LEWIATAN

Warszawa, 24 maja 2023 r.
KL/203/88/AM/2023

Pan
Janusz Cieszyński
Pełnomocnik Rządu ds. Cyberbezpieczeństwa
Minister Cyfryzacji

Szanowny Panie Ministrze,

W związku z publikacją najnowszej wersji *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, datowanej na 5 maja 2023 r., Konfederacja Lewiatan przedstawia w załączeniu stanowisko do projektu ustawy.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Łukasz Schreiber – Przewodniczący Stałego Komitetu Rady Ministrów, Sekretarz Rady Ministrów

Załącznik: Stanowisko Konfederacji Lewiatan do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, datowanej na 5 maja 2023 r.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

LEWIATAN

Stanowisko Konfederacji Lewiatan do *projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, datowanej na 5 maja 2023 r.

W związku z publikacją kolejnej wersji projektu ustawy o zmianie ustawy *o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw*, datowanej na 5 maja 2023 r. przedstawiamy poniższe stanowisko.

Odnotowujemy, że w projekcie wprowadzono pewne zmiany, które zasługują na szczególne poparcie. Dotyczy to przede wszystkim urealnienia terminu wejścia w życie ustawy, tj. przyjęcia 6-miesięcznego *vacatio legis*, a także dokonano niezbędnego dostosowania terminologii do projektu uPKE. Za właściwe uznajemy też wynikający z materiałów publikowanych na etapie SKRM kierunek dot. skoordynowania prac legislacyjnych nowelizacji uKSC oraz uPKE.

Jednocześnie, pozostają w projekcie istotne kwestie kluczowe, do których odnosiliśmy się także na poprzednich etapach. Mimo formułowanych w tym zakresie wniosków, nie zostało przedstawione odniesienie projektodawcy do formułowanych uwag.

W niniejszym stanowisku **przedstawiamy nasze kluczowe na tym etapie postulaty**. Wnioskujemy o ich uwzględnienie w toku dalszych prac legislacyjnych.

I. UWAGI MERYTORYCZNE

1. **Uruchomienia wymagają prace nad założeniami ustawy implementującej dyrektywy NIS2** (ws. środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148) **i CER** (dyrektywa ws. odporności podmiotów krytycznych)**, których termin implementacji upłynie 17.10.2024, a stosowanie ma rozpocząć się już 18.10.2024** – nie tylko w kontekście regulacji sektora komunikacji elektronicznej, ale także w kontekście projektu ustawy *o ochronie ludności oraz o stanie klęski żywiołowej*, który mając uchylić ustawę o zarządzaniu kryzysowym wprost dotyczy zakresu dyrektywy CER, a z uwagi na komplementarność NIS2 i CER powinien być elementem szerszej koncepcji wdrożenia przepisów.

   Analiza obu tych dyrektyw wskazuje jasno, że **ich wdrożenie będzie wiązało się z koniecznością dokonania głębokich i ściśle skoordynowanych zmian zarówno w uKSC, jak i ustawie o zarządzaniu kryzysowym**. Modyfikowane będą podstawowe instytucje prawne, rozszerzana lista podmiotów objętych regulacjami, a także wzmacniane uprawnienia organów. Spodziewamy się, że ta implementacja będzie ogromnym wyzwaniem na poziomie legislacyjnym i organizacyjnym dla samych organów administracji, a także dla podmiotów których rola się zmieni lub które po raz pierwszy wejdą w reżim wymagań cyberbezpieczeństwa lub infrastruktury krytycznej.

   W praktyce, **prace legislacyjne nad nowymi przepisami powinny zaczynać się już teraz**. Inaczej, albo terminy konsultacji i niezbędnego dialogu będą skracane, albo termin wdrożenia nie zostanie dochowany.

   W tych uwarunkowaniach uważamy, że **dokonywanie jakichkolwiek systemowych modyfikacji w krajowym systemie cyberbezpieczeństwa oraz w zarządzaniu kryzysowym jest głęboko**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

nieuzasadnione i naraża adresatów przepisów, zarówno po stronie administracji publicznej, jak i po stronie sektora prywatnego na ponoszenie nieuzasadnionych kosztów związanych z dokonywaniem zmian organizacyjnych oraz zakupów i zamówień. Należy przy tym pamiętać, że takimi pracami będą musiały się zajmować te same osoby, które normalnie przypisane są do realizacji konkretnych działań związanych z wykrywaniem i reagowaniem na zagrożenia i incydenty. Okres wdrożeniowy może być więc niepotrzebnie okresem zwiększonej wrażliwości.

Jeśli faktycznym celem jest zapewnienie najwyższego poziomu cyberbezpieczeństwa krajowych instytucji i przedsiębiorstw cały wysiłek należy alokować w **jak najszybsze wdrożenie zmian, które będą nie tylko skuteczne, ale też trwałe w szerokim horyzoncie czasowym. Za takie działanie rozumiemy przystąpienie do wdrożenia nowych przepisów unijnych** zamiast wprowadzania zmian cząstkowych. One bowiem mogły mieć swoją rolę w okresie ich pierwszej publikacji tj. w 2020 roku, a nie teraz, w połowie 2023. W obliczu faktycznego, wysokiego poziomu bezpieczeństwa sieci telekomunikacyjnych, również w obliczu wyzwań pandemii SARS-COV2 i zbrojnej agresji za wschodnią granicą, trudno nam uznać te okoliczności za wystarczające uzasadnienie dla wprowadzanych zmian.

Warto także w tym zakresie zwrócić uwagę na niezgodność z NIS2 w zakresie tych rozwiązań projektu, które nakładają obowiązki na przedsiębiorców telekomunikacyjnych, z tej przyczyny, że projekt ustawy zmierza do wdrożenia art. 40 i 41 EKŁE, które to przepisy są uchylane mocą NIS2. Polska, jako państwo członkowskie UE, powinna powstrzymać się od przyjmowania jakichkolwiek przepisów, które mogłyby poważnie zagrozić osiągnięciu rezultatu przewidzianego w dyrektywie NIS2 z uwagi na obowiązek lojalności wobec prawa europejskiego, wynikający z orzecznictwa TSUE[1].

2. **Włączenie przedsiębiorców komunikacji elektronicznej do uKSC powinno więc zostać zaniechane**, ponieważ w świetle spodziewanych zmian wynikających z implementacji NIS2 i CER oraz czasowej koincydencji regulacja ta będzie zdecydowanie spóźniona, nadmiarowa oraz będzie skutkować duplikacją wdrażania nowych lub zmodyfikowanych obowiązków. Mimo pewnego poziomu harmonizacji z NIS2 zawartego już w uKSC zauważyć trzeba, że realna materia NIS2 może wynikać z szeregu aktów wykonawczych, których jeszcze nie znamy. Tym samym szczegółowe rozwiązania krajowe będą zapewne przynajmniej częściowo niespójne. W praktyce oznacza to, że kolejne 2-3 lata będą okresem stałej i zbędnej zmiany w strukturach bezpieczeństwa operatorów telekomunikacyjnych – co będzie w efekcie niekorzystne dla faktycznego poziomu bezpieczeństwa sieci i usług, także po stronie użytkowników.

   Przepisy dot. cyberbezpieczeństwa niezbędne do implementacji EKŁE (bazujące na PT) powinny zostać wprowadzone do projektu PKE, w sposób umożliwiający realizację obowiązków przez przedsiębiorców telekomunikacyjnych w sposób dotychczasowy. Projekt PKE jaki zostanie ponownie przedłożony do Sejmu powinien już uwzględniać takie zmiany.

