LEWIATAN

Warszawa, 20 lutego 2026 r.
KL/130/36/AM/2026

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Ministrze,

w związku z zaproszeniem Konfederacji Lewiatan do udziału w konsultacjach tzw. pakietu cyberbezpieczeństwa, na który składają się projekt rozporządzenia w sprawie unijnego aktu o cyberbezpieczeństwie oraz projekt dyrektywy w sprawie środków upraszczających i dostosowania do Aktu o cyberbezpieczeństwie, Konfederacja Lewiatan, w załączeniu, przesyła stanowisko do pakietu.

Z poważaniem

Marek Górski
Prezydent Konfederacji Lewiatan

Do wiadomości
Pan Łukasz Wysocki – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik: Stanowisko Konfederacji Lewiatan do tzw. pakietu cyberbezpieczeństwa

LEWIATAN

Stanowisko Konfederacji Lewiatan wobec tzw. pakietu cyberbezpieczeństwa

W związku z przedstawieniem do konsultacji kolejnego pakietu przepisów dot. cyberbezpieczeństwa przekazujemy poniższe stanowisko wstępne. Sygnalizujemy jednocześnie, że wciąż trwają analizy wpływu procedowanych projektów, także w korelacji z już wprowadzanymi/wprowadzonymi rozwiązaniami. Stąd zastrzegamy możliwość uzupełniania niniejszej opinii w terminie późniejszym.

1. **Otoczenie prawne obszaru bezpieczeństwa staje się zbyt skomplikowane mimo deklaracji jego upraszczania**

Bezpieczeństwo usług w najważniejszych sektorach nabiera coraz większego znaczenia. Wynika to przede wszystkim ze zmian krajobrazu zagrożeń oraz zakresu wykorzystania i wpływu niektórych infrastruktur i usług, szczególnie w najważniejszych sektorach.
Zrozumiała jest odpowiedź regulacyjna, która ma dostosowywać poziom wymagań do nowego otoczenia i oczekiwań. Niesie ona też pozytywną standaryzację i zrozumiałość wymagań.
Z perspektywy podmiotów objętych tymi wymaganiami samo analizowanie i adresowanie wymagań bezpieczeństwa, czy samo śledzenie ich zmian staje się jednak coraz większym obciążeniem, które wymaga utrzymania dedykowanych zasobów. Dyrektywy NIS2 i CER są dopiero wdrażane, a tylko na przełomie 2025/2026 pojawiły się nowe: zmiana NIS2 w zakresie raportowania, nowe CSA, zapowiedź schematów certyfikacji dla usług zarządzanych cyberbezpieczeństwa, celowana zmiana NIS2, DNA (dla komunikacji elektronicznej) i szereg dokumentów „miękkich" dot. bezpieczeństwa dronowego, kabli podmorskich, łańcucha dostaw ICT. Część z nich zapowiada już kolejne uszczegółowienia tematyczne w aktach wykonawczych, planach lub rekomendacjach.
Tymczasem podmioty krajowe (i zapewne wiele europejskich) powinny skupiać się aktualnie na właściwym wdrożeniu implementacji NIS2 i CER. Tymczasem zmiany NIS2, które ogłaszane są jako uproszczenia są albo spóźnione, albo grożą dodatkowymi kosztami i komplikacjami.
W pierwszej kolejności przewidziane przeniesienie raportowania na poziom europejski (Digital Ombibus – zmiana NIS2) może spowodować, że krajowe podmioty po dostosowaniu się do raportowania w S46 będą musiały ponownie dostosowywać się do raportowania do pojedynczego punktu raportowego. Utrzymanie takiego „uproszczenia" w zaprezentowanym kształcie może okazać się *de facto* komplikacją.
W drugiej kolejności, zmiany NIS2 i CSA mają przynieść impulsy dla wypracowania narzędzi certyfikacyjnych upraszczających wykazywanie zgodności z przepisami dot. cyberbezpieczeństwa. To oczywiście pozytywna próba zaadresowania skomplikowanego systemu wymagań. Ma ona też potencjał dla uproszczenia mechanizmów wzajemnego potwierdzania zgodności na poziomie audytów, kontroli czy w łańcuchu dostaw. Są one jednak zdecydowanie spóźnione. Obserwując dotychczasową dynamikę prac nad schematami unijnymi należy założyć, że wypracowanie takiego schematu potrwa co najmniej kilka lat. Pojawi się on już o wiele później niż podmioty będą musiały same wypracować mechanizmy potwierdzania zgodności. Tym samym szacowane oszczędności z tego tytułu są bardzo dyskusyjne. Co więcej, wprowadzenie schematów certyfikacyjnych może oznaczać, że staną się one obowiązkowe, a jednocześnie przyjęta praktyka nie jest z nimi spójna na poziomie ułatwiającym łatwe wykorzystanie dotychczasowego dorobku. W tym ujęciu narzędzie upraszczające może okazać się dodatkowym kosztem.

