Uwagi do projektu ustawy z dnia 7 lutego 2025 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw - projekt z dnia 7 lutego 2025 r.

I. Uwagi ogólne

1. Uwagi do sposobu procedowania (dotychczasowego przebiegu prac legislacyjnych)

Dotychczasowy przebieg prac z Projektem ustawy budzi wątpliwości co do zgodności ze standardami obowiązującymi w procesie legislacyjnym, w szczególności ze względu na to, że:

- **Projekt ustawy nie był przedmiotem ponownych konsultacji publicznych i opiniowania, pomimo wprowadzenia w nim daleko idących zmian, istotnych dla całej projektowanej regulacji.**

  Chodzi m.in. o zmiany w załączniku nr 1, w zakresie pojęcia „podmiot publiczny", które mają znaczenie dla definicji podmiotu kluczowego i podmiotu ważnego, a których zakres został istotnie zmodyfikowany oraz wprowadzenie nowych zasad tymczasowego wstrzymywania koncesji, zezwoleń i zgód na działalność (opisane poniżej).

  Dlatego przed przystąpieniem do dalszego procedowania Projekt ustawy wymaga przeprowadzenia dodatkowych konsultacji i opiniowania w zakresie ww. zmian. Zwraca na to uwagę m.in. Rządowe Centrum Legislacji w swoich uwagach przekazanych w procesie legislacyjnym[1].

  Równocześnie, ze względu na liczbę uwag zgłoszonych przez Ministerstwa (protokół rozbieżności obejmujący niemalże 40 uwag wyłącznie z Komitetu ds. Europejskich, a więc ograniczony jedynie do uwag „europejskich"), apelujemy o skorzystanie z kompetencji, o których mowa w § 61 ust. 1 Regulaminu pracy Rady Ministrów i zobowiązanie organu wnioskującego do skierowania Projektu ustawy do ponownych uzgodnień oraz przeprowadzenie konferencji uzgodnieniowej z udziałem strony społecznej.

- **Projekt ustawy nie był przedmiotem rozpatrzenia przez właściwe komitety, tj. Komitet Ekonomiczny Rady Ministrów, ani Komitet Rady Ministrów do spraw Bezpieczeństwa Narodowego.**

[1] Zob. Pismo Wiceprezes RCL z dnia 13 lutego 2025 r. (RCL.DISIP.550.5.2024).

Biorąc pod uwagę treść i zakres projektowanych regulacji, Projekt ustawy wymaga rozpatrzenia przez:

- **Komitet Ekonomiczny Rady Ministrów (KERM)** – ze względu na potencjalne istotne skutki gospodarcze, a także brak rzetelnego oszacowania kosztów wprowadzenia nowych regulacji w OSR dołączonej do uzasadnienia. Do zadań KERM należy m.in. analizowanie i rozpatrywanie przedłożeń członków Rady Ministrów dotyczących gospodarki i w sprawach o przewidywanych istotnych skutkach finansowych lub gospodarczych. Ma to szczególne znaczenie ze względu na rolę KERM w wyznaczeniu optymalnych kierunków działań organów administracji rządowej w zakresie polityki gospodarczej (§ 2 ust. 1 pkt 1 i 3 Zarządzenia nr 11 Prezesa Rady Ministrów z dnia 5 lutego 2024 r. w sprawie Komitetu Ekonomicznego Rady Ministrów). Wobec istotnego wpływu, jaki Projekt ustawy może mieć dla zdolności rozwojowych gospodarki i jakości otoczenia regulacyjnego przedsiębiorców i obywateli, powinien on zostać skierowany pod obrady KERM;

- **Komitet Rady Ministrów do spraw Bezpieczeństwa Narodowego**, do którego zadań należy rozpatrywanie projektów aktów prawnych o istotnym wpływie na zagadnienia bezpieczeństwa i obrony państwa oraz bezpieczeństwa cyberprzestrzeni, niezbędne w ramach powierzonej Komitetowi koordynacji działań w tych sprawach (§ 2 pkt 1 i 3 w zw. z § 2 ust. 2 Zarządzenia nr 53 Prezesa Rady Ministrów z dnia 16 maja 2024 r. w sprawie Komitetu Rady Ministrów do spraw Bezpieczeństwa Narodowego).

W związku z tym apelujemy o podjęcie działań, zmierzających do skierowania Projektu ustawy do rozpatrzenia przez ww. Komitety. Zwracamy przy tym uwagę, że jest to obowiązek, a nie uprawnienie organu wnioskującego.

- **Projekt ustawy nie został dotąd skierowany do zaopiniowania przez Radę Legislacyjną.**

Tymczasem, ze względu na istotne skutki prawne i gospodarcze projektowanych przepisów, oraz fakt, że Projekt ustawy zawiera przepisy wykraczające poza zakres wynikający z obowiązku transpozycji Dyrektywy NIS2, powinien podlegać zaopiniowaniu przez Radę Legislacyjną. Jest to tym bardziej uzasadnione w świetle powierzonych Radzie Legislacyjnej zadań z zakresu oceny metod i sposobów wdrażania prawa Unii Europejskiej, w tym praktyki tzw. goldplatingu, zasad techniki prawodawczej, a także opiniowania projektów ustaw z punktu widzenia ich zgodności z Konstytucją Rzeczypospolitej Polskiej, prawem Unii Europejskiej oraz spójności z obowiązującym systemem prawa.

W tym miejscu podkreślamy, że Rada Legislacyjna wydała dotychczas opinię o ściśle związanej z Projektem ustawie o certyfikacji cyberbezpieczeństwa, jednak bez uwzględnienia relacji pomiędzy tymi projektami, przepisami unijnymi i wprowadzonymi zmianami.