3. **Projekt budzi istotne wątpliwości co do zgodności z prawem UE.** W tym zakresie dokumentacja przekazana przez wnioskodawcę do Rządowego Centrum Legislacji z wnioskiem o przeprowadzenie komisji prawniczej dla projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (dalej:

[1] Wyrok z 18.12.1997 sprawa C-129/96 *Inter-Environnement Wallonie*.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

„projekt") nie zawiera opinii ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej (dalej: „MdsUE") o zgodności projektu z prawem Unii Europejskiej wymaganej zgodnie z uchwałą nr 190 Rady Ministrów z dnia 29 października 2013 r. Regulamin pracy Rady Ministrów dalej (Dz. U. z 2022 r. poz. 348) dalej, „RpRM (§ 72 ust. 2 pkt 2 RPRM). Opinia ta była przedstawiana na wcześniejszych etapach RPL, a biorąc pod uwagę, że projekt przedstawiony na komisję prawniczą różni się od ostatniej wersji rozpatrywanej przez Stały Komitet Rady Ministrów (dalej: „SKRM"), niezbędna jest aktualna opinia. Jest to tym bardziej konieczne, że projekt został uznany za akt wykonujący prawo unijne, co znajduje odzwierciedlenie w treści odnośnika umieszczonego w tytule projektu i to zarówno w zakresie częściowego wdrażania dyrektywy Parlamentu Europejskiego i Rady jak i stosowania rozporządzenia Parlamentu Europejskiego i Rady Przedstawienie aktualnej opinii o zgodności z prawem UE jest zasadne tym bardziej, że w toku procesu legislacyjnego MdsUE zgłaszał szereg uwag i dotychczas nie zostały one w pełni uwzględnione (w zakresie operatora strategicznej sieci bezpieczeństwa), a także niezgodności wykluczeń stosowania ustawy Prawo zamówień publicznych zawartych w projekcie. W tym kontekście podkreślić także trzeba, że projekt procedowany jest w okresie obowiązku wdrażania dyrektywy 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 objęty jest procedurą notyfikowania przepisów technicznych w Komisji Europejskiej.

4. **W przypadku utrzymania regulacji przedsiębiorców komunikacji elektronicznej w projekcie nowelizacji uKSC:**
    a. **W miejsce zupełnie nierealistycznego terminu zgłaszania poważnych incydentów telekomunikacyjnych w 8 godzin, należy wprowadzić procedurę wg NIS2 tj. 24h na wstępne ostrzeżenie, 72h na zgłoszenie poważnego incydentu telekomunikacyjnego oraz miesiąc na pełny raport.**
    b. Wymagane **szacowanie ryzyka powinno odbywać się nie częściej niż co 2 lata, a nie corocznie.**
5. **Niezbędne jest wprowadzenie obowiązkowych przeglądów decyzji uznających dostawcę za dostawcę wysokiego ryzyka**. Jest to proporcjonalny środek zapewniający ograniczenie skutków wydanych decyzji, także w przypadku zmiany okoliczności. Wg zał. nr 1 do OSR w Słowenii taki przegląd miałby być realizowany co 2 lata, a w Wielkiej Brytanii „co jakiś czas".
6. **Przygotowania wymaga strategia działania organów Państwa w zakresie skutecznego nadzoru rynków objętych decyzjami wykluczającymi zasoby „dostawców wysokiego ryzyka" oraz wprowadzania środków zaradczych**. Ewentualne decyzje muszą poprzedzać dogłębne analizy ich skutków rynkowych, a także pod względem bezpieczeństwa i ciągłości świadczenia usług w sektorze z którego dane zasoby mają zostać usunięte.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

W dotychczas sygnalizowanych przez nas obszarach, tj. sektorze telekomunikacyjnym oraz farmaceutycznym istnieje poważne ryzyko faktycznego zlikwidowania konkurencji rynkowej lub w ogóle ograniczenia dostępności niezbędnych towarów. Ryzyko administracyjnego wykreowania monopolu lub duopolu w krytycznych dla ciągłości działania Państwa sektorach wymaga poważnej analizy i przedstawienia strategii działania, w tym ew. narzędzi władczych chroniących nabywców na rynkach dotkniętych wykluczeniem dostawcy, a ostatecznie także odbiorców ich usług. Potrzebne są do tego także odpowiednie analizy istniejących zasobów, rynku dostawców i proporcjonalna ocena wpływu wydania decyzji „ważąca" ryzyka dot. bezpieczeństwa oraz ryzyka „rynkowe". Powinny być one przeprowadzone przed wydaniem ewentualnej decyzji. Ich brak może bowiem doprowadzić do ograniczenia możliwości świadczenia usług lub realizacji dostaw istotnych dla funkcjonowania państwa i społeczeństwa zasobów – szczególnie gdyby wykluczenie zasobów danego dostawcy spowodowało, że danych zasobów nie da się zastąpić innymi, także uwzględniając uwarunkowania ekonomiczne. Szczególnie istotne jest przy tym zwiększone ryzyko stosowania praktyk niekorzystnych dla odbiorców, w tym monopolistycznych przez pozostałych dostawców, których warunki działania uległy poprawie. Jest to również szczególnie istotne w świetle otwartego katalogu urządzeń objętych decyzją ministra (w pkt 3 załącznika nr 3 związanego z zarządzaniem łącznością z urządzeniami użytkowników mowa o „innych funkcjach" oprócz 5G Radio Base Station Baseband Unit, co powoduje, że w pkt 3 mieszczą się wszystkie urządzenia zarządzające łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych, a nie tylko związane z RAN).

W OSR i uzasadnieniu powinny zostać przedstawione przynajmniej założenia takich działań oparte o analizy rynków dla których w szczególności identyfikowana jest potrzeba przeprowadzenia postępowania dotyczącego uznania dostawcy za dostawcę wysokiego ryzyka. Materiały te powinny zostać przygotowane w oparciu o analizy rynkowe Prezesa UOKiK, a także regulatorów sektorowych jak Prezes UKE, URE, UTK czy Głównego Inspektoratu Farmaceutycznego.

W szczególności należy zapewnić, że organy państwa wprowadzając administracyjny obowiązek wycofania dotychczasowego uczestnika rynku będą jednocześnie gotowe do wdrożenia środków zabezpieczających przed powstaniem w danym sektorze poważnych skutków negatywnych, które są typowe dla warunków obniżonej konkurencji, tj. wzrostu cen, ograniczenia dostępności, spadku jakości oraz wydłużenia terminów realizacji dostaw i usług. Rozwiązania takie powinny mieć w szczególności charakter ex-ante i zaczynać obowiązywać od momentu wydania decyzji wykluczającej zasoby określonego podmiotu z rynku. Projekt ustawy nie przewiduje również rozwiązania w przypadku, gdy ocena określająca wysokie ryzyko obejmie specyficzne urządzenia czy oprogramowanie, które jest unikatowe, a na rynku brak jest alternatywnych rozwiązań technicznych umożliwiających jego zastąpienie.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

W innym przypadku już teraz można prognozować, że wdrażanie nowoczesnych rozwiązań, w tym sieci 5G, będzie doznawało dalszych opóźnień, a może być również droższe i niższej jakości (co zaobserwowano w USA[2]). Nieznany jest dzisiaj wpływ takiej sytuacji na możliwe tempo rozwoju sieci, w tym wynikającego z projektowanej dokumentacji aukcyjnej dla pasma C celu ogólnopolskiego pokrycia kraju siecią 5G – i to niezależnie od tego czy dany operator korzystałby z rozwiązań „dostawcy wysokiego ryzyka". Tylko silna rola organów państwa, odpowiedzialnych przecież również za zmianę warunków na rynku dostawców, będzie mogła chronić ich klientów przed poważnym zniekształceniem warunków kontraktowania. Należy więc już teraz rozważyć wprowadzenie odpowiednich narzędzi wobec pozostałych na rynku dostawców w omawianym projekcie ustawy, których skutkiem będzie utrzymanie dotychczasowych warunków ekonomicznych, technicznych i organizacyjnych dostarczania zasobów niezbędnych do utrzymania ciągłości oraz bezpieczeństwa usług.

