Warszawa, 10 czerwca 2025 r.
KL/241/77/AM/2025

Pan **Maciej Berek**
Członek Rady Ministrów
Przewodniczący Komitetu Stałego Rady Ministrów

Pan **Andrzej Domański**
Minister Finansów

Pan **Adam Bodnar**
Minister Sprawiedliwości

Pan **Dariusz Klimczak**
Minister Infrastruktury

Pan **Krzysztof Paszyk**
Minister Rozwoju i Technologii

Pan **Radosław Sikorski**
Minister Spraw Zagranicznych

Pan **Adam Szłapka**
Minister do spraw Unii Europejskiej

oraz do pozostałych członków Komitetu Stałego Rady Ministrów

Szanowny Panie Przewodniczący, Szanowni Panowie Ministrowie,

w związku ze skierowaniem projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (nr z wykazu prac UC32) pismem znak: DP.MC.WL.0211.19.2025 z dnia 29 maja 2025 r. pod obrady Komitetu Stałego Rady Ministrów przedstawiamy w załączeniu stanowisko Konfederacji Lewiatan.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:

1) Pan Piotr Borys, Sekretarz Stanu, Ministerstwo Sportu i Turystyki
2) Pani Aleksandra Gajewska, Sekretarz Stanu, Ministerstwo Rodziny, Pracy i Polityki Społecznej
3) Pan Jan Grabiec, Minister, Szef Kancelarii Prezesa Rady Ministrów, Kancelaria Prezesa Rady Ministrów
4) Pan Marek Gzik, Sekretarz Stanu, Ministerstwo Nauki i Szkolnictwa Wyższego
5) Pan Jacek Karnowski, Sekretarz Stanu, Ministerstwo Funduszy i Polityki Regionalnej
6) Pan Marcin Kierwiński, Minister, Członek Rady Ministrów, Kancelaria Prezesa Rady Ministrów
7) Pan Wojciech Konieczny, Sekretarz Stanu, Ministerstwo Zdrowia
8) Pani Katarzyna Kotula, Ministra do spraw Równości
9) Pan Stefan Krajewski, Sekretarz Stanu, Ministerstwo Rolnictwa i Rozwoju Wsi
10) Pan Robert Kropiwnicki, Sekretarz Stanu, Ministerstwo Aktywów Państwowych
11) Pani Katarzyna Lubnauer, Sekretarz Stanu, Ministerstwo Edukacji
12) Pani Marzena Okła-Drewnowicz, Minister do spraw Polityki Senioralnej
13) Pani Adriana Porowska, Ministra do spraw Społeczeństwa Obywatelskiego
14) Pan Dariusz Standerski, Sekretarz Stanu, Ministerstwo Cyfryzacji
15) Pan Tomasz Szymański, Sekretarz Stanu, Ministerstwo Spraw Wewnętrznych i Administracji
16) Pan Cezary Tomczyk, Sekretarz Stanu, Ministerstwo Obrony Narodowej
17) Pan Wojciech Wrochna, Sekretarz Stanu, Ministerstwo Przemysłu
18) Pani Urszula Zielińska, Sekretarz Stanu, Ministerstwo Klimatu i Środowiska
19) Pani Bożena Żelazowska, Sekretarz Stanu, Ministerstwo Kultury i Dziedzictwa Narodowego

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 w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (nr z wykazu prac UC32)

I. Wprowadzenie

W epoce cyfrowej transformacji, cyberbezpieczeństwo stanowi fundament stabilności gospodarczej i zaufania publicznego. Środowisko polskich przedsiębiorców z pełnym przekonaniem wspiera dążenie do budowy odpornego i bezpiecznego ekosystemu cyfrowego. Z tym większym niepokojem obserwujemy jednak głęboki dysonans pomiędzy szczytnym celem projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (UC32) a jego realną treścią i formą legislacyjną. Zamiast tworzyć ramy dla partnerskiej współpracy i innowacji w dziedzinie bezpieczeństwa, projekt w obecnym kształcie ustanawia paradygmat regulacyjny oparty na nadmiernej ingerencji państwa, niepewności prawnej i nieproporcjonalnych obciążeniach, które w ostatecznym rozrachunku osłabią, a nie wzmocnią, polską gospodarkę – co trafnie podkreślono w ramach inicjatywy deregulacji SPRAWDZAMY.TO.

Nasza krytyczna ocena nie jest odosobnionym głosem. Znajduje ona pełne odzwierciedlenie w licznych zastrzeżeniach zgłaszanych na przestrzeni ostatnich miesięcy przez kluczowe instytucje państwowe, w tym Ministerstwo Rozwoju i Technologii, Ministerstwo Finansów, Ministerstwo Sprawiedliwości, Rządowe Centrum Legislacji, Rzecznika Praw Obywatelskich, a nawet Europejski Bank Centralny. Ta bezprecedensowa zbieżność krytycznych opinii ze strony tak szerokiego spektrum organów dowodzi, że projekt obarczony jest fundamentalnymi wadami konstrukcyjnymi.