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

Oceniając więc ogólnie zaprezentowane mechanizmy mające upraszczać ekosystem regulacji cyberbezpieczeństwa musimy jednoznacznie ocenić, że nie niosą one dla nas wartości, która byłaby realnie możliwa do wykorzystania w trwających procesach dostosowawczych. Co więcej, powodują, że krajowe przepisy będą musiały zostać wkrótce znowelizowane, co może powodować ich zmiany niemożliwe dzisiaj do przewidzenia.
Musimy również wskazać, że wymaga to wysiłku organizacji, który wydaje się, że mógłby być lepiej wykorzystany, jeśli firmy mogłyby skupić się na jak najlepszym wdrożeniu jasnego zestawu wymagań dla zarządzania bezpieczeństwem teleinformatycznym swoich organizacji.

2. Przeszacowanie redukcji kosztów i jej nieadekwatność wobec większości podmiotów

Oszacowano, że redukcja kosztów „zgodnościowych" to aż 14,6 mld EUR przez 5 lat – "*The generated benefits of the proposed initiative, as analysed in the Impact Assessment will be significant with up to EUR 14.6 billion of cost savings for businesses*.". Jest to imponująca liczba, która jednak ma niewiele wspólnego z realnymi korzyściami dla większości z funkcjonujących podmiotów. Składa się bowiem na nią przede wszystkim oszacowanie kosztów, których miałyby nie ponieść podmioty wyłączane z NIS2 (14,5 mld EUR). Mogły one je i tak ponieść z uwagi na to, że krajowe implementacje jeszcze zmiany NIS2 nie przewidziały. W żaden sposób nie ogranicza to jednak kosztów po stronie podmiotów, które wciąż będą musiały NIS2 wdrażać. A samo uproszczenie dot. schematów certyfikacji dla NIS2 to jedynie 30 mln EUR rocznie, które jak wskazaliśmy powyżej jest spóźnione i na koniec dnia może oznaczać wręcz dodatkowe koszty.
Tym samym, dla podmiotów, które będą musiały ponieść koszty NIS2 i CSA planowane zmiany nie mają istotnego znaczenia upraszczającego, a szczególnie takiego, które uzasadniałoby lub równoważyłoby wprowadzanie innych mechanizmów. Odwrotnie wręcz, dla istotnej części rynku nowe przepisy oznaczają przede wszystkim nowe, bardzo kosztowne ryzyka regulacyjne.

3. Konieczność zachowania proporcjonalności, precyzji i utrzymania impetu inwestycyjnego

Odnotowujemy, że część z przewidzianych środków, które miałyby przysługiwać Komisji Europejskiej wchodzi w kompetencje uregulowane lub będące przedmiotem regulacji przynajmniej w części krajów UE. Może jednocześnie dotyczyć bardzo szerokiego zakresu sektorów i wykorzystywanych rozwiązań technicznych. Obawiamy się, że bardzo restrykcyjne środki przyjmowane na poziomie europejskim, z pominięciem specyfiki danego kraju okażą się zbyt ambitne i mogą w efekcie niekorzystnie wpływać na przewidywalność otoczenia inwestycyjnego. Uważamy, że środki dotyczące łańcucha dostaw powinny być ściśle celowane, uwzględniające specyfikę sektora, konkretnego kraju oraz pełne obraz realnego zagrożenia oraz możliwych środków mitygujących zarówno po stronie dostawców, jak i dysponentów oraz władz krajowych. Innymi słowy powinny być środkiem ostatecznym, którego uruchomienie jest wynikiem jednoznacznych przesłanek. Warunki jego wdrożenia, w tym czasowe powinny być jednocześnie realistyczne i możliwe do wdrożenia w sposób, który pozwoli na utrzymanie ciągłości świadczenia usług, ich jakości oraz warunków cenowych dla odbiorców.