Warto mieć na uwadze, że obecna procedura uznania dostawcy wysokiego ryzyka może uznana zostać za dyskryminującą, a w konsekwencji naruszać TFUE (zasada niedyskryminacji – art. 18 TFUE, zasady swobodnego przepływu towarów i usług – art. 34 i 35 TFUE, zakaz nadużywania pozycji dominującej art. 102 TFUE), Karty Praw podstawowych (art. 20 i 21 ust. 2 Karty praw podstawowych), a także innych zobowiązań międzynarodowych Rzeczpospolitej Polskiej. Nie sposób również pominąć, Ograniczenie swobody przepływu towarów i zgodności z przepisami UE - projekt wprowadza postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, w ramach którego przewiduje się mechanizm powiadamiania o wszczęciu postępowania na stronie BIP oraz dopuszczeniem do postępowania jedynie największych przedsiębiorców telekomunikacyjnych. Jak zwrócił uwagę Minister ds. Unii Europejskiej – w opinii nr DPUE.920.1030.2021.AR(27) - komunikowanie (publiczne z art. 66a ust. 8), jak i ograniczone (do największych nabywców produktów ICT z art. 66a ust. 5), może stanowić środek o skutku równoważnym do ograniczeń ilościowych w przywozie i wywozie, o których mowa w art. 34 i 35 TFUE.

7. **Poważne wątpliwości budzi również odwoływanie się do norm technicznych (standardów) jako obowiązującego aktu prawa**, tj. choć załącznik nr 3 stanowi niewątpliwie część ustawy, to odwołanie się do funkcji 3GPP powoduje, że normy lub standardy tej organizacji stają się źródłem obowiązującego prawa w Polsce. Innymi słowy, 3GPP poprzez zmianę (np. aktualizację) standardu wpływać będzie na prawa i obowiązku adresatów załącznika nr 3 w Polsce, a tym samym moc prawna zostanie zrównana z ustawą.

8. **Projekt ustawy wprowadza postępowanie dla dostawców sprzętu lub oprogramowania, które mogą zostać uznane za dostawców wysokiego ryzyka (DWR), ale procedura ta dostępna jest tylko dla największych przedsiębiorców telekomunikacyjnych.** Taka selekcja narusza zasadę równości zawartą w art. 32 Konstytucji, wprowadzając dyskryminujące kryterium ekonomiczne. Kolejnym problemem jest czas realizacji wymogu wycofania sprzętu lub oprogramowania

[2] Have the Huawei Bans Achieved the US' Intended Goals? (internationalbanker.com)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

uznanych za wysokiego ryzyka, ustalony na 5-7 lat. Projekt nie przewiduje rekompensat dla operatorów, co budzi wątpliwości konstytucyjne. Brakuje również analizy dotyczącej żywotności różnych typów sprzętu czy oprogramowania, co sugeruje, że rozwiązanie zostało wprowadzone bez szerszej i pogłębionej analizy. Dostawcy objęci procedurą DWR, nie otrzymują treści całego wyroku w sprawie odwołania od Decyzji DWR, co więcej także elementy uzasadnienia Decyzji DWR mogą być niejawne (nawet jeśli byłyby reprezentowane przez osoby, posiadające dostęp do informacji objętych klauzulami tajności). Brak również dwuinstancyjności, tj. od decyzji DWR można odwołać się do sądu. **W konsekwencji, kwestionowana jest zgodność projektu z zasadą równości oraz adekwatności zastosowanych środków do celu, jakim jest zapewnienie cyberbezpieczeństwa.**

9. **W ramach procedury wydawania poleceń zabezpieczających niezbędne jest wprowadzenie mechanizmu weryfikacji możliwości jego wdrożenia** przez adresatów, w tym potencjalnie negatywnych skutków jego wdrożenia na ciągłość świadczenia usług oraz ich użytkowników. Co więcej polecenia zabezpieczające są natychmiast wykonalne, podczas gdy przecież taka decyzja może zostać opatrzona w rygor natychmiastowej wykonalności na podstawie art. 108 § 1 kpa.

10. **Wyrażamy poparcie dla precyzyjnych i poważnych zastrzeżeń wyrażanych przez Ministra ds. Unii Europejskiej** poddających w wątpliwość zgodność z prawem europejskim założeń dla powołania i świadczenia usług przez Operatora Strategicznej Sieci Bezpieczeństwa, wyłączenia ze stosowania ustawy PZP, a także wątpliwości w zakresie legalności planowanej do udzielenia na rzecz tego Operatora pomocy publicznej. Nie ulega wątpliwości, iż OSSB będzie prowadził działalność komercyjną, gdyż za świadczone usługi będzie naliczał i pobierał stosowne opłaty. Przepis art. 76g ust. 2 wyraźnie wskazuje, iż *„Cena za usługi świadczone przez Operatora strategicznej sieci bezpieczeństwa uwzględnia koszt usługi powiększony o rozsądną marżę przy uwzględnieniu, że w koszt usługi nie wlicza się usług lub sprzętu sfinansowanych z dotacji, o której mowa w art. 76u ust. 1.*" a więc działalność OSSB będzie działalnością komercyjną jednocześnie stanowiącą działalność konkurencyjną wobec działalności pozostałych przedsiębiorców, którzy aktualnie świadczą usługi telekomunikacyjne na rzecz podmiotów wymienionych w art. 76f projektu UKSC. OSSB zgodnie z projektem zostanie wskazany w drodze zarządzenia Prezesa Rady Ministrów, choć zgodnie z dyrektywą 2002/77/WE usługi lub sieci łączności elektronicznej powinny być udostępniane na podstawie ogólnego zezwolenia, a nie na podstawie licencji. Art. 12 ust. 1 i 2 dyrektywy 2018/1972 zakazują ponadto utrudniania przedsiębiorstwu dostarczania sieci łączności elektronicznej lub świadczenia usług łączności elektronicznej. Odstępstwo od wskazanych zasad jest dopuszczalne zgodnie z art. 52 ust. 1 TFUE w przypadkach uzasadnionych względami ochrony publicznego porządku, zdrowia lub bezpieczeństwa. Natomiast zgodnie z art. 2 ust. 4 dyrektywy 2002/77/WE i uwzględniając motyw 9 tej dyrektywy, warunki związane z ogólnym zezwoleniem udzielonym przedsiębiorstwu na świadczenie usług łączności elektronicznej lub utworzeniem lub zapewnieniem sieci łączności elektronicznej muszą opierać się na obiektywnych, niedyskryminacyjnych, proporcjonalnych i przejrzystych kryteriach.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

11. **Stanowczo protestujemy przeciwko stanowisku przedstawionemu w zestawieniu uwag z dnia 25 kwietnia 2023 r. w którym wskazano, że: *Obecnie organy administracji korzystają, przy realizacji zadań z zakresu obronności czy bezpieczeństwa państwa z usług operatorów znajdujących się, ze względu na strukturę, pod wpływem podmiotów trzecich**. Sytuacja ta może zagrażać bezpieczeństwu przekazywanych informacji a co za tym idzie **zagraża bezpieczeństwu państwa.***

    Wnioskiem z tego sformułowania jest, że sam fakt świadczenia usług przez operatora, który posiada kapitał spoza Polski, nawet jeśli jest to kapitał z kraju UE, NATO czy stowarzyszonego oznacza zagrożenie bezpieczeństwa Polski. Teza ta jest głęboko krzywdząca dla istotnej części z uczestników rynku telekomunikacyjnego, a zapewne jest też co najmniej niepokojąca z perspektywy oceny klimatu dla inwestycji zagranicznych w Polsce.

