KONFEDERACJA LEWIATAN

**Do druku nr 1955**

Warszawa, 24 listopada 2025 r.
KL/578/201/AM/2025

Pan
**Włodzimierz Czarzasty**
Marszałek Sejmu RP

WYDZIAŁ OBSŁUGI PREZYDIUM SEJMU
L. dz. SPS-III.020.368.5.2025
Data wpływu 26.XI.25r.

*Szanowny Panie Marszałku,*

w związku ze skierowaniem projektu *ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw* (druk nr 1955) do rozpatrzenia przez Sejm RP, pozwalam sobie przesłać, w załączeniu, stanowisko Konfederacji Lewiatan wobec projektu ustawy.

Z poważaniem

Marek Górski
Prezydent Konfederacji Lewiatan

Do wiadomości:

1) Pan Krzysztof Gawkowski – Wiceprezes Rady Ministrów, Minister Cyfryzacji
2) Pan Paweł Olszewski – Sekretarz Stanu, Ministerstwo Cyfryzacji
3) Pan Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik: Stanowisko Konfederacji Lewiatan wobec projektu ustawy zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (druk 1955).



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

KONFEDERACJA LEWIATAN

**Stanowisko Konfederacji Lewiatan wobec projektu ustawy zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw (druk 1955) (dalej: projekt ustawy)**

Konfederacja Lewiatan poniżej przedstawia propozycje poprawek do projektu ustawy:

**POPRAWKA nr 1:**

Określenie 12 miesięcznego okresu na dostosowanie

W art. 1 pkt 24 otrzymuje brzmienie:
*„Art. 16. Podmiot:*

1) *kluczowy lub ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 12 miesięcy,*
2) *kluczowy zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 24 miesięcy*

– *od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.";*

Uzasadnienie:

Aktualnie **wskazany w projekcie ustawy 6. miesięczny termin dostosowania jest zbyt krótki i nie jest realne dostosowanie się podmiotów obejmowanych krajowych systemem cyberbezpieczeństwa do nowych wymagań w tym terminie**. Termin ten musi zostać wydłużony przynajmniej do okresu 12 miesięcznego. Brak wydłużenia terminu grozi pospiesznym prowadzeniem prac wdrożeniowych, których celem nie będzie podniesienie poziomu bezpieczeństwa systemów teleinformatycznych, ale zabezpieczenie przed ryzykami związanymi z kontrolą i karami finansowymi.

Wyznaczenie nierealnego do dotrzymania terminu wobec bardzo wysokich kar finansowych oraz niespotykanych uprawnień kontrolnych i nadzorczych organów KSC stanowi **poważne zagrożenie dla regulowanych podmiotów, w tym sektora przedsiębiorstw**.

Podkreślamy także, że **opóźnienia w pracach legislacyjnych na poziomie rządowym nie mogą być kompensowane skracaniem terminów dla podmiotów obejmowanych nowymi wymaganiami.**

Ponadto, **dla istotnej części podmiotów wystąpi krzyżowanie wymagań nowego uKSC z projektowanymi na poziomie rządowym przepisami nowelizacji ustawy o zarządzaniu**



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

**kryzysowym**, która stanowi implementację dyrektywy CER dot. odporności podmiotów krytycznych. W myśl tamtych przepisów podmioty będące operatorami infrastruktury krytycznej (możliwe, że obejmie to zasoby regulowane także uKSC) będą miały 6 miesięcy od wpisu do wykazu infrastruktury krytycznej na analizę zagrożeń oraz kolejne 6 miesięcy na wdrożenie środków bezpieczeństwa. Z kolei podmioty krytyczne (klasyfikacja oparta o sektory takie jak w NIS2/uKSC) będą miały 9 miesięcy od informacji o wpisie na analizę zagrożeń o 3 miesiące na wdrożenie. Należy zakładać, że dla części podmiotów zakresy będą się przynajmniej częściowo pokrywać. Tym samym terminy wdrożeniowe powinny zostać zharmonizowane. Na zasadność spójnego spojrzenia na oba projekty wskazuje samo Rządowe Centrum Bezpieczeństwa, które w piśmie przekazującym nowy projekt pod obrady SKRM wskazało: *Ponadto* ***projektowane rozwiązania powinny być skorelowane z projektowanymi rozwiązaniami zawartymi w przepisach implementujących dyrektywę*** *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, zmieniającą rozporządzenie*** *(UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148. Mając na względzie, że przepisy implementujące dyrektywę 2022/2555 (nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa – UC32) są na bardziej zaawansowanym etapie prac rządowych – właściwym byłoby* ***prowadzenie prac nad przedkładanym projektem, tak aby oba projekty mogłyby być procedowane w tym samym czasie i na podobnych etapach w Sejmie i Senacie RP****.*