4. Rozszerzony mandat ENISy

Z zadowoleniem przyjmujemy wyjaśnienie dotyczące doradczej roli ENISy. Wniosek znacznie rozszerza jednak mandat ENISy, obejmując nadzór transgraniczny, wspólne zespoły kontrolne oraz

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

kompleksową analizę ryzyka dla podmiotów z wielu państw członkowskich. Nadaje on również ENISA status de facto europejskiego organu normalizacyjnego, równoległego do CEN, CENELEC i ETSI, szczególnie w odniesieniu do opracowywania systemów certyfikacji w ramach europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF).
Chociaż popieramy terminy składania uwag i podejmowania decyzji w sprawie systemów kandydujących, narzucenie terminów opracowania certyfikacji lub specyfikacji grozi obniżeniem jakości, wykonalności wdrożenia i wsparcia ze strony przemysłu. Obawiamy się, że ten rozszerzony mandat będzie kolidował z istotną rolą europejskich organizacji normalizacyjnych w kierowaniu opracowywaniem globalnych norm, umożliwiających domniemanie zgodności poprzez normy europejskie oraz harmonizację specyfikacji państw członkowskich UE.
Zalecenie: CSA 2.0 powinno:

i) wyjaśnić doradczą rolę ENISy,
ii) izapewnić, aby europejskie systemy certyfikacji cyberbezpieczeństwa (ramy) opierały się na normach europejskich lub specyfikacjach opracowanych przez europejskie organizacje normalizacyjne (ESO),
iii) umożliwić ENISie opracowywanie tymczasowych specyfikacji technicznych, jeżeli istnieje udokumentowana pilna potrzeba, a ocena potwierdza, że nie istnieją specyfikacje o takim samym lub podobnym zakresie, przy czym specyfikacje ENISA powinny zostać zastąpione normami lub specyfikacjami ESO w ciągu 2 lat,
iv) zapewnić, aby specyfikacje techniczne ENISy nie były sprzeczne z istniejącymi specyfikacjami globalnymi lub specyfikacjami państw członkowskich UE.

5. Bezpieczeństwo ram łańcucha dostaw ICT

Projekt przyznaje Komisji Europejskiej lub dowolnym (trzem) państwom członkowskim uprawnienia do żądania przeprowadzenia oceny ryzyka, w wyniku której kraje, sprzedawcy lub dostawcy mogą zostać sklasyfikowani jako „wysokiego ryzyka". Mechanizm ten budzi kilka poważnych obaw:

- Zbyt szerokie kryteria: Każdy kraj może zostać sklasyfikowany jako kraj wysokiego ryzyka na podstawie takich czynników, jak dostęp organów ścigania do danych, praworządność i stabilność systemu prawnego, co może potencjalnie wpłynąć nawet na zaufanych partnerów handlowych i bezpieczeństwa UE. W art. 100 ust. 1 wymieniono kryteria służące do weryfikacji, czy państwo trzecie stwarza poważne i strukturalne ryzyko nietechniczne, w tym:
  a) przepisy wymagające zgłaszania organom władzy przypadków podatności na zagrożenia;
  b) istniejące praktyki wymagające takiego zgłaszania;
  c) brak skutecznych środków odwoławczych i niezależnych demokratycznych mechanizmów kontroli;
  d) potwierdzone informacje o podmiotach stanowiących zagrożenie; oraz
  e) istotne informacje pochodzące z ocen ryzyka lub sprawozdań. Kryteria te mogą potencjalnie wpłynąć na zaufanych partnerów handlowych i bezpieczeństwa UE, powodując dyskryminację.