Dlatego oczekujemy, że Projekt ustawy zostanie skierowany do zaopiniowania przez Radę Legislacyjną, a wnioski sformułowane przez Radę – uwzględnione w toku dalszych prac legislacyjnych.

2. Uwagi do treści projektowanej regulacji

Niezależnie od powyższych uwag co do dotychczasowego sposobu procedowania z Projektem ustawy oraz postulatów dotyczących dalszego przebiegu prac, zwracamy uwagę, że **część projektowanych rozwiązań w ramach dodawanego do ustawy o krajowym systemie cyberbezpieczeństwa Rozdziału 12a, budzą uzasadnione wątpliwości co do ich zgodności z prawem Unii Europejskiej i Konstytucją RP, a także z zasadami techniki prawodawczej, w tym ze standardami prawidłowej legislacji dotyczącymi implementacji aktów prawa unijnego.**

a. Nadregulacja (goldplating) w stosunku do obowiązków wynikających z Dyrektywy NIS2

Projekt ustawy zawiera szereg rozwiązań, w tym obowiązki i przepisy sankcjonujące, których wprowadzenie do ustawy nie jest niezbędne dla prawidłowej implementacji Dyrektywy NIS2. Mimo, że ich wprowadzenie uzasadnia się koniecznością transpozycji Dyrektywy NIS2, nie tylko nie są one obowiązkowe w świetle przepisów Dyrektywy, ale też znacznie wykraczają poza zakres i cele tego aktu.

Tymczasem, jak wskazuje Europejski Komitet Ekonomiczno-Społeczny, *„państwa członkowskie nie powinny pod pretekstem transpozycji dyrektyw dokonywać rewizji części swoich przepisów krajowych, które nie są bezpośrednio objęte prawodawstwem wspólnotowym (gold plating) lub zmieniać niektórych przepisów prawa krajowego, ograniczając ich zakres oraz prawa obywateli lub przedsiębiorstw, przypisując „Brukseli" odpowiedzialność za zmiany*"[2].

Wśród przewidzianych w Projekcie ustawy rozwiązań, które wykraczają poza to, co niezbędne dla prawidłowej implementacji Dyrektywy NIS2, stanowiąc nadregulację, której motywy budzą uzasadnione wątpliwości są:

- obowiązek przygotowania i aktualizacji dokumentacji dotyczącej bezpieczeństwa systemów informacyjnych (projektowany art. 10),
- obowiązek wyznaczania co najmniej dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (projektowany art. 9 ust. 1 pkt 1),
- zakres obowiązków, jakie może nałożyć minister właściwy do spraw informatyzacji w poleceniu zabezpieczającym (projektowany art. 67g ust. 10),

[2] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie komunikatu Komisji Europejskiej „Skuteczna Europa — Stosowanie prawa wspólnotowego" (2008/C 204/02)

Jednak najbardziej oczywistym przykładem nadregulacji jest przyznanie organowi właściwemu do spraw cyberbezpieczeństwa kompetencji do ingerowania w wydane koncesje, zezwolenia i działalność, w tym działalność regulowaną, podmiotów kluczowych. Chodzi o projektowany art. 53 ust. 9 i n. ustawy o krajowym systemie cyberbezpieczeństwa, który przewiduje, że w razie niezastosowania się do nakazu podjęcia określonych czynności dotyczących obsługi incydentu lub niewykonania decyzji nakazującej podjęcie działań określonych w art. 53 ust. 5 pkt 2-8, **organ ten może wstrzymać lub ograniczyć ww. koncesje, zezwolenia lub działalność**. Jest to oczywista nadregulacja względem Dyrektywy NIS2, która w art. 32 ust. 5 wskazuje, iż w przypadku niewykonania tego rodzaju nakazu należy zapewnić, że organ właściwy do spraw cyberbezpieczeństwa może:

- tymczasowo zawiesić zezwolenie, certyfikat lub działalność podmiotu kluczowego, lub
- zwrócić się do organu, który przyznał zezwolenie, koncesje lub innej zgodę na prowadzenie działalności , lub do sądu, zgodnie z prawem krajowym, o tymczasowe zawieszenie certyfikacji lub zezwolenia na niektóre lub wszystkie odpowiednie usługi świadczone bądź na część lub całość działalności prowadzonej przez podmiot kluczowy.

Tak ukształtowany katalog Dyrektywy NIS2 pozostawia Państwu Członkowskiemu swobodę regulacyjną wyboru czy organ ds. cyberbezpieczeństwa może działać samodzielnie w zakresie tymczasowego zawieszenia zezwolenia, koncesji lub działalności, za pośrednictwem organu, który wydał koncesję, zezwolenie lub inną zgodę na działalność, czy też za pośrednictwem sądu. **Swoboda w tym zakresie została przyznana celowo, by dopasować wymogi Dyrektywy NIS2 do specyfiki i zasad krajowych, zgodnie z zasadą autonomii proceduralnej Państw Członkowskich, tak by krajowe zasady udzielania i wstrzymywania tego rodzaju zezwoleń, koncesji czy zgód były nienaruszone, a nowe procedury wymagane na mocy art. 32 ust. 5 Dyrektywy NIS2 poszanowane w jak największym stopniu.** Dyrektywa NIS2 **podkreśla to, używając wielokrotnie zwrotu „zgodnie z prawem krajowym" i wskazując,** iż owe tymczasowe środki stosuje się z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą Praw Podstawowych, w tym prawa do skutecznej ochrony prawnej i do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