Określany w przepisach termin na dostosowanie jest jednocześnie **znacznie krótszy niż w wielu innych krajach UE**. Przykładowo:

- **W Belgii**[1] przepisy wdrażające NIS2 weszły w życie 18 października 2024. Podmioty miały na identyfikację i rejestrację terminy zróżnicowane wobec typu działalności, lecz generalnie w przedziale od 2 do 5 miesięcy.
  Mechanizm wdrażania środków organizacyjnych bazuje na przyjętym standardzie CyFun®, który przewiduje zróżnicowane poziomy zaawansowania.
  **Termin dostosowania wynosi natomiast 18 miesięcy**, przy czym co do zasady nie powinien przekraczać 18 kwietnia 2026 r., a w niektórych wypadkach może być jeszcze 12 miesięcy dłuższy.
- **W Czechach**[2] przewidziano 60 dniowy termin na samoidentyfikację (władze udostępniły narzędzie on-line do weryfikacji). Pierwsze obowiązki (raportowanie podstawowych informacji) obowiązują już po 30 dniach od rejestracji. **Rozpoczęcie raportowania incydentów następuje jednak nie później niż po roku od rejestracji.** Podobny **roczny termin wprowadzono na stosowanie odpowiednich środków bezpieczeństwa** opisanych w rozporządzeniach zawierających wymagania niższego i wyższego poziomu zależne od rodzaju działalności.

[1] NIS2 FAQ Website v2.0.1 EN.pdf
[2] https://portal.nukib.gov.cz/information-about-portal-nukib



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

- **Na Litwie**[3] przepisy weszły w życie 18 października 2024 r. Od daty rejestracji podmiotom przysługuje **12 miesięcy na wdrożenie środków organizacyjnych i 24 miesiące na wdrożenie środków technicznych**.

Poza powyższym, oceniamy, że nie zostały przygotowane odpowiednie warunki umożliwiające niezwłoczne przystąpienie do wdrażania przepisów, w tym:

- Projekt uKSC jest bardzo obszerną nowelizacją obowiązujących przepisów, co utrudnia samo odkodowanie norm kierowanych do podmiotów obejmowanych wymaganiami. Jest to zadanie ogromnie czasochłonne i wynikające jedynie z niesłusznej w naszej ocenie decyzji o nowelizacji uKSC zamiast zastąpienia jej nową ustawą.
- Nie zostały wykonane żadne realne prace przygotowujące przyszłe podmioty kluczowe i ważne do wdrażania nowych obowiązków. Nie odbywały się spotkania konsultacyjne lub szkoleniowe, takie jak chociażby realizował KNF w ramach przygotowań do wdrożenia DORA.
- Nie zostały opublikowane żadne materiały pomocnicze, zbiory wyjaśnień, dobrych praktyk lub odpowiedzi na najczęściej zadawane pytania, które byłyby pomocne w przygotowaniach do wdrożenia.
- Termin na uruchomienie kluczowych dla realizacji ustawy CSIRT sektorowych to aż 18 miesięcy. Wskazuje to na świadomość projektodawców co do skomplikowania regulowanej materii.
- Nie zostały uruchomione narzędzia wspierające samoidentyfikację podmiotów, które mają być regulowane nowym uKSC.
- Nie są znane przepisy rozporządzeń obligatoryjnych, które zostaną w niewiadomym terminie wydane do uKSC. Istnieje poważne ryzyko, że nastąpi to dopiero w „przededniu" terminu na dostosowanie, co np. w zakresie progów incydentów uniemożliwi podmiotom dostosowanie się do ich wymagań. W zakresie zaś rozporządzeń fakultatywnych (doprecyzowania dla Systemu Zarządzania Bezpieczeństwem Informacji) nie są znane plany dotyczące wydania takich aktów, ani tym bardziej ich zakresu i sektorów jakich będą dotyczyć. Jest to natomiast podstawa dla efektywnych decyzji o sposobie wdrażania przepisów nowego uKSC.