    Jest również z wielu powodów nieprawdziwa, w tym pomija fakt, że część usług jest świadczona przez operatorów o kapitale wyłącznie krajowym. Całkowicie pominięto również fakt, że to organy publiczne konstruują wymagania wobec jakości i bezpieczeństwa świadczonych dla nich usług. Brak jest także jakichkolwiek danych o incydentach, które potwierdzałyby tak daleko idący zarzut.

    Bezwzględnego wyjaśnienia wymaga jednocześnie, co oznacza w tym sformułowaniu „znajdowanie się pod wpływem podmiotu trzeciego" oraz jaki ma to faktyczny wpływ na bezpieczeństwo Polski, w aktualnej sytuacji sojuszniczej i geopolitycznej.

    Dodatkowo KL podkreśla potrzebę stworzenia możliwości zawierania umów z SOCami poza granicami RP działającymi w ramach jednej grupy finansowej (właścicielskiej). W zakresie dużych grup finansowych operujących na całym świecie w ramach sektora usług finansowych jest to element mitygacji ryzyka.

Poniżej przedstawiamy uszczegółowione odniesienie do części z wyżej sygnalizowanych uwag:

1. **Zbyt krótki czas i zbyt szeroki zakres zgłoszeń poważnych incydentów telekomunikacyjnych**

Poważną zmianą dotyczącą przedsiębiorców komunikacji elektronicznej jest **radykalne skrócenie terminu na przygotowanie raportu o zaistnieniu i wykryciu poważnego incydentu telekomunikacyjnego, a także** rozszerzenie kryteriów klasyfikacji incydentów jako poważnych, zarówno na poziomie projektu ustawy, jak i w projekcie nowego rozporządzenia do art. 20d uKSC.

Na wstępie sygnalizujemy, że **mamy pełną świadomość, że art. 5 NIS2 wskazuje, że jest to dyrektywa harmonizacji minimalnej**, tj. nie uniemożliwia krajom wdrożenia środków dalej idących. Nie twierdzimy więc, że projektowane przepisy są w zakresie terminów raportowania podmiotów telekomunikacyjnych niezgodne z NIS2. Są natomiast wybiórcze,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

gdyż „implementacja” dotyczy tylko sektora komunikacji elektronicznej, a nie wszystkich sektorów objętych NIS2. Prowadzony proces legislacyjny jest również wątpliwy pod kątem możliwości uznania go za faktyczną, częściową implementację NIS2, gdyż dotychczas nie były spełniane żadne z wymagań obowiązujących dla projektów implementujących prawo unijne (tabele, odpowiednie odnośniki w tytule, rt..), co było też konsekwencją równoległego prowadzenia krajowej i unijnej procedury legislacyjnej.

Pomijając jednak kwestie formalne, **nie znajdujemy uzasadnienia dla wprowadzenia tak zdecydowanego rozróżnienia wobec regulacji unijnych oraz wybiórczej jedynie implementacji**. Znajdowałoby to swoje uzasadnienie jedynie w przypadku zdarzeń o charakterze krytycznym i zagrażających ciągłości funkcjonowania w wielkich rozmiarach.

W naszej ocenie **proponowane środki są zdecydowanie zbyt restrykcyjne**. Skutkiem ich wprowadzenia nie będzie zwiększenie odporności podmiotów krajowego systemu cyberbezpieczeństwa, ale przede wszystkim obniżenie jakości zgłoszeń oraz wzrost ich ilości.

W proponowanych przepisach, nowy zakres zgłoszeń będzie obejmować także **raportowanie zdarzeń niemających istotnego wpływu na bezpieczeństwo sieci, usług czy użytkowników**. Tym bardziej z perspektywy ich cyberbezpieczeństwa, gdyż zdecydowana większość zdarzeń dotyczących sieci i usług telekomunikacyjnych dotyczy awarii fizycznych, zdarzeń losowych lub pogodowych. Wzrost liczby zgłoszeń aktualnych naruszeń, jako poważnych incydentów telekomunikacyjnych będzie nieproporcjonalny do faktycznego poziomu bezpieczeństwa i wpływu na działanie sieci.

W efekcie skrócenia czasu na raportowanie oraz zwiększenia jego zakresu nastąpi **niepotrzebny w naszej ocenie wzrost obciążenia sprawozdawczego zespołów operatorów oraz ich odbiorców tj. CSIRT-ów**. Innymi słowy, z uwagi na ryzyko kary administracyjnej, zasoby operatorów będą zajmowały się sprawozdawczością, w czasie kiedy priorytetem powinna być obsługa incydentu. Tym samym, podkreślamy, że realny jest istotny, negatywny wpływ zwiększenia wymagań dot. raportowania na: czas identyfikacji i diagnozy awarii, czas jej usuwania, obsługę klientów.

W związku z tym zgłaszamy następujące propozycje:

1) **Termin zgłoszenia oraz procedura powinny zostać dostosowane do NIS2**

Stan aktualny wg PT	**Projekt noweli uKSC**	**Postulowana zmiana noweli uKSC**
Aktualnie (art. 175a PT) naruszenia zgłaszane są niezwłocznie. W praktyce termin ten uznaje się za spełniony jeśli	Projektowane (art. 20d ust. 1 pkt 2) jest radykalne skrócenie tego terminu: do 8 godzin od momentu wykrycia.	Zmiana postulowana: **1.** Wprowadzenie procedury zgłoszeniowej według NIS2 tj. jasne wskazanie w przepisach terminów i gradacji zgłoszenia:

zgłoszenie nastąpi w okresie 4-5 dni roboczych.		○ 24 godziny od powzięcia wiedzy o poważnym incydencie telekomunikacyjnym na przekazanie wczesnego ostrzeżenia; ○ 72 godziny od powzięcia wiedzy o poważnym incydencie telekomunikacyjnym na zgłoszenie incydentu ○ nie później niż miesiąc na sprawozdanie końcowe. **2.** Przywrócenie pierwotnie projektowanego terminu zgłoszenia w 24 godziny od wykrycia incydentu poważnego, co będzie zgodne z czasami zgłoszeń incydentów dla wszystkich innych podmiotów KSC (usługi, kluczowe, cyfrowe, podmioty publiczne).

Ponadto, w naszej ocenie:

- **Brak jest konieczności istotnego skracania terminów z uwagi na fakt, że CISRT-y będą miały dostęp do rejestrowanych incydentów (art. 20c pkt 3 noweli uKSC).**

Art. 20 pkt wskazuje, że: *Przedsiębiorca komunikacji elektronicznej* ***zapewnia dostęp do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych*** *właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań*. Dodatkowo zgodnie z art. 20c pkt 2 może też zgłaszać *informacje o cyberzagrożeniach, podatnościach i incydentach*.

Należy więc przyjąć, że **CSIRT-y będą miały dostęp do informacji o właściwych dla nich incydentach telekomunikacyjnych**. Będą też mogły prowadzić w ich zakresie adekwatną analitykę czy podejmować inne działania znajdują się w ich zakresie kompetencji.