W niniejszym stanowisku przedstawiamy szczegółową analizę tych wad, koncentrując się na kluczowych obszarach ryzyka. Obejmują one błędy w technice prawodawczej, systemową nadregulację (*gold-plating*) podważającą konkurencyjność polskich firm na jednolitym rynku, wprowadzenie arbitralnych i destabilizujących mechanizmów rynkowych, a także bezprecedensowy demontaż gwarancji prawnych dla przedsiębiorców. Wskazujemy również na chaos budżetowy i proceduralny, w tym brak notyfikacji technicznej TRIS, który grozi bezskutecznością całej regulacji.

Jesteśmy gotowi do merytorycznej współpracy w procesie tworzenia dobrych i skutecznych ram prawnych dla cyberbezpieczeństwa w Polsce. Wierzymy, że bezpieczeństwo można budować w oparciu o zasady proporcjonalności, pewności prawa i partnerstwa. Dalsze procedowanie obecnego projektu ustawy, wbrew tak licznym i fundamentalnym głosom krytycznym, byłoby jednak działaniem na szkodę polskiego państwa i jego gospodarki.

Pozytywnie oceniamy również szereg zmian wprowadzonych na ostatnim etapie, takich jak wydłużenie obowiązków audytów, zmiany w zakresie klasyfikacji podmiotów ważnych i kluczowych i inne.

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

Biorąc jednak pod uwagę powyższe, fundamentalne i wieloaspektowe wady projektu ustawy, szczegółowe wskazane w części szczegółowej, które podzielają kluczowe organy administracji rządowej, Konfederacja Lewiatan wnosi o:

1. Rozpoczęcie prac nad całkowicie nową ustawą o krajowym systemie cyberbezpieczeństwa, która będzie spójna, przejrzysta i zgodna z Zasadami techniki prawodawczej.

2. Oparcie nowej regulacji na zasadzie proporcjonalności i odrzucenie idei gold-platingu. Nowe przepisy powinny implementować wymogi dyrektywy NIS 2, nie nakładając dodatkowych, nieuzasadnionych obciążeń.

3. Zagwarantowanie poszanowania praw przedsiębiorców, w tym utrzymanie istniejących mechanizmów ochronnych dotyczących kontroli działalności gospodarczej.

4. Opracowanie transparentnej, opartej na obiektywnych kryteriach i gwarantującej prawo do skutecznej obrony procedury oceny dostawców, która nie będzie szkodzić konkurencji i innowacyjności.

II. Uwagi szczegółowe

2.1. Konieczność opracowania nowej ustawy, a nie nowelizacji

W pełni podzielamy stanowisko Ministra Sprawiedliwości, który w swojej opinii słusznie zauważa, że *„liczba wprowadzanych zmian negatywnie wpływa na konstrukcję i spójność nowelizowanej ustawy”*[1]. Projektowana regulacja nie jest drobną korektą, lecz rewolucją, która dotyka fundamentalnych pojęć i instytucji. Zgodnie z § 84 Zasad techniki prawodawczej[2], tak głęboka ingerencja w materię ustawy powinna skutkować opracowaniem projektu zupełnie nowej ustawy analogicznie do sposobu, w jaki ustawę Prawo telekomunikacyjne zastąpiono nowym Prawem Komunikacji Elektronicznej (dokładnie tak samo jak dyrektywę NIS1 zastępuje NIS2). Forsowanie tak obszernej nowelizacji zamiast przygotowania nowego, spójnego aktu prawnego prowadzi bezpośrednio do braku przejrzystości, chaosu prawnego oraz ryzyka wewnętrznych sprzeczności, które będą źródłem sporów interpretacyjnych i niepewności prawnej po stronie przedsiębiorców.

2.2. Gold-plating i nieproporcjonalna ingerencja w swobodę gospodarczą

[1] Tak pismo Ministerstwa Sprawiedliwości znak: L-VIII.454.247.2024 z 22.10.2024 r.
[2] Załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie "Zasad techniki prawodawczej" (t.j. Dz. U. z 2016 r. poz. 283).

