Warszawa, 23 grudnia 2024 r.
KL/664/182/AM/2024

Pan
Maciej Berek
Minister - członek Rady Ministrów
Przewodniczący Komitetu Stałego Rady Ministrów

Szanowny Panie Ministrze,

W związku ze skierowaniem projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw, do rozpatrzenia Komitetu do Spraw Europejskich (znak pisma KPRM: DKSE.7004.10.41.2024.BB(4) z 6.12.2024 r.) w załączeniu przesyłam stanowisko Konfederacji Lewiatan dotyczące projektu ustawy.
Jednocześnie, wnosimy o podjęcie działań przez Pana Ministra w celu zorganizowania konferencji uzgodnieniowej z udziałem strony społecznej, mając na względzie, że znaczna część zgłoszonych uwag nie została uwzględniona.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
- Pan **Krzysztof Gawkowski**, Wiceprezes Rady Ministrów, Minister Cyfryzacji
- Pani **Anna Piesiak**, Sekretarz Komitetu do Spraw Europejskich, Kancelaria Prezesa Rady Ministrów

Załącznik: Stanowisko Konfederacji Lewiatan wobec projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (wersja z dnia 2 grudnia 2024 r.)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Stanowisko Konfederacji Lewiatan wobec projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (wersja z dnia 2 grudnia 2024 r.)

Uwagi wstępne

Zasada proporcjonalności (nakładanie kolejnych obciążeń na przedsiębiorców)

Przedmiotowy projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, poprzez kolejne zaostrzanie wymogów prowadzenia działalności gospodarczej, stanowi istotne zagrożenie dla konkurencyjności polskich przedsiębiorców. Dążenie do przeregulowania w tym obszarze pozostaje w sprzeczności z fundamentalną zasadą proporcjonalności, wywiedzioną zarówno z Konstytucji RP, jak i prawa Unii Europejskiej, w tym dyrektywy NIS2. Ograniczanie swobody działalności gospodarczej w stopniu wykraczającym poza to, co jest niezbędne do osiągnięcia uzasadnionych celów w zakresie cyberbezpieczeństwa, prowadzi do nieuzasadnionego i nadmiernego obciążenia polskich przedsiębiorców.

Obowiązki nakładane przez niniejszy projekt obejmują nie tylko sferę związaną bezpośrednio z usługami świadczonymi przez podmioty kluczowe i ważne, lecz także całość działalności przedsiębiorstwa, co znacząco wykracza poza ramy wytyczone w prawie unijnym. Konsekwencją takiego rozszerzenia jest wzrost kosztów prowadzenia działalności – obejmujący m.in. wymianę sprzętu i oprogramowania – który w przypadku setek milionów złotych może poważnie nadwyrężyć stabilność finansową podmiotów działających na polskim rynku (w zakresie procedury dostawcy wysokiego ryzyka). Tego rodzaju obciążenia nie tylko osłabiają zdolność konkurowania z przedsiębiorcami z innych państw członkowskich UE, ale mogą również przełożyć się na ograniczenie inwestycji oraz zmniejszone wpływy budżetowe.

W kontekście trudnej sytuacji budżetowej oraz istniejącego dystansu gospodarczego pomiędzy Polską a innymi, zamożniejszymi państwami członkowskimi UE, przyjmowanie rozwiązań przeregulowanych i niedostosowanych do krajowych realiów stanowi nadmierną ingerencję w sferę działalności gospodarczej. Zamiast nieproporcjonalnie zaostrzać wymogi, należy rozważyć wprowadzenie rozwiązań bardziej elastycznych i adekwatnych do polskich możliwości, co pozwoli zminimalizować negatywne skutki ekonomiczne i zapewni utrzymanie równowagi pomiędzy bezpieczeństwem cybernetycznym a swobodą działalności gospodarczej.