Na tym tle Projekt ustawy błędnie i nietrafnie wprowadza nieznaną prawu polskiemu instytucję, której nie przewiduje Prawo przedsiębiorców, ani regulacje sektorowe. Biorąc pod uwagę szeroki zakres branż i działalności, jakich może dotyczyć to uprawnienie, skorzystanie z kompetencji przyznanych przez art. 53 ust. 9 może skutkować paraliżem funkcjonowania wielu podmiotów, w tym podmiotów, których działalność służy zaspokajaniu kluczowych potrzeb społecznych i gospodarczych (dystrybucja leków i wyrobów medycznych, gospodarka odpadami, przewozy lotnicze, wytwarzanie i przesyłanie ciepła i energii elektrycznej). Ponadto organ właściwy do spraw cyberbezpieczeństwa **może właściwie wkroczyć w kompetencje organu merytorycznego, właściwego w sprawie wydania danego zezwolenia, udzielenia koncesji lub wpisu na listę działalności regulowanej, co nie jest ani celem, ani wymogiem art. 32 ust. 5 Dyrektywy NIS2**. Projektowana regulacja nie została w żaden sposób skorelowana z przesłankami udzielania, cofania lub zawieszenia udzielonych zezwoleń (koncesji, wpisów), określonymi w odpowiednich regulacjach sektorowych. Niejasna jest relacja pomiędzy zakresem kompetencji organu właściwego do spraw cyberbezpieczeństwa i organu merytorycznego (właściwego w sprawie wydania zezwolenia, koncesji itd.), a także charakter i zakres związania organu merytorycznego działaniem organu właściwego do spraw cyberbezpieczeństwa.

W związku z tym apelujemy o wprowadzenie odpowiednich gwarancji proceduralnych, zapewniających z jednej strony adekwatną kontrolę sądową, z drugiej – należytą koordynację pomiędzy organem właściwym do spraw cyberbezpieczeństwa i organem merytorycznym. Ponadto, jeśli – zgodnie z deklaracjami projektodawców – środek ten ma stanowić „ultima ratio", przesłanki jego zastosowania powinny być określone w sposób jasny, precyzyjny i zawężający, chroniąc podmioty kluczowe przed nieuzasadnioną ingerencją w ich prawa nabyte i interesy w toku (a w skrajnych przypadkach – w istotę gwarantowanej konstytucyjnie swobody działalności gospodarczej).

3. Obowiązek notyfikacji technicznej

Projekt ustawy zawiera przepisy techniczne w rozumieniu Dyrektywy 2015/1535[3] i rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych.

W związku z tym powinien podlegać notyfikacji w trybie określonym w tych przepisach.

Chodzi o projektowane art. 67b-67g i art. 67h-67l ustawy o krajowym systemie cyberbezpieczeństwa (art. 1 pkt 71 Projektu ustawy), które wprowadzają ograniczenia w obrocie komponentami ICT. Przepisy te należy uznać za przepisy techniczne, ponieważ zakazują wprowadzania do obrotu lub stosowania produktu. Stanowią „inne wymagania", o których mowa w art. 1 ust. 1 lit. f Dyrektywy 2015/1535, czyli „*wymagania inne niż specyfikacje techniczne, nałożone na produkt w celu ochrony, w szczególności konsumentów lub środowiska, które wpływają na jego cykl życia po wprowadzeniu go na rynek, takie jak warunki użytkowania, powtórnego przetwarzania, ponownego zastosowania lub usuwania, gdzie takie warunki mogą mieć istotny wpływ na skład lub rodzaj produktu lub obrót nim*".

Ograniczenia te wykraczają poza zakres Dyrektywy NIS2, a ich przyjęcie nie jest niezbędne do jej skutecznej transpozycji, dlatego nie korzystają z wyłączenia od obowiązku notyfikacyjnego, o którym mowa w art. 5 ust. 1 Dyrektywy 2015/1535.

A zatem – wbrew ocenie projektodawców, zawartej w uzasadnieniu projektu – przepisy te powinny być przedmiotem notyfikacji technicznej. Naruszenie tego obowiązku spowoduje, że będą one nieskuteczne i nie można ich można egzekwować w stosunku do podmiotów indywidualnych. W takim przypadku, w razie powołania się przez jednostkę na brak notyfikacji w postępowaniu przed sądem krajowym, będzie on musiał odmówić zastosowania nienotyfikowanych przepisów[4].

[3] Dyrektywa (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiająca procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (ujednolicenie) (Dz. U. UE. L. z 2015 r. Nr 241, str. 1).
[4] Zob. wyrok TSUE z dnia 26 września 2000 r., Unilever, sprawa C-443/98, EU:C:2000:496, pkt 44, 49–51.

Wskazujemy, iż inne kraje implementujące rozwiązania związane z bezpieczeństwem sieci 5G dokonały notyfikacji technicznej TRIS m.in. hiszpański Dekret Królewski zatwierdzający Krajowy System Bezpieczeństwa sieci i usług 5G (2023/0761/ES), belgijska ustawa wprowadzająca dodatkowe środki bezpieczeństwa w **odniesieniu** do świadczenia usług telefonii komórkowej 5G (2021/0206/B), belgijski projekt dekretu królewskiego w sprawie wymagań dotyczących lokalizacji sieci 5G (2022/0396/B), belgijski projekt dekretu królewskiego w sprawie zezwoleń ministerialnych w kontekście wdrażania sieci 5G (2022/0397/B), irlandzka część 3 projektu ustawy o regulacji łączności z 2022 r. (2022/0850/IRL), fiński projekt rozporządzenia w sprawie kluczowych części sieci łączności (2021/0137/FIN), słoweński akt komunikacji elektronicznej (2021/0899/SI) oraz hiszpańska Ustawa o wymogach zapewniających bezpieczeństwo sieci i usług łączności elektronicznej piątej generacji (2021/0604/E), a także portugalski wniosek dotyczący ustawy upoważniającej rząd do transpozycji dyrektywy (UE) 2022/2555 w sprawie środków mających na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii, zatwierdzającej ramy prawne cyberbezpieczeństwa.