Powyższe oznacza, że w naszej ocenie wystąpi sytuacja, w której po wejściu w życie przepisów dopiero rozpoczną się prace na wieloma szczegółowymi, a jednocześnie kluczowymi dla realizacji wdrożeń zagadnieniami. Będą one jednocześnie konsumować – i tak zbyt krótki – czas na wdrożenie wymagań. Dlatego należy przewidzieć odpowiednio

[3] https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/22f960219fff11ef9db2c9aaf9c67042?jfwid=l7s3186g7https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/22f960219fff11ef9db2c9aaf9c67042?jfwid=l7s3186g7



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

długi czas na dostosowanie, który pozwoli skompensować czasochłonność prac koniecznych do podjęcia po wejściu w życie przepisów.

**Poprawka nr 2**

W art. 1:

1) w pkt 55 w lit a tiret drugie w dodawanym pkt 8 wyrazy „art. 67b ust. 15" zastąpić wyrazami „art. 67b ust. 14";
2) w pkt 75 w lit. d w dodawanych punktach 7 i 8 wyrazy „art. 67b ust. 13" zastąpić wyrazami „art. 67b ust. 12";
3) w art. 1 w pkt 76 w dodawanym art. 67b:
   a) w ust. 1 wyrazy „które są" zastąpić wyrazami „które zostały wskazane jako krytyczne produkty ICT, usługi ICT lub produkty ICT przez Komisję Europejską zgodnie z art. 22 ust. 2 dyrektywy 2022/2555",
   b) ust. 2 nadać brzmienie:
      „2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.",
   c) skreślić ust. 4,
   d) w ust. 10 skreślić zdanie czwarte,
   e) ust. 11 pkt 2 nadać brzmienie:
      „2) ukrytych podatności lub umyślnie stworzonych luk w produktach ICT, usługach ICT lub procesach ICT, które zostały wskazane jako krytyczne przez Komisję Europejską zgodnie z art. 22 ust. 2 dyrektywy 2022/2555;",
   f) w ust. 15 po wyrazach „procesów ICT, " dodaje się wyrazy „które zostały wskazane jako krytyczne przez Komisję Europejską zgodnie z art. 22 ust. 2 dyrektywy 2022/2555";
4) w dodawanym art. 67c:
   a) w ust. 1 we wprowadzeniu do wyliczenia oraz w pkt 2 wyrazy „art. 67b ust. 15" zastąpić wyrazami „art. 67b ust. 14",
   b) skreślić ust. 2,
   c) w ust. 3 skreślić wyrazy „oraz w ust. 2",
   d) w ust. 4 wyrazy „art. 67b ust. 15" zastąpić wyrazami „art. 67b ust. 14",
   e) w ust. 5 wyrazy „art. 67b ust. 15" zastąpić wyrazami „art. 67b ust. 14";



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

5) w dodawanych art. 67d w ust. 1 i ust. 3 pkt 2, w dodawanym art. 67e ust. 1, w dodawanym 2 art. 67f, dodawanym art. 67j ust. oraz art. 17 w pkt 2 w dodawanym pkt 19 wyrazy „art. 67b ust. 15" zastąpić wyrazami „art. 67b ust. 14".

UZASADNIENIE

**a) Dostosowanie do standardów europejskich**

Obecny projekt zmienia katalog dostawców wysokiego ryzyka w oparciu m.in. o kryterium pochodzenia. Proponuje się raczej odwołanie do unijnego wzorca – oceny konkretnych „krytycznych" usług, systemów i produktów ICT wskazanych przez Komisję Europejską i ENISA w myśl art. 22 ust. 2 dyrektywy NIS2. Taka zmiana zapewni spójność z unijnym podejściem opartym na analizie luk i podatności technicznych zamiast arbitralnego kryterium narodowości. Podkreślenia wymaga unikanie tzw. goldplatingu – nakładania nadmiernych wymagań nieprzewidzianych w dyrektywie NIS2. Docelowa ustawa powinna obejmować tylko te rozwiązania, które wynikają z bezpośrednich zobowiązań europejskich (np. uwzględnienie 5G Toolbox), aby nie naruszać zasady proporcjonalności i uniknąć zbędnych obciążeń dla operatorów.

**b) Zapewnienie sprawiedliwej procedury administracyjnej**

Procedura uznania dostawcy za wysokiego ryzyka powinna być prowadzona według ogólnych zasad prawa administracyjnego i konstytucyjnych standardów postępowania. Oznacza to zagwarantowanie stronie prawa do obrony, jawnego rozstrzygania sprawy przez niezależny organ oraz możliwości odwołania – co wynika z art. 2 konstytucji RP (zasada państwa prawnego) oraz prawa do sprawiedliwego rozpatrzenia sprawy. Rzecznik Praw Obywatelskich w toku prac nad UC32 zwracał uwagę na konieczność respektowania prawa do uczciwego procesu administracyjnego. W związku z tym proponuje się, by projektowane regulacje umożliwiały rozpoczęcie procedury po uprzednim zawiadomieniu i przedstawieniu dowodów – zapewniając pełne prawa podmiotów uczestniczących (por. uwagi RPO do projektu UC32). Taka korekta usunie wątpliwości co do zgodności ustawy z Konstytucją (art. 2 Konstytucji, który gwarantuje sprawiedliwość proceduralną oraz art. 45 gwarantuje prawo do rzetelnego rozpatrzenia sprawy przez właściwy, niezawisły organ)