Negatywnym przykładem są proponowane zmiany zawarte w art. 53 i art. 53e projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, które w sposób szczególnie jaskrawy ilustrują filozofię nadmiernej i nieproporcjonalnej ingerencji państwa w działalność gospodarczą, wykraczającą poza standardy wynikające z dyrektywy NIS2 oraz standardy konstytucyjne. Zgodnie z prawem Unii Europejskiej, w tym z dyrektywą NIS2, działania organów powinny być adekwatne do naruszenia i stosowane wyłącznie wtedy, gdy mniej

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

restrykcyjne środki nie przyniosły skutku. Motyw (133) dyrektywy NIS2 wyraźnie podkreśla, że tymczasowe środki, takie jak zawieszenie certyfikacji, zezwolenia lub pełnienia funkcji zarządczych, mogą zostać nałożone jedynie w ostateczności, proporcjonalnie do powagi naruszenia oraz z uwzględnieniem wszystkich istotnych okoliczności sprawy. Działania te powinny być stosowane wyłącznie do czasu, aż przedsiębiorca podejmie niezbędne kroki w celu przywrócenia zgodności z wymogami.

Analizując proponowane polskie przepisy, można dostrzec ryzyko przekroczenia wskazanych ram. Rozwiązania krajowe wydają się bowiem obejmować nie tylko usługi i działalność objętą przedmiotem regulacji bezpieczeństwa teleinformatycznego, lecz także całą działalność gospodarczą danego podmiotu. Zawieszenie lub ograniczenie koncesji, wpisu do rejestru działalności regulowanej, czy też działalności rejestrowanej w CEIDG, może potencjalnie prowadzić do nadmiernego obciążenia przedsiębiorców oraz ograniczenia ich podstawowych wolności gospodarczych. Takie działanie wykracza poza zakres określony w NIS2, który przewiduje przede wszystkim środki ukierunkowane na obszary bezpośrednio związane z usługami kluczowymi oraz bezpieczeństwem sieci i systemów informatycznych (dopuszczając zawieszenie częściowo lub całkowite).

Ponadto, choć dyrektywa NIS2 przewiduje stosowanie odpowiednich gwarancji proceduralnych, w tym prawa do skutecznego środka prawnego i rzetelnego procesu, w praktyce odwołanie się do drogi sądowej w Polsce może okazać się mało efektywne. W kontekście opieszałości, przewlekłości postępowań oraz generalnej nieefektywności polskiego sądownictwa, skorzystanie z prawa do skutecznej ochrony sądowej staje się w dużej mierze iluzoryczne. W efekcie, nawet formalne gwarancje proceduralne mogą nie zapewnić przedsiębiorcom realnej, szybkiej i skutecznej ochrony przed nadmiernymi i nieproporcjonalnymi środkami egzekwowania przepisów.

Należy zwrócić uwagę na planowane odstępstwa od zasad Konstytucji dla Biznesu w zakresie kontroli przedsiębiorców, które podważają sens wprowadzania Prawa przedsiębiorców. Projekt przewiduje wyłączenie art. 54, zakazującego równoczesnego prowadzenia więcej niż jednej kontroli, oraz art. 55, ograniczającego czas trwania kontroli. Nowy limit 48 dni roboczych w roku kalendarzowym, proponowany w art. 54 ust. 2, nie stanowi realnej bariery i nie zapewnia sprawnego zakończenia kontroli. Nie zostało również wyjaśnione, dlaczego dotychczasowe limity, np. 24 dni dla średnich przedsiębiorstw, są niewystarczające dla organów właściwych do spraw cyberbezpieczeństwa.

Wątpliwości budzi także projektowany art. 58 ust. 8 ustawy o krajowym systemie cyberbezpieczeństwa. Umożliwia on wznowienie kontroli i podjęcie dodatkowych czynności kontrolnych „w razie potrzeby", nie precyzując przesłanek podjęcia takich działań przez osobę prowadzącą kontrolę (a nie jej kierownika). W efekcie wyłączenia te wydają się wprowadzane na wyrost, bez dowodów na to, iż dotychczas obowiązujące zasady utrudniałyby osiągnięcie celów kontroli. Zastrzeżenia te podziela Minister Rozwoju i Technologii w swoim stanowisku do projektu (pismo znak: DGC-V.003.42.2024 z 22.10.2024 r.).