Brak wymaganej notyfikacji będzie skutkował naruszeniem przez Polskę obowiązków traktatowych i Dyrektywy 2015/1535. W związku z tym przyjęcie projektowanych przepisów bez ich uprzedniej notyfikacji może **być podstawą roszczeń** odszkodowawczych **do Skarbu Państwa z tytułu tzw. bezprawia legislacyjnego. Skutkiem będzie też stan niepewności prawnej**, związany z brakiem skuteczności nienotyfikowanych przepisów i możliwością podważenia ich mocy wiążącej w każdym postępowaniu sądowym

4. Wątpliwości co do zgodności z prawem UE i zasadą proporcjonalności

Projektowane rozwiązania dotyczące procedury uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka (projektowany art. 67b-67g i art. 67h-67l ustawy o krajowym systemie cyberbezpieczeństwa) budzą poważne wątpliwości co do zgodności z prawem Unii Europejskiej, w tym:

- **z art. 4 ust. 1, art. 27 i art. 54 Rozporządzenia 2024/2847 (Cyber Resilience Act)**[5] – zgodnie z którymi państwa członkowskie nie utrudniają udostępniania na rynku produktów z elementami cyfrowymi zgodnych z Rozporządzeniem (w odniesieniu do spraw objętych jego zakresem), a domniemuje się, że produkt jest bezpieczny, jeśli producent stosuje procedury i normy wskazane w Rozporządzeniu i w aktach wykonawczych Komisji. Rozporządzenie wprowadza też specjalną procedurę, w ramach której producent powinien podjąć działania naprawcze, w wykluczenie produktów z rynku jest możliwe dopiero w razie ich nieprzeprowadzenia lub w braku ich skuteczności – co jest wprost sprzeczne z rozwiązaniami zawartymi w Projekcie ustawy;

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz. U. UE. L. z 2024 r. poz. 2847).

- **z treścią i samymi założeniami Rozporządzenia Parlamentu Europejskiego i Rady 2019/881**[6] - w zakresie, w jakim za dostawcę wysokiego ryzyka mógłby zostać uznany podmiot legitymujący się certyfikatami wydanymi w trybie określonym w tym Rozporządzeniu (w ramach europejskich programów certyfikacji cyberbezpieczeństwa);
- **z celami Dyrektywy NIS2 -** podczas gdy Dyrektywa NIS2 w art. 24 przyznaje państwom członkowskim możliwość wymagania od podmiotów ważnych i kluczowych korzystania z komponentów ICT, które posiadają odpowiednie certyfikacje, w Projekcie ustawy przewidziano rozwiązania, które w istocie zakazują korzystania z niektórych komponentów (projektowany art. 67c). Celem prawodawcy unijnego było ustanowienie rozwiązań, które nie będą się wiązały z „nakładaniem nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na podmioty kluczowe i ważne" (motyw 81. Preambuły). Tymczasem dokładnie takie skutki wiążą się z projektowaną konstrukcją;
- **ogólnymi zasadami traktatowymi wynikającymi z art. 34 i 35 Traktatu o funkcjonowaniu Unii Europejskiej** – ponieważ prowadzą do nieproporcjonalnego ograniczenia swobody przepływu towarów wprowadzanych na rynek unijny przez podmioty z innych krajów UE. Chociaż uzasadniana względami bezpieczeństwa państwa, ingerencja ta nie spełnia testu proporcjonalności i może być uznana za dyskryminującą. Wynika to zarówno z samej konstrukcji procedury, jak i z arbitralnego charakteru przesłanek uznania dostawcy za dostawcę wysokiego ryzyka.
- **z art. 19 ust. 1 Traktatu o Unii Europejskiej w zakresie prawa do sądu** – ponieważ zgodnie z Projektem ustawy wydawanej przez ministra decyzji lub poleceniu zabezpieczającemu ma z mocy ustawy przysługiwać rygor natychmiastowej wykonalności. Wprawdzie od decyzji tej ma przysługiwać skarga do sądu administracyjnego, jednak bez przeprowadzania rozprawy, a także z ograniczeniem prawa skarżącego do zapoznania się z pełną treścią uzasadnienia (to ma otrzymać wyłącznie minister.

Wobec tego apelujemy o usunięcie tych przepisów z Projektu ustawy, albo co najmniej uspójnienie przepisów odnoszących się do procedury HRV z bezpośrednio skutecznymi przepisami prawa unijnego i standardami wynikającymi z aktów prawa unijnego.

W szczególności uspójnienia wymaga relacja między procedurą certyfikacji, będącą główną ścieżką unijnego rozwoju cyberbezpieczeństwa, a procedurą HRV.

W efekcie optymalnym i rekomendowanym rozwiązaniem byłoby wyodrębnienie przepisów poleceń zabezpieczających oraz procedury dostawcy wysokiego ryzyka do odrębnego projektu ustawy. W tym zakresie wnosimy o podzielenie projektu na dwa odrębne: jeden będący implementacją dyrektywy NIS2, który powinien być szybko procedowany, bez zbędnych nadregulacji.

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15 z późn. zm.).

Drugi projekt zawierałby rozwiązania nie wynikające z dyrektywy NIS2, które wymagają pogłębionej analizy i oceny skutków regulacji oraz uspójnienia z regulacjami o certyfikacji cyberbezpieczeństwa.