Zgłoszenie incydentu poważnego powinno w tej sytuacji dotyczyć incydentów, które mogły zostać przez operatora właściwie przeanalizowane i zaklasyfikowane, w sposób uzasadniający wysłanie możliwie kompletnego zgłoszenia.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- **Zbyt krótki czas na rzetelne przygotowanie spowoduje zbędne obciążanie zespołów zgłoszeniami niepełnymi lub nieprawidłowymi**

Aktualnie, w zależności od rodzaju naruszenia/incydentu, zespoły dokonujące klasyfikacji oraz wypełnienia formularza sprawozdawczego składają się z kilku do kilkunastu osób z różnych obszarów organizacji i pracujących na różnych stanowiskach. Jedynie część z nich, w szczególności odpowiedzialna za monitorowanie sieci i reakcję na incydenty pracuje w trybie ciągłym lub dyżurowym. Pozostałe funkcje, nie są i z punktu widzenia bezpieczeństwa, nie muszą być realizowane w trybie 24/7. Brak jest więc funkcjonalnego i ekonomicznego uzasadnienia dla takiego sposobu działania, a może on zostać wymuszony projektowanymi przepisami. Ograniczona jest również dostępność podmiotów zewnętrznych, w tym dostawców urządzeń lub oprogramowania, których informacje są niezbędne do ustalenia okoliczności zdarzenia, a także przygotowania raportu. Nie dotyczy to oczywiście zdarzeń o charakterze faktycznie krytycznym, kiedy stosowane są niestandardowe procedury. Kryteria określone w projektowanym rozporządzeniu trudno jednocześnie uznać za faktycznie krytyczne.

Powoduje to, że tryb 8 godzinny, obowiązujący każdego dnia roku, w tym w weekendy i święta, będzie dla części przypadków niemożliwy do dotrzymania w sposób dający rękojmię przekazywania w zgłoszeniu informacji pełnych lub nawet prawdziwych.

Takie zgłoszenia będą musiały być uzupełniane lub nawet korygowane co będzie dodatkowo angażować zespoły zarówno podmiotu raportującego, jak i przyjmującego zgłoszenia.

POSTULATY

- **Uważamy, że termin 24 godzinny, stosowany także w innych podobnych przepisach dot. zgłaszania incydentów, jest absolutnym minimum na dokonanie wstępnego zgłoszenia, które i tak będzie musiało być uzupełniane w toku obsługi incydentu poważnego.**
- Wnosimy o wprowadzenie zmian projektu zgodnie z powyżej zamieszczoną tabelą.

2) **Zakres kryteriów uznania incydentu za incydent poważny, zawarty w projekcie ustawy oraz w projekcie nowego rozporządzenia do art. 20d nowelizowanej uKSC jest zbyt szeroki i nieprecyzyjny.**

Do tzw. progów skutku zakłócającego służących do klasyfikacji incydentu jako poważnego obok liczby użytkowników i czasu **dodano w projekcie nowelizacji 6 nowych kategorii kryteriów**:

- obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego;
- zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług;
- wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej;

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
- wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych;
- wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

W wyniku rozszerzenia upoważnienia ustawowego, w projekcie rozporządzenia do art. 20d uKSC **nowymi kryteriami** są:

3) *incydent telekomunikacyjny miał wpływ na zachowanie tajemnicy telekomunikacyjnej dotyczącej co najmniej 100 użytkowników;*
4) *obszar dotknięty incydentem telekomunikacyjnym przekroczył obszar jednego powiatu, z wyłączeniem miast na prawach powiatu, w rozumieniu ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym;*
5) *incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy o zarządzaniu kryzysowym (Dz. U. z 2022 r. poz. 2022 r. poz. 261 i 583);*
6) *incydent telekomunikacyjny uniemożliwia wykonywanie obowiązków przedsiębiorcy komunikacji elektronicznej z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.*

Mamy świadomość, że projekt rozporządzenia może być na tym etapie jedynie jego wczesną wersją przedstawioną na potrzeby spełnienia formalnych warunków przedłożenia projektu ustawy do rozpatrzenia przez Stały Komitet Rady Ministrów. Niemniej jednak waga problemu uzasadnia odniesienie się do niego także już na tym wczesnym etapie.

Odnosząc się do tych nowych kryteriów wskazujemy następująco:

3) incydent telekomunikacyjny miał wpływ na zachowanie tajemnicy telekomunikacyjnej dotyczącej co najmniej 100 użytkowników

- W związku z tym, że określenie **„***miał wpływ na zachowanie tajemnicy telekomunikacyjnej*” jest według nas nieostre, proponujemy zmianę przepisu i nadanie mu następującego brzmienia:

  „incydent telekomunikacyjny skutkował naruszeniem tajemnicy telekomunikacyjnej dotyczącej co najmniej 5 % użytkowników danej usługi”

- Skoro incydent telekomunikacyjny to zdarzenie z rzeczywistym niekorzystnym skutkiem, to konsekwentnie (podobnie jak w pkt 2) powinniśmy do tego skutku się odwoływać. Poza tym nie należy naszym zdaniem wskazywać konkretnej liczby użytkowników (100), tylko odwołać się do adekwatnego procenta użytkowników danej usługi.

4) obszar dotknięty incydentem telekomunikacyjnym przekroczył obszar jednego powiatu

- Sygnalizujemy, że projektowane kryterium nie przystaje do praktyki funkcjonowania sieci telekomunikacyjnych. Przede wszystkim sieci nie są projektowane z uwzględnieniem podziału administracyjnego kraju.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

- Szczególnie w przypadku większych sieci stacjonarnych oraz w przypadku wszystkich sieci ruchomych przekroczenie obszaru jednego powiatu będzie występowało niemal zawsze.
- Brak jakiegokolwiek doprecyzowania spowoduje, że incydentów poważnych pojawi się bardzo dużo. Kryterium spowoduje konieczność informowania o awariach z bardzo małym wpływem usługowym, np.: transmisyjnych, których wpływ na klientów może być niewielki. Problemem będzie również określenie rzeczywistego wpływu awarii w odniesieniu do granic administracyjnych powiatów (zarówno dla usług mobilnych jak i FIX). W praktyce będzie to bardzo obciążające dla operatorów i CSRIT, a także będzie tworzyło niewłaściwy obraz w raportach, a incydenty faktycznie nie będą poważnymi, mimo, że za takie musiały być uznane.

5) incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej oraz funkcjonowanie infrastruktury krytycznej

- Po raz kolejny wskazujemy, że operator telekomunikacyjny nie ma wiedzy kto jest operatorem usługi kluczowej lub dysponentem infrastruktury krytycznej. Takie informacje można przekazać w raporcie, o ile one są znane, np. dany podmiot poinformował publicznie o statusie OUK albo status danych zasobów jest operatorowi raportującemu znany z uwagi na relacje z OUK lub dysponentem IK. W żadnym wypadku nie może to stanowić bezwzględnego kryterium uznania incydentu za poważny. Zobowiązuje się bowiem operatora do klasyfikowania incydentu na podstawie kryterium o którym nie ma wiedzy, a przynajmniej nie musi mieć wiedzy, a więc obowiązku wykonać nie może.
- Postulujemy wykreślenie kryterium lub wskazanie, że stosuje się jedynie wówczas gdy to zgłaszający raport operator jest OUK lub dysponentem IK, którego dotyczył incydent.

6) incydent telekomunikacyjny uniemożliwia wykonywanie obowiązków przedsiębiorcy komunikacji elektronicznej z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego

Kryterium jest zbyt ogólne i powinno być doprecyzowane, o które konkretnie obowiązki chodzi oraz jaki jest minimalny czas trwania tej niemożliwości.