Postępowanie w sprawie dostawcy wysokiego ryzyka

Przepisy regulujące postępowanie w sprawie uznanie danego podmiotu za dostawcę wysokiego ryzyka, zaproponowane przez projektodawcę, wciąż budzą wątpliwości rynku odnośnie ich właściwej interpretacji.
Część firm zwraca uwagę na to, że brakuje podstaw do wykluczenia dostawcy wysokiego ryzyka na podstawie kryterium politycznego, które pozornie łączy się z państwem pochodzenia dostawcy, podzielając pogląd przyjęty przez ekspertów z Ministerstwa Cyfryzacji:

„Za dostawcę wysokiego ryzyka może być uznany podmiot działający w Unii Europejskiej jak i poza UE, niezależnie od pochodzenia kapitału.

Proces ten jest dokładnie uregulowany i wymaga przeprowadzenia sformalizowanej, wieloetapowej procedury administracyjnej, w ramach której dostawca będzie miał możliwość przedstawienia swoich argumentów„.[1]

Nie brakuje jednak głosów z rynku, które podważają sens zamieszczania w ustawie kryterium pochodzenia dostawcy w katalogu przesłanek, jakie powinny być brane pod uwagę w ramach analizy towarzyszącej wyznaczaniu dostawcy wysokiego ryzyka.
Wprowadzenie procedury klasyfikowania dostawcy wysokiego ryzyka, opierającej się na nietechnicznych kryteriach, takich jak państwo pochodzenia dostawcy, rodzi szereg poważnych zagrożeń gospodarczych i regulacyjnych. Kolejna iteracja projektu dostarcza nowych wątpliwości, ponieważ w art. 67b ust. 15 wprowadzono zmianę polegającą na wydaniu decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka w przypadku, gdy stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa, dające dużą przestrzeń interpretacyjną, prowadząc do arbitralności i dowolności decyzji w sprawie dostawcy wysokiego ryzyka. Co więcej procedura ta narusza zasadę równego traktowania podmiotów gospodarczych w ramach unijnego rynku wewnętrznego, zgodnie z art. 18 Traktatu o Funkcjonowaniu Unii Europejskiej (TFUE). Artykuł ten zakazuje wszelkiej dyskryminacji ze względu na przynależność państwową, co oznacza, że decyzje administracyjne muszą opierać się na obiektywnych, technicznych kryteriach, a nie na przesłankach politycznych – przepis ten dotyczy również dostawców mających siedzibę w innych krajach Unii Europejskiej, choćby ich macierzyste spółki wywodziły się spoza rynku europejskiego (por. przepisy ustawy z dnia 6 marca 2018 r. o zasadach uczestnictwa przedsiębiorców zagranicznych i innych osób zagranicznych w obrocie gospodarczym na terytorium Rzeczypospolitej Polskiej (t.j. Dz. U. z 2022 r. poz. 470).
Kwestie związane z kosztami tego postępowania, w tym wpływem na rynek, konkurencyjność, ceny usług oraz dostęp do komponentów i technologii, zostały pominięte

[1] https://www.gov.pl/web/cyfryzacja/to-nie-panstwo-pochodzenia-bedzie-decydowac-o-uznaniu-za-dostawce-wysokiego-ryzyka-w-ksc#:~:text=Instytucja%20dostawcy%20wysokiego%20ryzyka&text=Chodzi%20wi%C4%99c%20o%20identyfikacj%C4%99%20dostawcy,UE%2C%20niezale%C5%BCnie%20od%20pochodzenia%20kapita%C5%82u.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

w przygotowanej Ocenie Skutków Regulacji (OSR). Jednocześnie Ministerstwo Cyfryzacji nie odnosi się do tych pominięć, ignorując potencjalne negatywne konsekwencje finansowe dla przedsiębiorców i gospodarki. Ograniczenie dostępu do sprzętu oraz oprogramowania od dostawców spoza EOG i NATO zmniejszy liczbę podmiotów konkurujących na rynku. W efekcie może to prowadzić do wzrostu cen usług i produktów, co uderzy zarówno w konsumentów, jak i przedsiębiorców. Takie podejście ogranicza również dostęp do innowacyjnych rozwiązań technologicznych, utrudniając polskim firmom skuteczne konkurowanie na arenie międzynarodowej.