II. Uwagi szczegółowe

Lp.	Jednostka redakcyjna projektu ustawy, do którego odnosi się uwaga	Proponowana zmiana przepisu	Uzasadnienie zmiany przepisu
1	**Art. 1 pkt 8**		Projekt ustawy w art. 1 pkt 8 dokonuje zmiany art. 5 ustawy o KSC znacznie rozszerzając zakres podmiotowy obecnie obowiązującej ustawy. Art. 1 pkt 8 projektu ustawy znacznie rozszerza katalog podmiotów objętych znowelizowaną ustawą oraz nakłada szereg obowiązków na podmioty, które zostaną uznane za podmioty kluczowe i ważne, a dotychczas nie miały statusu operatora usług kluczowych. W szczególności, przy tak szeroko sformułowanych zapisach, odwołujących się nadto do rozporządzenia 651/2014/UE, oznaczać to może, że spółka z grupy kapitałowej może być uznana za podmiot kluczowy lub ważny tylko z powodu przynależności do grupy (wyłączenia ze zmienianego art. 5 ust. 2 pkt 6 i 7 ustawy o KSC należy uznać za niewystarczające). Ponadto, **wnosimy o sprecyzowanie zwrotu "nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi"**, poprzez wskazanie kierunków jego interpretacji, bądź to bezpośrednio w treści aktu, bądź poprzez uzupełnienie w tym zakresie uzasadnienia projektu; w szczególności wymaga wyjaśnienia, czy chodzi wyłącznie o bezpośredni udział tych podmiotów w świadczeniu usług (jak na przykład występowanie względem kontrahentów, osobisty udział w wytwarzaniu, dostawie lub sprzedaży produktów), czy też ustanawiana przesłanka negatywna ma nie mieć zastosowania już w sytuacji jedynie pośredniego

			udziału (jak na przykład zapewnianie know-how, zaplecza osobowego, administracyjnego lub technicznego, i tym podobne); wyjaśnienie pomoże usunąć potencjalne wątpliwości odnośnie objęcia niektórych podmiotów obowiązkami z ustawy, a z drugiej strony ograniczy ryzyko nadużywania przesłanki, która wydaje się mieć ocenny charakter.
2	**Art. 1 pkt 12**		Podmioty kluczowe i ważne będą musiały, odmiennie niż ma to miejsce do tej pory, dokonać **w ciągu 3 miesięcy** samooceny, czy spełniają kryteria dla podmiotu kluczowego ważnego oraz same złożyć wniosek o wpis w wykazie (Art. 7 c zmienianej ustawy o KSC), przy czym wniosek o wpis będzie podpisywał kierownik jednostki w rozumieniu ustawy o rachunkowości pod rygorem odpowiedzialności karnej. Nakłada to, w odróżnieniu od poprzedniego stanu prawnego, na szereg podmiotów nieobjętych dotąd zakresem podmiotowym ustawy o KSC nowe obowiązki w zakresie samoidentyfikacji oraz nowe obowiązki wynikające ze zmienianego art. 8 ustawy o KSC (m.in. Art. 1 pkt 13 i 14 projektu ustawy). Należy w związku z tym postulować wydłużenie ww. terminu 3 miesięcy do co najmniej 6 miesięcy.
3	**Art. 1 pkt 15**		Zgodnie z nowym Art. 8 c ustawy o KSC odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa będzie ponosić kierownik podmiotu, którym zgodnie z nowym art. 2 pkt 8 a) ma być kierownik jednostki w rozumieniu ustawy o rachunkowości. Jest to znaczne rozszerzenie kręgu osób odpowiedzialnych w porównaniu z Dyrektywą NIS 2, która mówi o „organie zarządzającym". Tym samym projektowane zapisy znacznie wychodzą poza zakres Dyrektywy NIS 2, co wprowadza odpowiedzialność w zakresie wykonywania obowiązków z zakresu cyberbezpieczeństwa także innych osób, nie tylko członków zarządu spółki (Art. 8 c i nast. zmienianej ustawy o KSC). Ponadto, obowiązki i odpowiedzialność kierownika podmiotu kluczowego lub podmiotu ważnego zostały sformułowane bardzo szeroko, np. zgodnie z nowym Art. 8 d pkt 4 kierownik ten ma zapewnić, „że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie", co oznacza, że w przypadku spółki liczącej kilkuset pracowników kierownik ma odpowiadać za znajomość zagadnień z cyberbezpieczeństwa przez każdego pracownika, nawet wykonującego pracę zupełnie niezwiązaną z cyberbezpieczeństwem. Zdecydowanie wykracza to poza motyw 89 Dyrektywy NIS2, zgodnie z którym podmioty kluczowe i ważne powinny „organizować szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, pishingu lub technik inżynierii społecznej". Nowy Art. 8 d pkt 4 ustawy o KSC powinien zatem brzmieć: „zapewnia, że personel podmiotu ma dostęp do szkoleń na temat cyberzagrożeń, pishingu lub technik inżynierii społecznej".

4	**Art. 1 pkt 2 lit. k**		Zgodnie z proponowanym brzmieniem nowego art. 2 pkt 14 ustawy o KSC system informacyjny to m.in. „urządzenie lub grupa połączonych urządzeń”. Literalna wykładnia tak sformułowanego przepisu może prowadzić do wniosku, że za system informacyjny należy uznać także pojedynczy komputer. Należy zatem postulować wykreślenie słów: „urządzenie lub”.
5.	**Art. 1 pkt 9**		W poprzedniej wersji projektu (z 18/11/2024) wprowadzono zmiany w art. 5a, w których w miejsce wskazania na stosowanie ustawy krajowej przez podmioty posiadające jednostkę organizacyjną w RP wskazano na stosowanie jej jeżeli *podmiot ma miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzi działalność na terytorium RP przez swoją siedzibę, oddział lub w ramach działalności transgranicznej*. W szczególności wątpliwości budzi dodanie zwrotu „lub w ramach działalności transgranicznej”. Tabela zgodności załączona do projektu zamieszczonego 6/12/2024 jest w tym zakresie nieaktualna.