POSTULAT

- Odejście od aktualnie sformułowanych, zbyt ogólnych kryteriów klasyfikacji, które nie spowodują, że raportowane będą incydenty poważne, czyli *incydenty telekomunikacyjne o znaczącym wpływie na bezpieczeństwo sieci lub usług komunikacji elektronicznej* .

W przypadku uruchomienia prac legislacyjnych dotyczących nowych kryteriów postulujemy rozpoczęcie od prac roboczych zespołów Ministerstwa Cyfryzacji, UKE oraz operatorów, z ewentualnym udziałem CSIRT NASK w celu ustalenia optymalnego zakresu kryteriów.

3. Nadmiarowe wymaganie szacowania ryzyka raz w roku.

Zgodnie z art. 20a ust. 2 pkt 1 projektu ustawy przedsiębiorca komunikacji elektronicznej ma przeprowadzać systematyczne szacowanie ryzyka wystąpienia sytuacji szczególnego

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

zagrożenia co najmniej raz w roku. W porównaniu do poprzedniej wersji zaostrzono ten wymóg właśnie w zakresie min. corocznego szacowania ryzyka. Nie znajdujemy uzasadnienia dla takiego działania. Szczególnie, że nawet obowiązek operatorów usług kluczowych nie jest tak daleko idący i ogranicza się do systematycznego szacowania ryzyka. W naszej ocenie taki obowiązek jest zdecydowanie nadmiarowy.

Jest to również niespójne i bardziej rygorystyczne niż aktualne wymagania wynikające z rozporządzenia do art. 175d PT, które wskazuje, że *przedsiębiorca przeprowadza ocenę bezpieczeństwa sieci i usług telekomunikacyjnych co najmniej raz na dwa lata.*

POSTULAT

Przywrócenie poprzedniej wersji projektu poprzez wykreślenie zwrotu: „co najmniej raz w roku", ewentualnie wskazanie terminu dwuletniego.

4. Należy dostosować nierealny termin rozpoczęcia raportowania przez OUK przez S46

Podtrzymujemy nasze dotychczasowe uwagi dot. wyłączenia bezwzględnego obowiązku raportowania przez system S46 przez operatorów usług kluczowych. W przypadku jego utrzymania należy zapewnić finansowanie przyłączenia wszystkich objętych obowiązkiem podmiotów.

Zupełnie nierealny jest natomiast wskazany w projekcie ustawy termin rozpoczęcia takiego raportowania: *Art. 4. 1. Operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą systemu teleinformatycznego* ***od 1 stycznia 2024 r.***

POSTULAT

Rozpoczęcie raportowania z wykorzystaniem systemu S46 od stycznia 2024 jest niemożliwe. Po pierwsze obowiązek rozpoczęcia raportowania powinien zostać dostosowany do spodziewanego terminu udostępniania narzędzi, w tym finansowych umożliwiających podłączenie operatorów usług kluczowych do systemu S46. W naszej ocenie, biorąc pod uwagę termin najwcześniejszego wejścia w życia projektowanej ustawy, który nastąpi już w 2024 r. oraz czas niezbędny na przyłączenie do systemu uważamy, że termin ten powinien zostać określony na 1 stycznia 2025 r.

5. Konieczność dookreślenia krajowego programu certyfikacji cyberbezpieczeństwa

W dodawanym art. 59d ust. 2 projektu ustawy zawarto fakultatywne upoważnienie do wydania rozporządzenia Rady Ministrów określającego krajowy program certyfikacji cyberbezpieczeństwa dla wybranych produktów, usług lub procesów ICT. Zgodnie z § 68 ust. 2 zdanie pierwsze Zasad Techniki Prawodawczej, jeżeli do funkcjonowania ustawy jest niezbędne wydanie rozporządzenia, upoważnieniu nadaje się charakter obligatoryjny. W przypadku opisanego rozporządzenia tak właśnie jest. Jeżeli rozporządzenie nie zostanie wydane, w obrocie prawnym brak będzie tak istotnych elementów funkcjonowania

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

krajowego systemu cyberbezpieczeństwa jak zakres dokumentacji technicznej, sposób przechowywania dokumentacji technicznej czy treści i wzór graficzny krajowego certyfikatu cyberbezpieczeństwa. Co równie istotne, poza regulacją prawną pozostaną „warunki wydawania, utrzymywania, przedłużania i odnawiania ważności certyfikatów" (art. 59d ust. 2 pkt 6 znowelizowanego KSCU). Taką sytuację należy uznać z konstytucyjnymi wymogami formułowania upoważnień przez to, że to upoważnienie przenosi na poziom pod ustawowy materię ustawową i przenosi na poziom organów wykonawczych decyzję o stosowaniu znacznego zakresu podmiotowego i przedmiotowego ustawy, przekazując w Radzie Ministrów uprawnienia samoistne. Warto przypomnieć, że zgodnie z rozporządzeniem 2019/881 „krajowy program certyfikacji cyberbezpieczeństwa" oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych i przyjętych przez krajowy organ publiczny, i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT i procesów ICT". Rozporządzenie fakultatywne, poza tym, że dopuszcza częściowy brak regulacji, nie spełnia warunku „kompleksowości" regulacji w polskich przepisach prawa.

POSTULAT

Wprowadzenie obligatoryjnego rozporządzenia Rady Ministrów określającego krajowy program certyfikacji cyberbezpieczeństwa dla wybranych produktów, usług lub procesów ICT.

6. Propozycja zmiany treści art. 14 ust. 10 - 11 projektu ustawy w zakresie dotyczącym funkcjonowania zespołów pełniący funkcję operacyjnego centrum bezpieczeństwa

Jednostka redakcyjna	Aktualna treść	Proponowana treść	Uzasadnienie
art. 14 ust. 10	Infrastruktura SOC wewnętrznego lub SOC zewnętrznego wykorzystywana do realizacji zadań, o którym mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 znajduje się na terytorium Rzeczypospolitej Polskiej.	Infrastruktura SOC wewnętrznego lub SOC zewnętrznego wykorzystywana do realizacji zadań, o którym mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 znajduje się na terytorium Rzeczypospolitej Polskiej bądź poza nim w przypadku zawarcia z SOC umów regulowanych	Podmioty powinny mieć możliwość zawierania umów z SOCami poza granicami RP działającymi w ramach jednej grupy finansowej (właścicielskiej). W zakresie dużych grup finansowych operujących na całym świecie w ramach sektora usług finansowych jest to element mitygacji ryzyka poprzez: · Istnienie paru równolegle działających SOC pracujących 24/7 w

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

		poprzez szczegółowe przepisy sektorowe regulujące wymogi w zakresie powierzania usług podmiotom trzecim.	różnych częściach świata, z których każde jest w stanie wesprzeć OUK, co niweluje problemy w przypadku zaistnienia problemów na terytorium RP, · Benefit skali wynikający z wykorzystania standardów oraz procesów „grupowych" umożliwiający szybsze oraz bardziej kompleksowe działanie, · Szeroką perspektywę w zakresie wykrywania potencjalnych zagrożeń, co przekłada się na ich szybsze wykrycie oraz eliminację. Dodatkowo przepisy ar.t 6a-6d już w sposób bardzo restrykcyjny określają jakie czynności mogą podlegać outsourcingowi, a dodatkowo poddają takie powierzenie szczególnemu nadzorowi ze strony KNF.
art. 14 ust. 11	Personel SOC wewnętrznego lub SOC zewnętrznego realizujący zadania, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 posiada poświadczenie bezpieczeństwa osobowego do klauzuli „poufne".	Personel SOC wewnętrznego lub SOC zewnętrznego realizujący zadania, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13 posiada poświadczenie bezpieczeństwa osobowego do klauzuli „poufne, bądź równoważne w przypadku zawarcia z SOC umów regulowanych poprzez szczegółowe przepisy sektorowe regulujące wymogi w zakresie powierzania usług podmiotom trzecim.	