Doprecyzowanie stosowania kryteriów w celu określenia relacji dostawcy z krajem budzącym obawy

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

Mechanizm wykorzystywany przez Komisję do sporządzania listy dostawców wysokiego ryzyka, gdy uzna się, że państwo trzecie stwarza zagrożenie dla cyberbezpieczeństwa, jest niejasny. Wydaje się on w dużej mierze zależny od tego, które sektory krytyczne zostały objęte wstępną oceną ryzyka bezpieczeństwa, oraz posługuje się pojęciami wymagającymi bardziej szczegółowego wyjaśnienia. Przykładowo Komisja może stosować następujące kryteria w celu określenia dostawców wysokiego ryzyka:
a. Miejsce siedziby spółki – może to oznaczać lokalizację jej centrali, ale także dowolny kraj, w którym posiada personel lub infrastrukturę.
b. Kontrola przez państwo trzecie – może odnosić się do kontroli wynikającej z obowiązującego prawa w danej jurysdykcji, ale także do innych mechanizmów twardego lub miękkiego wpływu.
c. Obywatele państwa trzeciego – opieranie się na obywatelstwie osób jako gwarancji wiarygodności jest problematyczne. Czy na przykład posiadanie w zarządzie osoby będącej obywatelem państwa trzeciego oznaczałoby uznanie spółki za dostawcę wysokiego ryzyka? Czy status spółki mógłby się zmienić wskutek zatrudnienia takiej osoby? Czy na mocy Artykułu 104 ustęp 4 przedsiębiorstwa będą zobowiązane do przedstawiania wykazów pracowników wraz z ich obywatelstwem?

Uproszczenie ocen państw trzecich poprzez oddzielenie ich od kryteriów sektorowych
Nie jest jasne, dlaczego oceny państw trzecich muszą być przeprowadzane w kontekście konkretnego sektora, skoro większość kryteriów (tj. Artykuł 100 ustęp 1 lit. (a)–(d), z wyjątkiem (e)) nie ma charakteru sektorowego. Prostsze i bardziej efektywne mogłoby być proaktywne ocenianie państw.

- Brak kompleksowej oceny skutków: art. 99 stanowi, że skoordynowane na szczeblu unijnym oceny ryzyka bezpieczeństwa należy przeprowadzić w ciągu sześciu miesięcy, ale nie wymaga kompleksowego przeglądu technicznego konsekwencji przed dokonaniem wyznaczenia na podstawie art. 100. We wniosku nie przewidziano obowiązku przeprowadzania ocen skutków towarzyszących aktom wykonawczym na podstawie art. 100 ust. 2, które wyznaczają państwa trzecie jako stwarzające zagrożenie dla cyberbezpieczeństwa.
- Potencjał dyskryminacyjny: proces ten może osłabić stosunki z państwami trzecimi, które są partnerami UE w dziedzinie handlu, bezpieczeństwa lub obrony.
- Wymogi dotyczące wycofania: sprzęt uznany za wysokiego ryzyka podlegałby obowiązkowemu wycofaniu z infrastruktury UE, co spowodowałoby znaczne koszty wymiany i zakłócenia w łańcuchu dostaw. Nie jest jasne, jak długi byłby okres wycofywania i w jaki sposób KE określi takie wycofywanie oraz jego skutki, np. poprzez ocenę skutków towarzyszącą aktowi wykonawczemu.
- Bezpieczeństwo łańcucha dostaw: Obowiązkowe środki bezpieczeństwa łańcucha dostaw mogą zwiększyć obciążenia związane z zapewnieniem zgodności, ograniczając jednocześnie wybór technologiczny i konkurencyjność. Projekt nie wyjaśnia, w jaki sposób urządzenia, usługi lub towary ICT zostaną oddzielone od łańcucha dostaw UE i co to będzie oznaczać dla konkretnego dostawcy, jeśli jego urządzenia, usługi lub towary są dystrybuowane w infrastrukturze krytycznej w kilku krajach UE. Przykład: Artykuł 103 ust.