Art. 26	Artykuł 26 Jurysdykcja i terytorialność 1. Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym mają miejsce prowadzenia działalności, z następującymi wyjątkami: a) dostawców publicznych sieci łączności elektronicznej lub dostawców publicznie dostępnych usług łączności	TAK	Art. 1 pkt 9 (art. 5a ust. 1, 2 i 8)	9) Art. 5a. 1. Podmiot kluczowy i podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej. 2. Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy

Strona **167** z **244**

Tabela zgodności do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustawy (UC32)

	elektronicznej uznaje się za podlegających jurysdykcji państwa członkowskiego, w którym świadczą usługi; b) dostawców usług DNS, rejestry nazw TLD, podmioty świadczące usługi rejestracji nazw domen, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, a także dostawców internetowych platform handlowych, wyszukiwarek internetowych lub platform usług sieci społecznościowych uznaje się za podlegających jurysdykcji państwa członkowskiego, w której mają główne miejsce prowadzenia działalności w Unii zgodnie z ust. 2; c) podmioty administracji publicznej uznaje się za podlegające jurysdykcji państwa członkowskiego, które je ustanowiło.			usługi na terytorium Rzeczypospolitej Polskiej. 8. Ustawę stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby.

Uzasadnienie na str. 40 również nieadekwatnie wskazuje: *art. 5a ust. 1 (zasada, że podmiot kluczowy/podmiot ważny podlega obowiązkom ustawy, jeśli ma na terenie RP jednostkę organizacyjną)*. Odniesienie na str. 18 wydaje się jedynie ogólnym sformułowaniem problematyki, a nie uzasadnieniem wprowadzenia takiej zmiany: *Podmioty świadczące usługi niezbędne dla funkcjonowania współczesnego społeczeństwa informacyjnego mają charakter transgraniczny. Należało więc przesądzić, zgodnie z dyrektywą NIS 2, jurysdykcję państwa nad podmiotami świadczącymi te usługi.*

Transgraniczne świadczenie usług nie zostało zdefiniowane ani nie wskazano innych aktów określających jego znaczenie.

Dotychczasowe brzmienie odpowiadało wprost dyrektywie NIS2. Przykładowo wskazujemy także na brzmienie przepisów przyjętych w Belgii oraz procedowanych we Francji. Nie zawierają one odniesień do działalności transgranicznej.

NIS2	uKSC	Belgia	Francja
Art. 26	Art. 5a.	Art. 4.	Art. 11
Podmioty objęte zakresem stosowania niniejszej dyrektywy uznaje się za podlegające jurysdykcji państwa członkowskiego, **w którym mają miejsce prowadzenia działalności**, z następującymi wyjątkami:	1. Podmiot kluczowy i podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli ~~posiada jednostkę organizacyjną~~ ma miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzi działalność na terytorium RP przez swoją siedzibę, oddział lub w ramach działalności transgranicznej.	1. This Law shall apply to the entities referred to in Article 3 which are **established in Belgium** and which provide their services or carry out their activities within the European Union.	I. – Essential entities and significant entities shall be governed by the provisions of this Title when, as the case may be: 1° They are **established on the national territory**;

W naszej ocenie zmiana może skutkować wątpliwościami co do uznawania za podlegające przepisom uKSC także podmiotów, które zostały ustanowione w innym kraju członkowskim i podlegają już tamtejszym przepisom. Rodzi to wątpliwości co do potencjalnego zaburzenia określonego w dyrektywie systemu klasyfikowania podmiotów do jurysdykcji konkretnych krajów.

Wnosimy o przywrócenie w tym zakresie dotychczasowego brzmienia projektu ustawy. Ewentualnie, należy doprecyzować przepisy oraz wyjaśnić ich intencje w uzasadnieniu.

6	**Art. 1 pkt 14**		Nowy Art. 8 ust. 1 pkt 2 a) ustawy o KSC stanowi rozszerzenie Art. 21 ust. 1 lit. a) Dyrektywy NIS 2, wprowadzając nowe pojęcie „polityk tematycznych". Jest to wprowadzenie dla podmiotów kluczowych i ważnych nowego obowiązku, nie przewidzianego w Dyrektywie NIS2. Jako że definicje ustawy o KSC nie zawierają definicji „polityk tematycznych", będzie to powodować praktyczne problemy dla przedsiębiorców związane z niepewnością, jakie to konkretnie „polityki tematyczne" mają wdrażać.
7	**Art. 1 pkt 15**		Nowy Art. 8 f ust. 2 ustawy o KSC wprowadza nieprzewidziany przez Dyrektywę NIS2 obowiązek przedkładania przez szereg osób zaświadczeń z KRK, co spowoduje dodatkowe nakłady czasowe oraz koszty (30 zł za zaświadczenie z KRS – kto miałby ponosić te koszty ?). Należy postulować np. złożenie stosownych oświadczeń, a możliwość wezwania do przedstawienia zaświadczenia o niekaralności pozostawić dla podmiotu w przypadku zaistnienia uzasadnionych podejrzeń co do karalności danej osoby.
8	**Art. 1 pkt 16**		Nowy Art. 9 ust. 1 pkt 1) ustawy o KSC wprowadza wymóg wyznaczania dwóch osób „odpowiedzialnych za utrzymywanie kontaktów (…)", co oznacza obowiązki podmiotów w zakresie ciągłej aktualizacji takich danych oraz obowiązki RODO. Należy postulować następujące brzmienie nowego Art. 9 ust. 1 pkt 1: "wskazuje adres email oraz numer telefonu do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa obsługiwane przez osoby odpowiedzialne za obsługę spraw z zakresu cyberbezpieczeństwa".
9	**Art. 1 pkt 16**		Nowy Art. 10 ust. 8 ustawy o KSC wprowadza wymóg każdorazowego sporządzania protokołu brakowania przy niszczeniu wycofanej z użytkowania dokumentacji, w którym zawarte będą m.in. oznaczenie niszczonej dokumentacji i dane osoby zatwierdzającej protokół. W przypadku dużych organizacji oznacza to wprowadzenie szeregu nowych, uciążliwych obowiązków, w tym m.in. odpowiedniego inwentaryzowania dokumentacji, konieczności sporządzania i przechowywania dodatkowych dokumentów itp. Należy postulować wykreślenie Art. 10 ust. 8.
10	**Art. 1 pkt 22**	Proponowane brzmienie Art. 16 pkt 1: „kluczowy i podmiot ważny realizuje	Nowy Art. 16 pkt 1 ustawy o KSC wprowadza zbyt krótki termin 6 miesięcy, zważywszy, że wiele podmiotów, które do tej pory nie były uznawane za kluczowe czy ważne, zostanie objęte zakresem przedmiotowym ustawy o KSC.