7. Nadmierny zakres przetwarzanych danych osobowych

W uwagach do projektu ustawy minister ds. UE wskazał, że w projektowanym art. 39 ust. 3 pkt 5 oraz ust. 4 pkt 4 UKSC dodaje się możliwość przetwarzania przez określone podmioty danych gromadzonych przez przedsiębiorców komunikacji elektronicznej. Wyjaśnienia wymaga niezbędność poszerzenia zakresu danych gromadzonych przez podmioty określone w projektowanych przepisach o „dane osobowe gromadzone przez przedsiębiorców komunikacji elektronicznej w związku ze świadczeniem usług komunikacji elektronicznej". Jest to o tyle istotne, iż projektowane wraz z Prawem komunikacji elektronicznej akty

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

wykonawcze do Prawa komunikacji elektronicznej wskazują niezwykle szeroki katalog danych które będą podlegać gromadzeniu przez przedsiębiorców komunikacji elektronicznej, w tym m.in. numer PUK pozwalający na zmianę numeru PIN do karty SIM i jej odblokowanie a tym samym dostęp do wszelkich informacji zapisanych na karcie. Informacja dotychczas traktowana jaka bardzo poufna gwarantująca bezpieczeństwo w korzystaniu np. z aplikacji bankowych, ma stanowić część informacji gromadzonej przez przedsiębiorców a w rozumieniu projektowanych przepisów spełnia przesłanki danych gromadzonych w związku ze świadczeniem usług, jednocześnie nie będąc związaną z incydentem telekomunikacyjnym. W odpowiedzi na tę uwagę projektodawca wskazał, że dane są przetwarzane w celu ich ochrony, a nie dalszego wykorzystania w innym celu. Argument ten wydaje się być nietrafiony, gdyż trudno uznać numer PUK jako pomocny np. przy identyfikacji urządzeń wchodzących w skład dużych sieci botnet, obserwowanie anomalii w ruchu sieciowym. Wyjaśnienia wciąż więc wymaga brak zawężenia projektowanego art. 39 ust. 4 pkt ustawy o krajowym systemie cyberbezpieczeństwa do danych gromadzonych przez przedsiębiorców komunikacji elektronicznej w związku ze świadczeniem usług komunikacji elektronicznej. Jest to bardzo istotne dla zapewnienia, aby dane te nie zostały wykorzystane do innych celów, zwłaszcza iż cel przetwarzania tych danych został określony maksymalnie szeroko i żaden podmiot, którego dane będą przetwarzane nie będzie w stanie stwierdzić jaki jest ten cel.

POSTULAT

Ograniczenie zakresu danych określonych w art. 39 ustawy o krajowym systemie cyberbezpieczeństwa.

II. WĄTPLIWOŚCI KONSTYTUCYJNE

Art. 2 i wynikająca z niego zasada prawidłowej legislacji, utożsamiana z zasadą określoności przepisów

Projekt budzi istotne zastrzeżenia z pespektywy zgodności z Konstytucją w następującym zakresie. Projekt narusza wymóg określoności przepisów wynikający z art. 2 Konstytucji RP, z którego wynika, że przepis prawa, a zwłaszcza ograniczający konstytucyjne wolności lub prawa, powinien być sformułowany w sposób pozwalający jednoznacznie ustalić, kto i w jakiej sytuacji podlega ograniczeniom. Przyjęte rozwiązania legislacyjne prowadzą do naruszenia wymogu dostatecznej jasności precyzyjności i komunikatywności przepisów. Przekroczenie pewnego poziomu niejasności przepisów prawnych stanowić może samoistną przesłankę stwierdzenia ich niezgodności z art. 2 Konstytucji . W tym przypadku – mimo wprowadzenia wielu nowości normatywnych i zasadniczej zmiany systematyzacji ustawy – zamiast wydania nowej ustawy zaproponowano ustawę zmieniającą. Spowodowało to naruszenie szczegółowych dyrektyw zasad prawidłowej legislacji. Zgodnie z § 84 ZTP: Jeżeli zmiany wprowadzane w ustawie miałyby być liczne

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

albo miałyby naruszać konstrukcję lub spójność ustawy albo gdy ustawa była już poprzednio wielokrotnie nowelizowana, opracowuje się projekt nowej ustawy. Projekt zawiera bardzo liczne przepisy zmieniające. Obecnie ustawa KSC składa się z 76 artykułów zawierających przepisy merytoryczne, a art. 1 projektu składa się z 74 punktów; ich brzmienie jest obszerniejsze niż ustawa nowelizowana. Dodatkowo, pomimo relatywnie krótkiego, 5-letniego okresu obowiązywania (obowiązuje od 28 sierpnia 2018 r.), ustawa była aż 8 razy nowelizowana i ukazały się już jej dwa teksty jednolite. W efekcie spełnione zostały wszystkie trzy przesłanki uzasadniające konieczność przygotowania nowej ustawy, chociaż zgodnie z § 84 ZTP już jedna z nich powinna być podstawą do opracowania nowej ustawy. Przyjęta metoda nowelizacji spowodowała popełnienie licznych błędów lub niekonsekwencji utrudniających korzystanie z ustawy.

Zasadniczym błędem dyskwalifikującym projekt z punktu widzenia poprawności legislacyjnej jest odwoływanie się w 12 przepisach projektu, w tym pięciu definicjach ustawowych, do ustawy Prawo komunikacji elektronicznej. Projekty aktów normatywnych mogą uwzględniać w swoim brzmieniu przepisy, które nie weszły jeszcze w życie, ale pod warunkiem, że zostały ogłoszone w dzienniku urzędowym. Zgodnie z art. 88 ust. 1 Konstytucji warunkiem wejścia w życie ustawy jest jej ogłoszenie. To oznacza, że ustawa wchodzi do porządku prawnego po jej ogłoszeniu i dopiero od tego momentu może być przedmiotem odesłań w innych przepisach. Zaproponowane rozwiązanie w sposób oczywisty narusza zasadę określoności przepisów, ponieważ do dnia ogłoszenia przepisy zawierające odesłania do Prawa telekomunikacji elektronicznej są puste lub niepełne. Pomijając kwestię, że nowy projekt ustawy Prawo telekomunikacji elektronicznej nie wpłynął nawet do laski marszałkowskiej, nie można przyjąć, oba projekty tak się zgrają, że nowela KSC wejdzie w życie nie wcześniej, niż w tym samym dniu co Prawo komunikacji elektronicznej. Będzie to tym trudniejsze, że nowela KSC podlegać będą notyfikacji przepisów technicznych, co biorąc po uwagę zakres przedmiotowy i podmiotowy ustaw może prowadzić do niezależnych od polskiego prawodawcy opóźnień w przyjęciu jednej albo drugiej ustawy.