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

1 upoważnia Komisję do przyjęcia aktów wykonawczych zakazujących podmiotom wymienionym w załącznikach I i II do dyrektywy (UE) 2022/2555 stosowania komponentów ICT pochodzących od dostawców wysokiego ryzyka określonych w art. 104 w kluczowych zasobach ICT określonych w art. 102. We wniosku brakuje jasności co do procesów oddzielania lub wpływu na dostawców prowadzących działalność w wielu państwach członkowskich.

- Kwestia kompetencji i współpracy między państwami UE a UE: Artykuł 99 ust. 1 pozwala Komisji lub grupie co najmniej trzech państw członkowskich zwrócić się do grupy ds. współpracy w zakresie bezpieczeństwa sieci i informacji o przeprowadzenie skoordynowanej oceny ryzyka bezpieczeństwa na szczeblu unijnym. Artykuł 99 ust. 3 stanowi, że jeżeli Komisja ma wystarczające powody, aby sądzić, że istnieje poważne zagrożenie cybernetyczne, konsultuje się z państwami członkowskimi w sprawie środków łagodzących. Jednak trzy państwa członkowskie wraz z Komisją mogłyby zainicjować wyznaczenia na podstawie art. 100, powodując potencjalne poważne problemy dla innych państw członkowskich – podważając zasadę, że wszystkie kraje UE powinny mieć znaczący wpływ na decyzje dotyczące ich bezpieczeństwa narodowego, obrony, zamówień publicznych i infrastruktury krytycznej.
- Aspekty prawne, proceduralne i nadzorcze wyznaczenia: Projekt przyznaje Komisji Europejskiej lub dowolnym trzem państwom członkowskim uprawnienia do żądania przeprowadzenia oceny ryzyka klasyfikującej kraje, sprzedawców lub dostawców jako „wysokiego ryzyka". Budzi to poważne obawy dotyczące demokratycznej kontroli i ochrony państw członkowskich. Czy takie oznaczenie (dokonywane za pomocą aktów wykonawczych, a więc poza zwykłym procesem legislacyjnym) będzie miało skutek ex ante, ex post, czy też oba te skutki? Jakie są dokładne powiązania między oznaczeniem kraju, dostawcy wysokiego ryzyka oraz urządzenia/usługi?
- **Konsultacje z dostawcami wysokiego ryzyka przed nałożeniem ograniczeń** Komisja i/lub Grupa Współpracy NIS mogą wyznaczyć dostawcę jako podmiot wysokiego ryzyka w trakcie prowadzenia i publikowania oceny ryzyka bezpieczeństwa, bez szczegółowych kryteriów przewodnich. Proponowane CSA 2.0, Artykuł 103 ustęp 2 (a)-(f), upoważnia następnie Komisję do wprowadzania bardzo szczegółowych przepisów dotyczących sposobu, w jaki podmioty z sektorów krytycznych muszą ograniczać ryzyka związane z dostawcami wysokiego ryzyka, na przykład poprzez zakaz korzystania ze zdalnego przetwarzania danych. Stwarza to możliwość uznania dostawców za wysokiego ryzyka i nałożenia ograniczeń na korzystanie z ich usług z przyczyn nietechnicznych, nawet przy braku powiązań dostawcy z krajem budzącym obawy. Należy wprowadzić mechanizm przewidujący konsultacje z dostawcami przed uznaniem ich za podmioty wysokiego ryzyka, aby umożliwić zrozumienie obaw Komisji oraz przedstawienie propozycji satysfakcjonujących środków ograniczających ryzyko przed publikacją aktu wykonawczego przez Komisję zgodnie z Artykułem 103 ustęp 1.
- **Doprecyzowanie potrzeby i zakresu ocen ryzyka bezpieczeństwa prowadzonych przez Komisję**
  Artykuł 99 przewiduje, że oceny ryzyka bezpieczeństwa mogą być przeprowadzane przez (a) Grupę Współpracy NIS lub (b) Komisję (w konsultacji z państwami członkowskimi). Wydaje się, że Komisja nie jest zobowiązana do koncentrowania się na krytycznych usługach, systemach, produktach ICT lub łańcuchach dostaw, podczas gdy Grupa

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

Współpracy NIS jest do tego zobowiązana. Wyjaśnienie, dlaczego konieczne są dwa odrębne mechanizmy przeprowadzania ocen ryzyka bezpieczeństwa, pomogłoby podmiotom wdrażającym zrozumieć, czy zakres ocen Komisji obejmie również usługi, systemy, produkty i łańcuchy dostaw o charakterze niekrytycznym.