		obowiązki, o których mowa w niniejszym rozdziale, w terminie 18 miesięcy”.	Proponowane brzmienie Art. 16 pkt 1: „kluczowy i podmiot ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 18 miesięcy”. Należy zmienić dodatkowo zapis w ten sposób, aby owe 18 miesięcy liczyć nie od „dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny”, ale od „daty wpisu do wykazu”. W przeciwnym razie mogą powstać w wielu przypadkach niepotrzebne wątpliwości, do kiedy podmiot ma spełnić nowe wymagania prawne w zakresie cyberbezpieczeństwa oraz do kiedy musi zapewnić przeprowadzenie audytu. Dotychczasowe zapisy w tym zakresie były jasne, jako że biegły one od doręczenia decyzji – należy utrzymać ten stan pewności prawnej dla szeregu podmiotów.
11	**Art. 1 pkt 36**	Proponowane brzmienie: Art. 36 b.1 Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona na zlecenie organu właściwego do spraw cyberbezpieczeństwa, za uprzednią zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub w formie elektronicznej pod rygorem nieważności.	Nowy Art. 36 b ust. 1 ustawy o KSC wprowadza możliwość przeprowadzenia oceny bezpieczeństwa systemu Informacyjnego bez zgody podmiotu, który ma zostać oceniony. Należy postulować konieczność każdorazowego uzyskiwania zgody podmiotu, który ma podlegać ocenie.
12	**Art. 1 pkt 41**		Nowy Art. 41 ustawy o KSC wprowadza szereg organów kontrolno-nadzorczych właściwych do spraw cyberbezpieczeństwa w podziale na sektory. Podmioty prowadzące działalność w więcej niż 1 sektorze będą zatem podlegać kilku organom, co może prowadzić do wielu praktycznych komplikacji. Należy postulować docelowo, aby podmiot kluczowy lub ważny podlegał pod jeden organ kontrolno-nadzorczy.
13	**Art. 1 pkt 48 a)**		Nowy Art. 46 ust. 1 pkt 7 ustawy o KSC stanowi, że minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w tym przepisie. Wprowadza to niepewność

			dla IOD, czy będzie to powodować zmiany w dotychczas przyjętym sposobie zgłaszania naruszeń, w szczególności na przykład, czy zgłoszenie będzie musiało/mogło być dokonywane za pośrednictwem S46.
14	**Art. 1 pkt 48 e)**	Proponowane brzmienie: „Podmioty kluczowe i podmioty ważne obowiązane są zapewnić zgodność swoich systemów informatycznych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu teleinformatycznego w terminie 9 miesięcy od udostępnienia tych wymagań”.	Nowy Art. 46 ust. 6 ustawy o KSC stanowi, że podmioty kluczowe i ważne mają 6 miesięcy na zapewnienie zgodności, o której mowa w tym przepisie. Jest ryzyko, że – w zależności od wymagań – niektóre podmioty nie będą w stanie zapewnić tej zgodności, zwłaszcza w przypadku konieczności wprowadzania istotnych zmian w ich systemach informatycznych.
15	**Art. 1 pkt 59**	Proponowane brzmienie Art. 53 c ust. 1 pkt 5: „Wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do zakresu tego żądania, nie krótszego niż 21 dni;”	Nowy Art. 53 c ust. 1 pkt 5 ustawy o KSC wprowadza zbyt krótki termin 7 dni, co może prowadzić do znacznych niedogodności po stronie podmiotów, zwłaszcza w przypadku szerokiego zakresu żądanych danych, informacji czy dokumentów. Proponowane brzmienie Art. 53 c ust. 1 pkt 5: „Wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do zakresu tego żądania, nie krótszego niż 21 dni;”
16	**Art. 1 pkt 59**		Nowy Art. 53 d ust. 1 pkt 1 ustawy o KSC wprowadza niezwykle szerokie uprawienia urzędnika monitorującego, w tym prawo swobodnego dostępu za pomocą przepustki, wydanej bezzwłocznie, której wydania nie można odmówić”. Należy postulować doprecyzowanie przepisu, tak aby nie generował niepotrzebnych ryzyk dla podmiotu z powodu uznania, że przepustka nie została wydana