**c) Usunięcie kryteriów pochodzeniowych na rzecz luk technicznych**

Obecna regulacja sugeruje automatyczne uznawanie dostawców spoza UE/NATO za „wysokiego ryzyka", co jest nieprecyzyjne i może kolidować z międzynarodowymi zobowiązaniami Polski (np. zasadami niedyskryminacji handlowej). Zaleca się zastąpienie



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

tych kryteriów faktycznymi lukami bezpieczeństwa wykrytymi w produktach ICT. Taki kierunek odpowiada unijnym rekomendacjom (np. 5G Toolbox) i zapewnia większą pewność prawa. Dzięki skupieniu się na konkretnych podatnościach (np. zaistniałych w sprzęcie od producentów zidentyfikowanych jako krytyczne zgodnie z art. 22 ust. 2 NIS2) uniknie się uznaniowości. Pozwoli to też realizować zasadę proporcjonalności – możliwa będzie selektywna reakcja na realne zagrożenia, zamiast generalnego zakazu. W efekcie zmniejszy się ryzyko naruszenia międzynarodowych zobowiązań (w tym reguł Światowej Organizacji Handlu) przez obywatelstwo czy pochodzenie towaru. Podkreślenia wymaga, że eksperci (jak prof. Piotrowski) ocenili, iż obecne propozycje zawierają rozwiązania budzące wątpliwości prawne – ich eliminacja zwiększy przejrzystość i zgodność norm z konstytucją oraz prawem UE

**d) Zmiany redakcyjne**

Skutkiem przyjęcia poprawki będzie zmiana numeracji ustępów 5-19 - poprawka wskazuje na niezbędne zmiany wynikowe w związku z odwołaniami do tych jednostek redakcyjnych.

**POPRAWKA nr 3:**

W art. 1:

1) w pkt 16 w nowelizowanym art. 8 w ust. 3 wyrazy „nr 4" zastąpić wyrazami „nr 3";
2) w pkt 90 skreślić wyrazy „i 4".

Skreślić dodawany do ustawy Załącznik nr 3 i dotychczasowy załącznik nr 4 oznaczyć jako „Załącznik nr 3".

UZASADNIENIE

Poprawka ma na celu usunięcie z ustawy dotychczasowego Załącznika nr 3, który określa funkcje krytyczne, jednak w sposób niespójny z 5G Toolbox. Obecny projekt nowelizacji wprowadza w Załączniku nr 3 katalog funkcji krytycznych sieci telekomunikacyjnych, który jednak znacząco wykracza poza zalecenia unijnego „5G Toolbox". Jak wskazują analizy, w tym raport gold-plating przygotowany przez inicjatywę SprawdzaMy, polski katalog „nie odzwierciedla krytycznych zasobów zidentyfikowanych w 5G Toolbox" i nakłada obowiązek wycofywania sprzętu bez uwzględnienia jego rzeczywistej krytyczności. Dodatkowo projekt rozszerza zastosowanie tych zasad „na wszystkie sektory gospodarki objęte ustawą i wszystkie komponenty ICT" – w praktyce obejmując sieci 3G, 4G, 5G oraz sieć stacjonarną. Taki zakres wykracza poza założenia 5G Toolbox (który dotyczy



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

wyłącznie bezpieczeństwa sieci 5G) i generuje niepotrzebne koszty oraz ryzyko pogorszenia sytuacji przedsiębiorców w Polsce w porównaniu z podmiotami w innych państwach członkowskich UE. W związku z wprowadzeniem odniesienia do procedury uznawania procesów ICT, produktów ICT lub usług ICT za krytyczne przez Komisję Europejską w porozumieniu z ENISA, Załącznik nr 3 mógłby okazać się niespójny z decyzjami wydanymi na podstawie z art. 22 ust. 2 dyrektywy 2022/2555, stąd, dla uniknięcia niezgodności, proponuje się jego usunięcie i wprowadzenia niezbędnych zmian wynikowych.

***KL/578/201/AM/2025***



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