- **Jasne zdefiniowanie aktywnego wykorzystania jako działania złośliwego** Artykuł 100 zawiera kryteria, które wymagają od podmiotów zgłaszania podatności zanim zostaną one uznane za wykorzystane. CSA powinno kwalifikować takie wykorzystanie jako złośliwe – w taki sam sposób, jak czyni to CRA w sekcji definicji w Artykule 3 – w przeciwnym razie dowody koncepcyjne (proof-of-concept), powszechnie opracowywane przez badaczy bezpieczeństwa w celu weryfikacji podatności, mogą zostać zinterpretowane jako aktywne wykorzystanie. W obecnym brzmieniu państwa trzecie mogłyby obejść kryteria CSA 2.0, wymagając jedynie, by zgłoszenia podatności zawierały dowód koncepcyjny (który obecny projekt CSA 2.0 mógłby interpretować jako przypadek aktywnego wykorzystania).

Zalecenie: Środki bezpieczeństwa łańcucha dostaw powinny pozostać dobrowolne, a jeśli zostaną wprowadzone jako obowiązkowe, muszą być zrównoważone potrzebą wspierania wdrażania technologii i wyboru oraz konkurencyjności UE, przy jednoczesnym poszanowaniu priorytetów bezpieczeństwa i łańcucha dostaw poszczególnych krajów. Każdy proces klasyfikacji dostawców jako wysokiego ryzyka musi obejmować kompleksowe oceny wpływu technicznego, znaczące zaangażowanie wszystkich zainteresowanych państw członkowskich oraz poszanowanie kompetencji krajowych. Środki bezpieczeństwa łańcucha dostaw powinny pozostać dobrowolne lub, jeśli są obowiązkowe, muszą być zrównoważone z przyjęciem technologii, konkurencyjnością UE i priorytetami bezpieczeństwa narodowego.

6. Uprawnienia Komisji Europejskiej a kompetencje państw członkowskich

Projekt powoduje niespójność między kompetencjami UE a kompetencjami państw członkowskich. Podczas gdy państwa członkowskie zachowują swobodę decydowania o tym, które sektory uwzględnić, Komisja zyskuje znaczne uprawnienia w zakresie technicznych i nietechnicznych kryteriów ryzyka. Budzi to obawy dotyczące:

- Spójności regulacyjnej: potencjalnych konfliktów z innymi inicjatywami UE, takimi jak ustawa o przyspieszeniu rozwoju przemysłu, która promuje opłacalne zakupy sprzętu.
- Obciążenia związane z zapewnieniem zgodności: pomimo dążenia do uproszczenia, wniosek wprowadza nowe uprawnienia w zakresie kontroli i oceny, które zwiększają, a nie zmniejszają wymogi administracyjne.
- Odpowiedzialność demokratyczna: równowaga między uprawnieniami Komisji a suwerennością państw członkowskich w zakresie decyzji dotyczących infrastruktury krytycznej.

7. Przyjęcie systemu certyfikacji

Wniosek ma na celu harmonizację certyfikacji w zakresie cyberbezpieczeństwa poprzez europejskie ramy certyfikacji cyberbezpieczeństwa (ECCF), zastępujące systemy krajowe. Jednakże KE uznała również we wstępie do CSA 2.0 oraz w ocenie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i europejskich ram certyfikacji w zakresie cyberbezpieczeństwa (ECCF), że doświadczenia

związane z europejskim systemem certyfikacji w zakresie cyberbezpieczeństwa (EUCS) pokazują, w jaki sposób wymogi polityczne i nietechniczne mogą podważać cele jednolitego rynku. Główne obawy obejmują:

- Ogólny proces i mechanizm certyfikacji i ustalania norm: Normy i specyfikacje odnoszą sukces i osiągają swoje cele tylko wtedy, gdy dostawcy i klienci uznają je za wartościowe. To samo dotyczy systemów certyfikacji UE w ramach CSA 2.0. Dobrym przykładem tej propozycji wartości jest harmonizacja zastępująca fragmentaryczne systemy krajowe lub indywidualne akty wykonawcze wymaganiami technicznymi. Artykuł 86 dotyczy krajowych systemów certyfikacji cyberbezpieczeństwa, ale może on zostać rozszerzony na akty wykonawcze KE, takie jak NIS2. Komisja uznała w tekście wprowadzającym CSA 2.0 oraz w ocenie ENISA i ECCF, że doświadczenia EUCS pokazują, w jaki sposób wymogi polityczne i nietechniczne podważają cele jednolitego rynku.
- Powolne wdrażanie: obecnie tylko 13 państw członkowskich wdrożyło części zestawu narzędzi 5G od 2019 r. Wskazuje to na wyzwania związane z wdrażaniem, prawdopodobnie spowodowane niejasną propozycją wartości.
- Niewystarczający czas na opracowanie i brak przejrzystości: organy normalizacyjne (CEN-CENELEC, ETSI) potrzebują odpowiedniego czasu, aby przedstawić fachowe opinie techniczne (jak również podkreślono powyżej). Artykuł 74 ust. 1 stanowi, że ENISA przygotowuje projekt systemu w ciągu 12 miesięcy od otrzymania wniosku Komisji, ale normalizacja wymaga odpowiedniego czasu, aby eksperci mogli przedstawić opinie techniczne. Należy zauważyć, że opóźnienie w przyjęciu europejskiego systemu certyfikacji cyberbezpieczeństwa (EUCS) spowodowane było dyskusjami o charakterze nietechnicznym między Komisją Europejską i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa (ECCG), a nie ze względu na proces techniczny w ramach grupy roboczej ad hoc ENISA ani na poziomie CEN/CENELEC. Wymogi techniczne dotyczące EUCS zostały już przyjęte jako CEN/CENELEC TS 18026 w 2024 r. To właśnie (jak przyznaje również KE) dyskusje polityczne i nietechniczne oraz nieprzejrzysty proces decyzyjny spowodowały opóźnienie w przyjęciu systemu certyfikacji EUCS, z którego korzyści mogłoby skorzystać wiele podmiotów.
- Stosunek ECCF do certyfikacji sektorowej: We wniosku KE wskazano, że certyfikaty opracowane w ramach nowego CSA 2.0 będą miały zastosowanie we wszystkich sektorach i zapewnią zgodność z systemami sektorowymi, takimi jak ustawa o cyberodporności (CRA) lub rozporządzenie w sprawie cyfrowej odporności operacyjnej sektora finansowego (DORA). Artykuł 78 ust. 1 stanowi, że jeżeli przewiduje to konkretny akt prawny Unii, certyfikat wydany w ramach europejskiego systemu certyfikacji cyberbezpieczeństwa wykazuje zgodność i przyznaje domniemanie zgodności z odpowiednimi wymogami określonymi w tym akcie prawnym. Wymaga to dalszych wyjaśnień dotyczących procesu, wycofywania systemów sektorowych zastąpionych przez ECCF, ważności w różnych krajach i podobnych kwestii.

Zalecenie: Systemy certyfikacji muszą pozostać czysto techniczne, wykorzystywać zharmonizowane normy europejskich organizacji normalizacyjnych i zapewniać wystarczającą ilość czasu na przejrzysty, obejmujący całą branżę rozwój, aby zapewnić przyjęcie i wdrożenie przez dostawców zapewniać zaufanie klientów.