			„bezzwłocznie", podczas gdy ze względów organizacyjnych często nie będzie możliwe natychmiastowe wydanie takiej przepustki.
17	**Art. 1 pkt 61**		Nowy Art. 56 ust. 3 i 4 ustawy o KSC wprowadza konieczność zlecania tłumaczeń, m.in. niekiedy bardzo obszernej dokumentacji technicznej, co może generować istotne koszty dla podmiotów.
18	**Art. 1 pkt 71**		Nowy Art. 67 c. ust. 2 ustawy o KSC wprowadza konieczność wycofania przez podmioty kluczowe lub ważne produktów ICT, usług ICT i konkretnych procesów ITC najpóźniej w terminie 7 lat od uznania ich dostawcy za dostawcę wysokiego ryzyka. W przypadku dużych przedsiębiorstw, w tym np. z tak krytycznego sektora jak energetyka, może oznaczać to konieczność istotnych zmian, poniesienia ogromnych kosztów i może okazać się niemożliwe do przeprowadzenia w ciągu 7 lat. Należy postulować wydłużenie terminu do 10 lat lub przynajmniej wprowadzenie możliwości przedłużenia tego terminu na wniosek podmiotu.
19	**Art. 1 pkt 71**	Proponowane brzmienie nowego Art. 67 g ust. 12: „ Polecenie zabezpieczające wydaje się na czas koordynacji incydentu krytycznego lub na czas oznaczony, nie dłuższy niż 6 miesięcy".	Nowy Art. 67 g. ust. 12 – zbyt długi termin 2 lat.
20	**Art. 1 pkt 77**		Nowe brzmienie art. 73 ust. 1 i nast. ustawy o KSC oznacza możliwość nałożenia na wiele podmiotów kar do 10.000.000,00 EUR za bardzo wiele naruszeń, sformułowanych bardzo ogólnie.
21	**Art. 1 pkt 78**		Zgodnie z nowym ust. 1 i nast. karze pieniężnej może podlegać kierownik podmiotu (por. uwagi wyżej co do pojęcia kierownika), nawet za zaniechanie jednorazowe (ust. 2) – do 300% wynagrodzenia (ust. 4).

22	**Art. 1 pkt 81**		Zgodnie z nowym Art. 76 b. ust. 1 ustawy o KSC kara w wysokości 100 000 zł za dzień opóźnienia została ustanowiona na zbyt wysokim pułapie.
23	**Art. 17**	W praktyce wnosimy o nadanie zmianie w art. 17 projektu uKSC następującego brzmienia: ***Art. 14.*** *W ustawie z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221) w art. 40 w ust. 1 w pkt 2 uchyla się lit. b i c.*	W art. 14 wprowadzana jest – wydawałoby się techniczna jedynie - zmiana art. 40 w ust. 1 pkt 2 lit. b ustawy PKE poprzez zastąpienie zwrotu „operatorów usług" zwrotem „podmiotów". Uzasadnienie i OSR nie odnoszą się do tej zmiany. Jedynie w odwróconej tabeli zgodności wskazano, że *„Zmiana ta dostosuje te przepisy do nowej siatki pojęciowej zawartej w ustawie o krajowym systemie cyberbezpieczeństwa.*" Jest to sformułowanie nieprawdziwe. Faktycznym dostosowaniem byłoby wskazanie na podmioty kluczowe, a nie wszystkich podmiotów Podkreślamy, że zmiana niesie za sobą bardzo poważne skutki praktyczne. Należy wskazać, że art. 40 PKE dotyczy możliwości nałożenia przez Prezesa UKE, w sytuacji szczególnego zagrożenia, na przedsiębiorcę telekomunikacyjnego obowiązku *odtwarzania dostarczania publicznych sieci telekomunikacyjnych lub przywrócenia świadczenia publicznie dostępnych usług telekomunikacyjnych, z uwzględnieniem pierwszeństwa dla* m.in. dla *operatorów usług kluczowych, o których mowa w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*. Różnica polega na ogromnej zmianie zakresu podmiotów na rzecz, których taka decyzja mogłaby zostać wydana. Aktualnie operatorów usług kluczowych jest 378. Według OSR nowelizacji uKSC podmiotów będzie niecałe 40 tysięcy. Oznacza to, że zakres potencjalnego obowiązku rośnie ponad 100-krotnie. Nie dokonano w tym zakresie żadnej analizy w Ocenie Skutków Regulacji. Zwraca także uwagę, że podmiotami KSC będą także przedsiębiorcy telekomunikacyjni co mogłoby oznaczać możliwość nakładania obowiązku odtwarzania przez jednego operatora na rzecz innego operatora. Ponadto dotyczy to także odtwarzania na rzecz szeregu organów występujących w KSC będących jego podmiotami, np. organów centralnych. Dotyczy to także wszystkich samorządów i ich jednostek. Zmiana ta nie wynika z dyrektywy NIS2. Taka zmiana jest skrajnie nieproporcjonalna i nadmiernie ingeruje także w swobodę działalności gospodarczej. To przedmiotem umów między określonymi podmiotami a operatorami

			telekomunikacyjnymi powinno być określania warunków świadczenia usługi, SLA, w tym okresów przywracania. Kwestie te są ściśle związane również z wyceną kosztu świadczenia usługi. Podkreślamy także, że już obecna regulacja jest nadmiarowa i była negatywnie opiniowana w toku prac legislacyjnych dot. PKE. Podobne uwagi dotyczą wprowadzonego już wskazania na pierwszeństwo dla operatorów infrastruktury krytycznej, których liczba zapewne poważnie wzrośnie po rozpoczęciu stosowania wdrożenia dyrektywy CER. Wnosimy o przywrócenie brzmienia Prawa telekomunikacyjnego, które w zrozumiały dla nas i proporcjonalny sposób odnosiło się do potencjalnego wydania decyzji UKE na rzecz pierwszeństwa dla podmiotów i służb, o których byłą mowa w art. 178 ust. 2 pkt 1 PT czyli: *koordynujących działania ratownicze, podmiotów właściwych w sprawach zarządzania kryzysowego, służb ustawowo powołanych do niesienia pomocy, a także innych podmiotów realizujących zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.* Zakres ten jest już ujęty w art. 40 ust. 1 pkt 2 lit. a.

KL/80/25/AM/2025