Niezależnie od powyższego zgodnie z § 9 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 239 oraz z 2004 r poz. 597) projekt przed przekazaniem do Sejmu przekazany będzie do notyfikacji przepisów technicznych. Dla przeprowadzenia poprawnego i pełnego procesu notyfikacji Komisja Europejska musi dysponować tekstem, w którym brzmienie poszczególnych przepisów pozwala odtworzyć zawarte w nich normy prawne. Przekazanie do notyfikacji technicznej będzie więc możliwe dopiero po ogłoszeniu ustawy Prawo komunikacji elektronicznej.

art. 22 w związku z art. 31 ust. 3 Konstytucji

Projekt przewiduje istotne ograniczenia zasady swobody działalności gospodarczej wynikającej z art. 22 w związku z art. 31 ust. 3 Konstytucji i w tym zakresie może być uznany za wykraczający poza konstytucyjne granice określające dopuszczalność takiego

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

ograniczenia. W tym przypadku ograniczenia swobody działalności gospodarczej wynikające z decyzji uznającej dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka może prowadzić do istotnego ograniczenia wykonywania działalności gospodarczej bez wykazania, że w konkretnym przypadku zachodzą przesłanki określone w art. 31 ust. 3 Konstytucji. Z jednej strony chodzi o działalność podmiotów uznanych za DWR, z drugiej o przedsiębiorców, których działalność prowadzona jest w oparciu o sprzęt lub oprogramowanie dostarczone przez DWR.

art. 32 Konstytucji zasada równości i zakaz dyskryminacji

Projekt wprowadza postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za DWR, w ramach którego przewiduje się mechanizm powiadamiania o wszczęciu postępowania na stronie Biuletynu Informacji Publicznej oraz dopuszczenie do postępowania jedynie największych przedsiębiorców telekomunikacyjnych. Narusza to nakaz równego traktowania podmiotów, które są obdarzone określoną cechą relewantną (istotną) z punktu widzenia danej sfery stosunków prawnych, gdy dyspozycja normy prawnej wyróżnia daną sferę stosunków ze względu na wskazaną cechę relewantną oraz gdy istnieje związek pomiędzy cechą relewantną danej kategorii podmiotów a treścią przyjętej regulacji.

Do postępowania o uznanie za DWR może przystąpić na wniosek na prawach strony przedsiębiorca komunikacji elektronicznej, który w poprzednim roku obrotowym uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej. Narusza to zasadę równości poprzez wprowadzenie kryterium ekonomicznego zróżnicowania praw podmiotów w sytuacji, gdy zasadniczy cel instytucji uznania za DWR ma wykluczyć każdy sprzęt lub oprogramowania ze względu na zagrożenie cyberbezpieczeństwa. Powoduje to niedopuszczalne rozdzielenie podmiotów posiadających tę samą istotną cechę wspólną (relewantną).

W OSR pisze się, że: „Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. W przekazanym projekcie jest mowa o 5-7 latach - termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Z uwagi na wskazanie tak długiego okresu na wdrożenie decyzji o ocenie ryzyka, nie są planowane rekompensaty dla operatorów z uwagi na konieczność wycofania sprzętu lub oprogramowania od dostawców uznanych za dostawców wysokiego ryzyka.”. To założenie jest wątpliwe – czy naprawdę nie ma sprzętu, który taką decyzją mógłby zostać objęty, a który wymienia się rzadziej? W projekcie brak jest przesłanek do analizy żywotności poszczególnych rodzajów sprzętu czy oprogramowania, więc założenie to jest, jeśli nie bezpodstawne, to niedostatecznie udowodnione merytorycznie. Jeśli zaś jest sprzęt, który wymienia się rzadziej, to przejście nad tym do porządku dziennego przez

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.
NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

projektodawców świadczy o powierzchowności analizy skutków finansowych i wobec braku rekompensat – o wątpliwościach konstytucyjnych

art. 45, zasada prawa do sądu

Projekt wyłącza istotną grupę podmiotów z udziału w postępowaniu w sprawie uznania za DWR, mimo, że skutki decyzji w tej sprawie de facto przesadzają o ich wolnościach i prawach gospodarczych. Projekt wprowadza cenzus majątkowy wykluczają z udziału w postępowaniu szereg przedsiębiorców średniej wielkości, na których będą spoczywały obowiązki w wyniku przyjęcia decyzji (obowiązki będą spoczywać na 69 przedsiębiorcach, a udział będzie mogło wziąć kilkunastu z nich). Tymczasem wszyscy zostaną dotknięci ograniczeniami z tytułu uznania za DWR. W OSR wskazuje się, że: „Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy telekomunikacyjni oraz operatorzy infrastruktury krytycznej w związku z wycofaniem produktów, usług i procesów pochodzących od dostawców wysokiego ryzyka, ponieważ nie można w tej chwili przewidzieć jaką decyzję wyda minister właściwy do spraw informatyzacji i w związku z tym jakie koszty poniosą podmioty zobowiązane do wycofania sprzętu" oraz że „Nie jest możliwe w tej chwili wskazanie kosztów jakie poniosą podmioty krajowego systemu cyberbezpieczeństwa, przedsiębiorcy komunikacji elektronicznej, operatorzy infrastruktury krytycznej, dostawcy usług zaufania, krajowe instytucje płatnicze ponieważ polecenie zabezpieczające będzie wydawane po wystąpieniu incydentu krytycznego.". Można było, przykładowo, zweryfikować, czy zbliżone decyzje i polecenia zostały wydane już w innych państwach, a jeśli tak – to czego dotyczyły. W następnym etapie z kolei można by przeprowadzić symulację, jaki byłby koszt dla polskich przedsiębiorców telekomunikacyjnych, gdyby wydano analogiczne decyzje.

Jak stwierdza się w uzasadnieniu projektu, wyłączenie organizacji społecznych z udziału w postępowanie o uznanie za DWR wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego, jednak nie ma podanych żadnych powodów, dlaczego taka konkluzja może wyłączać w tym przypadku art. 31 Kpa.

Nieostrość przesłanek podjęcia decyzji w przedmiocie uznania za dostawcę wysokiego ryzyka

Analiza możliwości przyjęcia mniej dotkliwych skutków uznania podmiotu za dostawcę wysokiego ryzyka jest o tyle istotna, że przesłanki takiego uznania są nieostre, co grozi arbitralności rozstrzygnięć (szczególnie wobec ograniczenia jawności postępowania). Decyzja ma być wydawana wobec podmiotu, który „stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi", zaś opinia kolegium uwzględniać ma „zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich". Wszystko to wydają się być kwestie stosunkowo ocenne. Można argumentować, że istotny luz decyzyjny, jaki

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy

powstaje po stronie organu państwa, powinien zostać zrównoważony transparentnością procedur (w tym procedur odwoławczych) i powinien być uwzględniony przy projektowaniu skutków wydania takiej decyzji, w tym skutków dla innych podmiotów.

Dostawcy objęci Procedurą DWR, nie otrzymują treści całego wyroku w sprawie odwołania od Decyzji DWR, co więcej także elementy uzasadnienia Decyzji DWR mogą być niejawne (nawet jeśli byłyby reprezentowane przez osoby, posiadające dostęp do informacji objętych klauzulami tajności). Kwestię te podniosła także Rada Legislacyjna w opinii do projektu z dnia 23 lutego 2021 r., która zwróciła uwagę na brak dostatecznej precyzji w przepisach o doręczaniu odpisów wyroków sądu administracyjnego w sprawach skarg na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Rada Legislacyjna podnosiła także wątpliwość o charakterze konstytucyjnym, a mianowicie, czy w ogóle jest zgodne z Konstytucją RP odstępowanie od doręczania stronie pełnego uzasadniania wyroku sądu administracyjnego (według Rady, nie ulega wątpliwości, że w świetle konstytucyjnego prawa do sądu (art. 45 Konstytucji RP) zasadą musi być dostarczanie stronie pełnego uzasadnienia faktycznego decyzji administracyjnej, tak aby strona (będąca adresatem decyzji) mogła w sposób skuteczny, zaskarżyć tę decyzję do sądu administracyjnego.

KL/203/88/AM/2023

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
00-727 Warszawa

tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org.

NIP 5262353400
KRS 0000053779
Sąd Rejonowy dla
m. st. Warszawy w Warszawie XIII
Wydział Gospodarczy