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

LEWIATAN

8. Zaangażowanie branży

CSA 2.0 znosi tzw. SCCG (Stakeholders Cybersecurity Certification Group – grupa certyfikacyjna ds. cyberbezpieczeństwa dla zainteresowanych stron) i zastępuje ją „corocznym zgromadzeniem". Komisja Europejska przyznaje jednak, że proces EUCS napotykał pewne trudności, częściowo z powodu braku przejrzystości dla zewnętrznych zainteresowanych stron. Jak podkreślono powyżej, ramy certyfikacji będą miały znaczący wpływ na konkurencyjność i bezpieczeństwo UE, co wymaga, aby systemom certyfikacji towarzyszyła odpowiednia ocena skutków, którą mogą zapewnić odpowiednie zainteresowane strony z branży. Konkurencyjność UE musi być poprawiana wspólnie z przedsiębiorstwami, a nie bez nich. Raport Draghiego z 2025 r. w rozdziale „Nowe ukierunkowanie działań UE" podkreśla, że: [„... W określonych sektorach gospodarki można by rozważyć utworzenie nowej struktury skupiającej Komisję, przemysł i państwa członkowskie, a także odpowiednie agencje sektorowe...".

9. NIS2 i konsekwencje dla infrastruktury krytycznej

Zmiany w dyrektywie NIS2 wprowadzone w ramach wniosku nakładają na operatorów infrastruktury krytycznej nowe wymogi dotyczące zgodności, w tym:

- Obowiązkową migrację do kryptografii postkwantowej (do 2030 r. w przypadku zastosowań krytycznych, do 2035 r. w przypadku zastosowań o średnim/niskim ryzyku).
- Wzmocnione wymogi dotyczące zgłaszania oprogramowania ransomware.
- Nowe kategorie podmiotów o znaczeniu kluczowym, w tym operatorzy podmorskich infrastruktur transmisji danych.

Chociaż środki te odpowiadają na rzeczywiste obawy dotyczące bezpieczeństwa, muszą one być wdrażane w realistycznych terminach i po odpowiednich konsultacjach z branżą, aby uniknąć zakłóceń w zakresie usług podstawowych.

10. Doprecyzowanie składu Europejskiego Zgromadzenia ds. Certyfikacji Cyberbezpieczeństwa (Artykuł 72)

Ustanowienie Europejskiego Zgromadzenia ds. Certyfikacji Cyberbezpieczeństwa na mocy Artykułu 72 postrzegamy jako krok pozytywny. Aby zapewnić, że Zgromadzenie będzie dostarczać merytoryczny, technicznie ugruntowany i reprezentatywny wkład, rekomendujemy, by Rozporządzenie wprost wymieniało odpowiednie kategorie interesariuszy, które mają być reprezentowane, zamiast opierać się wyłącznie na otwartym odniesieniu do „odpowiednich interesariuszy".

Byłoby to spójne z podejściem redakcyjnym przyjętym w Artykule 32(6) dotyczącym doraźnych grup roboczych ENISA. Artykuł 72 mógłby doprecyzować, że w skład Zgromadzenia powinni wchodzić przedstawiciele m.in. dostawców produktów i usług ICT (w tym dostawców usług chmurowych i usług cyfrowych), MŚP, użytkowników i organizacji reprezentujących stronę popytową, jednostek oceny zgodności oraz krajowych jednostek akredytujących na mocy Rozporządzenia (WE) nr 765/2008, europejskich i międzynarodowych organizacji normalizacyjnych, środowisk akademickich i instytucji badawczych, a także organizacji konsumenckich i społeczeństwa obywatelskiego.

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

Takie doprecyzowanie zapewniłoby pewność prawa i równowagę, pomogłoby uniknąć nadreprezentacji lub niedoreprezentowania określonych interesów oraz zagwarantowałoby, że Zgromadzenie będzie funkcjonować jako rzeczywisty mechanizm współpracy publiczno-prywatnej.

Wnioski

CSA 2.0. odpowiada na rzeczywiste wyzwania związane z bezpieczeństwem, przed którymi stoi UE. Jednak osiągnięcie prawdziwej cyberodporności wymaga zrównoważenia celów bezpieczeństwa z utrzymaniem jednolitego rynku, wspieraniem innowacji i zachowaniem partnerstw międzynarodowych. Proces legislacyjny musi zapewnić, aby środki bezpieczeństwa pozostały proporcjonalne, oparte na podstawach technicznych i wspierające konkurencyjność UE w globalnej gospodarce cyfrowej.

KL/130/36/AM/2026

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