiednika w przepisach dyrektywy NIS 2**, a także **nie znajduje uzasadnienia dla jej wprowadzenia**, jako że określony w dyrektywie NIS 2 oraz projekcie nowelizacji UKSC pułap kar na poziomie nawet 10 mln euro zdecydowanie przewyższa obecnie obowiązujące limity kar, a tym samym **w pełni realizuje prewencyjne i represyjne funkcje kar pieniężnych**.

Co więcej, taki sposób zredagowania analizowanego przepisu przyznaje organom administracji publicznej **dowolność co do sposobu interpretacji przesłanek do nałożenia kary pieniężnej**, umożliwiając nałożenie kary w wysokości nawet 100 mln zł za praktycznie każde naruszenie przepisów. Przyjęcie tak niedookreślonych przesłanek do nałożenia kary pieniężnej **narusza przy tym zasadę określoności przepisów prawnych**, wyrażoną chociażby w § 75 ust. 1 w zw. z § 81a ust. 3 Zasad techniki prawodawczej, zgodnie z którym znamiona czynu zabronionego powinny zostać określone w sposób wyczerpujący.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje wykreślenie art. 73 ust. 5 nowelizowanego UKSC**. Alternatywnie, na wypadek nieuwzględnienia powyższego postulatu, **KRRP wskazuje na potrzebę doprecyzowania przesłanek do nałożenia kary pieniężnej na podstawie tego przepisu**.

11. Natychmiastowa wykonalność kar pieniężnych

W projekcie nowelizacji UKSC przewidziano, że właściwy organ nadzoru będzie mógł nadać decyzji o nałożeniu kar pieniężnych rygor natychmiastowej wykonalności, jeśli – w ocenie organu – wymaga tego ochrona bezpieczeństwa lub porządku publicznego.

W opinii KRRP **trudno wskazać sytuację, w których natychmiastowa egzekucja kary pieniężnej – mającej charakter wyłącznie represyjny i następczy wobec popełnionego naruszenia – byłaby niezbędna dla zapewnienia bezpieczeństwa lub porządku publicznego**. Pojęcia te mają zresztą bardzo szeroki i nieprecyzyjny charakter, co umożliwia ich swobodną interpretację przez organy nadzoru.

W konsekwencji istnieje ryzyko, że **regulacje dotyczące nadawania natychmiastowej wykonalności będą stosowane w sposób nadmierny**, prowadząc do sytuacji, w której organ mógłby niemal natychmiast nałożyć i wyegzekwować karę sięgającą nawet 100 mln zł, podczas gdy ocena legalności takiego działania pozostawałaby w gestii sądów administracyjnych, rozpatrujących sprawę w długotrwałym postępowaniu.

Propozycja KRRP:

Mając powyższe na uwadze **KRRP postuluje wykreślenie art. 74 ust. 4 nowelizowanego UKSC**.

Autor opinii: r.pr. Agnieszka Wachowska