Wprowadzenie restrykcji wobec dostawców spoza EOG i NATO może wywołać reakcje odwetowe ze strony państw trzecich, co szczególnie dotknęłoby gospodarkę silnie zależną od eksportu. Retorsje handlowe, w tym nałożenie dodatkowych ceł czy ograniczeń dostępu do tamtejszych rynków, mogą znacznie osłabić pozycję polskich eksporterów. Przykładowo, wcześniejsze decyzje w sprawie ceł antydumpingowych na produkty z Chin pokazały, że takie działania mogą zniechęcić kluczowych partnerów handlowych i pogorszyć relacje gospodarcze. Fakt, że OSR nie uwzględnia tych ryzyk, a Ministerstwo Cyfryzacji nie odnosi się do nich, powoduje poważne luki w rzetelnej ocenie skutków projektowanych przepisów.

Ograniczenia w dostępie do komponentów i technologii od dostawców spoza EOG i NATO uderzą przede wszystkim w polskie przedsiębiorstwa, w tym MŚP, często opierające swoją ofertę na tańszych i równie innowacyjnych rozwiązaniach zagranicznych. Wzrost kosztów produkcji i trudności w pozyskiwaniu kluczowych zasobów mogą uniemożliwić rozwój i ekspansję na nowe rynki.

Planowane w art. 67c ust. 4 ustawy oraz związanych z nim przepisach w Prawie zamówień publicznych (art. 11) ograniczenia dotyczące kwalifikacji wykonawców nie znajdują uzasadnienia w świetle dyrektywy 2014/24/UE. Próby zawężania możliwości udziału wykonawców spoza EOG i NATO naruszają unijne zasady swobody przepływu towarów i usług, na co w toku konsultacji zwracał uwagę Minister ds. UE (pismo z 3.06.2024 r. znak: DPUE.720.508.2024(8); pismo znak DPUE.720.508.2024(14).KWM).

Uwzględniając powyższe zagrożenia, zasadne jest wezwanie do ponownej analizy projektu z uwzględnieniem wszystkich aspektów kosztowych i ekonomicznych, zarówno tych bezpośrednich, jak i wynikających z potencjalnych retorsji handlowych. Polska, jako kraj silnie zorientowany na eksport i współpracę międzynarodową, nie może pozwolić sobie na wprowadzanie regulacji bez rzetelnej oceny ich skutków finansowych. Przed ich wdrożeniem konieczne jest przeprowadzenie pełnej analizy kosztów w OSR oraz otwarta debata, do której Ministerstwo Cyfryzacji powinno aktywnie się włączyć, zamiast pomijać tak istotne kwestie.

Brak notyfikacji technicznej

Projektodawca utrzymuje stanowisko o braku konieczności przeprowadzenia notyfikacji technicznej TRIS, pomimo istnienia takiego obowiązku wynikającego z przyjętych mechanizmów wykraczających poza prawo UE, tj.:

a) procedury dostawcy wysokiego ryzyka,

b) procedury poleceń zabezpieczających.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

Wspomniane postępowania nie odnoszą się wyłącznie do sieci 5G, jak wskazuje *EU toolbox on 5G cybersecurity*, lecz obejmują 18 sektorów gospodarki, a zatem znacząco wykraczają poza zakres tego dokumentu (nb. nie stanowiącego prawa europejskiego, lecz będący jedynie rekomendacją Komisji Europejskiej). 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). Na konieczność notyfikacji zwracali uwagę eksperci, także były dyrektor departamentu cyberbezpieczeństwa w Ministerstwie Cyfryzacji i KPRM[2].

Brak przeprowadzenia notyfikacji technicznej TRIS będzie podważał skuteczność przepisów w tym zakresie. Jak wynika z orzecznictwa TSUE niedopełnienie obowiązku notyfikacji technicznej powoduje, iż dane przepisy techniczne stają się nieważne, a zatem nie mają mocy obowiązującej wobec jednostek (por. sprawa C-194/94 CIA Security, sprawa C-65/06 Komisja przeciwko Republice Greckiej, sprawa C-20/05 Schwibbert). Nawet pilność rozwiązania problemów społecznych nie zwalnia z obowiązku notyfikacji. Oznacza to, że brak notyfikacji jest traktowany jako istotne naruszenie procedury legislacyjnej, które może prowadzić do uznania przepisów za bezskuteczne.

Jeśli zatem projektodawca podtrzymuje swoje stanowisko, postulujemy wyodrębnienie procedury dostawcy wysokiego ryzyka oraz poleceń zabezpieczających do odrębnego projektu, który nie będzie musiał być procedowany w trybie przyspieszonym ze względu na przekroczony termin implementacji dyrektywy NIS2.

Świadczenie usług transgranicznych

Zgodnie z projektowanym art. 5a podmioty kluczowe i ważne podlegają obowiązkom wynikającym z ustawy, jeżeli posiadają jednostkę organizacyjną na terytorium Polski. Artykuł ten ma stanowić implementację art. 26 ust. 1 dyrektywy NIS 2, zgodnie z którym podmioty objęte dyrektywą uznaje się za podlegające jurysdykcji państwa członkowskiego, w którym faktycznie prowadzą działalność. Motyw 114 dyrektywy NIS 2 podkreśla, że kryterium miejsca prowadzenia działalności oznacza realną aktywność gospodarczą realizowaną poprzez stabilne struktury. Brak definicji pojęcia „jednostka organizacyjna" w projekcie ustawy sprawia, że posiadania jej na terytorium Polski nie można automatycznie utożsamiać

[2] https://cyberdefence24.pl/polityka-i-prawo/notyfikacja-komisji-europejskiej-w-nowelizacji-ksc-rzad-usunal-zapisy

z faktycznym prowadzeniem tam działalności. W celu zapewnienia zgodności z dyrektywą NIS 2 art. 5a należy zatem doprecyzować.

Niedookreślenie tego kryterium niesie potencjalne negatywne konsekwencje dla polskich przedsiębiorców, którzy nie świadczą usług w Polsce, a całość ich obrotu ma charakter eksportowy. W takiej sytuacji podmiot, mimo braku oddziaływania na krajową infrastrukturę czy użytkowników, musiałby spełniać wymogi ustawy, ponosić dodatkowe koszty i obciążenia administracyjne, nie uzyskując jednocześnie żadnych realnych korzyści. Powoduje to niepotrzebne podwyższenie kosztów działalności i pogarsza pozycję polskich eksporterów na rynkach zagranicznych. Mogą oni znaleźć się w mniej korzystnej sytuacji niż zagraniczni konkurenci, którzy nie są objęci analogicznymi wymogami, co prowadzi do asymetrii regulacyjnej i nie sprzyja budowaniu konkurencyjności polskich podmiotów poza granicami kraju.

W 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*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

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.

Art. 14 – odtwarzanie infrastruktury

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

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.

W praktyce wnosimy o nadanie zmianie w art. 14 projektu uKSC następującego brzmienia:

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

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.*

Mając na uwadze powyższe wnosimy o wprowadzenie następujących uwag w projekcie ustawy o krajowym systemie cyberbezpieczeństwa:

- **Wyodrębnienie 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. Drugi projekt zawierałby rozwiązania nie wynikające z dyrektywy NIS2, które wymagają pogłębionej analizy i oceny skutków regulacji.

- **W przypadku braku uwzględnienia ww. uwagi, jako minimum lub też jako postulat dotyczący wyodrębnionego projektu nowelizacji, wnosimy o**

    - **Ponowna analiza przepisów regulujących procedurę uznawania dostawcy za dostawcę wysokiego ryzyka, w tym kryterium państwa pochodzenia dostawcy;**

    - **dostosowanie kryteriów i zakresu procedury uznania dostawcę za dostawcę wysokiego ryzyka do dyrektywy NIS2**: w tym zakresie zalecamy dostosowanie polskich przepisów dotyczących uznania dostawcy za wysokiego ryzyka do minimalnych wymogów wynikających z dyrektywy NIS2, aby zapewnić spójność z unijnymi regulacjami. Dyrektywa NIS2 określa wyraźne techniczne kryteria oceny ryzyka, związane z cyberbezpieczeństwem, bez odwoływania się do geopolitycznych czynników. Przestrzeganie tych wytycznych pozwoli uniknąć sprzeczności między polskim prawem a przepisami unijnymi oraz zapobiegnie dyskryminacji dostawców spoza UE;

    - **ograniczenie stosowania narzędzia 5G Toolbox wyłącznie do sieci 5G**. narzędzie „5G EU Toolbox" zostało opracowane z myślą o zabezpieczeniu sieci 5G i nie powinno być stosowane do innych sektorów lub technologii. Wykorzystywanie narzędzia w sektorach niezwiązanych z 5G wprowadza niepotrzebne polityczne kryteria, które mogą ograniczać swobodny przepływ towarów i usług na jednolitym rynku UE. Proponujemy ograniczenie zastosowania „5G EU Toolbox" wyłącznie do sieci 5G, zgodnie z jego pierwotnym założeniem, co pozwoli uniknąć nieproporcjonalnych obciążeń

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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

dla innych branż. Wprost wyłączone powinny być także elementy pasywne. Zał. 3 ustawy bazuje na rozwiązaniu wprowadzonym we Francji, które wprost odnosi się do sieci 5G, stacji bazowych New Radio oraz wyłącza elementy pasywne tj. anteny pasywne oraz niezarządzane elementy sieci.

- **wprowadzenie technicznych kryteriów inicjowania procedury dostawcy wysokiego ryzyka**: decyzja o wszczęciu procedury uznania dostawcy za dostawcę wysokiego ryzyka powinna opierać się na precyzyjnie określonych technicznych przesłankach, związanych z zagrożeniami dla cyberbezpieczeństwa. Takie podejście zapewni obiektywizm i wyeliminuje subiektywne elementy oceny;
- **rozszerzenie kręgu decyzji w sprawie dostawcy wysokiego ryzyka:** w celu zapewnienia odpowiedniego poziomu transparentności oraz zgodności z interesem bezpieczeństwa narodowego, decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka powinna być podejmowana wspólnie przez Ministerstwo Obrony Narodowej, Ministerstwo Spraw Zagranicznych, Ministerstwo Finansów, Ministerstwo Sprawiedliwości oraz Ministerstwo Cyfryzacji. Taki model podejmowania decyzji wyeliminuje ryzyko nadmiernej koncentracji władzy decyzyjnej w jednym organie i zapewni szersze podejście do kwestii oceny ryzyka.
- **włączenie innych interesariuszy do procesu oceny**: zalecamy, aby w procedurę oceny dostawców wysokiego ryzyka byli włączeni inni interesariusze, w tym przedstawiciele sektora prywatnego, regulatorów rynku i organizacji branżowych. Pozwoli to na uzyskanie bardziej zrównoważonej oceny i uniknięcie sytuacji, w której decyzje będą podejmowane bez odpowiedniego dialogu społecznego;
- **ustanowienie wyjątku w przypadku akceptacji dostawcy w innych krajach UE:** wnioskujemy o wprowadzenie przepisu, który pozwala na akceptację dostawcy, produktu, usługi lub procesu w Polsce, jeśli jest on akceptowalny w innych krajach Unii Europejskiej. Taki zapis pozwoli uniknąć deharmonizacji przepisów i zapewni większą spójność na jednolitym rynku UE.

- Doprecyzowanie art. 5a projektu ustawy;
- Zmianę zakresu podmiotowego w art. 14 projektu ustawy.

KL/664/182/AM/2024

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 5
00-727 Warszawa
tel. +48 22 55 99 900
lewiatan@lewiatan.org
www.lewiatan.org

Polish Confederation
Lewiatan
Brussels Office
Avenue de Cortenbergh 168
tel. +32 2 732 12 10

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