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

Projekt ustawy, pomimo kilku korzystnych zmian wprowadzonych przed Komitetem Stałym Rady Ministrów, stanowi podręcznikowy przykład tzw. **gold-platingu**, czyli nakładania na przedsiębiorców obowiązków znacznie wykraczających poza minimum wymagane przez dyrektywę NIS 2. Jak zdefiniowano w raporcie inicjatywy SprawdzaMY[3], gold-plating to sytuacja, w której *„prawodawca krajowy w ramach lub przy okazji wdrażania prawa UE – wprowadza nowe, dodatkowe lub dalej idące regulacje, które nie są niezbędne dla implementacji przepisów unijnych”*[4]. Potwierdza to raport firmy doradczej EY pt. *„Implementacja Dyrektywy NIS2 w Polsce na tle wybranych państw UE”*[5], który wprost wskazuje, że Polska przyjmuje jedno z najbardziej rygorystycznych stanowisk w Unii Europejskiej, wprowadzając rozwiązania stanowiące nadregulację. Skutkiem jest sytuacja, w której polskie podmioty będą podlegały surowszym wymogom niż ich konkurenci z innych państw europejskich , co prowadzi do fragmentacji rynku wewnętrznego i osłabienia ich pozycji.

Przejawami tej tendencji są m.in.:

- **arbitralne rozszerzenie katalogu sektorów kluczowych -** analiza najnowszej wersji projektu ustawy, w szczególności jej załączników, wskazuje, że część pierwotnych obaw dotyczących masowego przenoszenia całych sektorów z kategorii "ważnych" do "kluczowych" została częściowo zaadresowana. Sektory takie jak produkcja, wytwarzanie i dystrybucja chemikaliów, produkcja, przetwarzanie i dystrybucja żywności oraz ogólna produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro zostały w projekcie (Załącznik nr 2) finalnie sklasyfikowane jako sektory ważne. Jest to zgodne z podziałem przyjętym w Załączniku II do Dyrektywy NIS2 i stanowi pozytywną zmianę w stosunku do wcześniejszych wersji projektu.

  Niemniej, problematyka gold-platingu w tym obszarze nie zniknęła, a jedynie zmieniła swój charakter. Zamiast przenoszenia całych sektorów, projektodawca zdecydował się na bardziej selektywne, ale wciąż nieuzasadnione dyrektywą, rozszerzenie katalogu podmiotów kluczowych. Przykładem jest podsektor ochrony zdrowia, gdzie do kategorii podmiotów kluczowych (Załącznik nr 1) zaliczono:
  - Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego.

  Dyrektywa NIS2 w Załączniku I (sektory kluczowe) również wymienia tę kategorię, jednak polski projekt idzie dalej, dodając do sektora kluczowego również:
  - Przedsiębiorcę prowadzącego działalność polegającą na prowadzeniu hurtowni farmaceutycznej,
  - Przedsiębiorcę prowadzącego działalność w formie apteki ogólnodostępnej,

[3] Raport dostępny na stronie: SprawdzaMY.com - Deregulacja i Lepsze Prawo dla Polski
[4] Por. str. 7 tego raportu.
[5] ey_law_goldplating_nis2.pdf

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

- Wytwórców, importerów oraz dystrybutorów substancji czynnych i produktów leczniczych.

Wszystkie te kategorie podmiotów nie są wprost wymienione jako "kluczowe" w Dyrektywie NIS2. Ta z pozoru techniczna zmiana, polegająca na podniesieniu statusu wybranych grup podmiotów, niesie za sobą poważne konsekwencje. Zgodnie z logiką dyrektywy, podmioty kluczowe podlegają znacznie bardziej rygorystycznemu i proaktywnemu nadzorowi, co wiąże się z surowszymi wymaganiami oraz wyższymi kosztami, m.in. w zakresie obowiązkowych audytów i implementacji środków bezpieczeństwa. Takie wybiórcze zaostrzanie wymogów dla określonych uczestników rynku, wykraczające poza unijne minimum, stanowi formę nadregulacji, która może w sposób nieproporcjonalny obciążyć te podmioty i zaburzyć ich konkurencyjność względem odpowiedników w innych państwach członkowskich.

- **drastycznie zaostrzone kary** - projekt wprowadza dodatkową karę pieniężną w wysokości **aż do 100 mln zł** za stworzenie zagrożenia dla bezpieczeństwa państwa. Jest to sankcja znacznie surowsza niż przewidziana w NIS2, oparta na niedookreślonych i ocennych przesłankach.

2.3. Procedura uznania za dostawcę wysokiego ryzyka (HRV) - brak uzasadnienia dla tak szerokiego jej zakresu

Szczególny sprzeciw budzi procedura HRV (art. 67a-67k), której wprowadzenie jest kolejnym, jaskrawym przykładem gold-platingu. Jak podkreślają raporty EY oraz SprawdzaMY, instytucja ta **pochodzi z niewiążących zaleceń (tzw. 5G Toolbox), a nie z tekstu samej dyrektywy NIS 2**. Co więcej, Polska **jako jedyny kraj w Europie** rozszerza jej zastosowanie na wszystkie 18 sektorów gospodarki, a nie tylko na krytyczne elementy sieci 5G. Jak wskazano w raporcie, projekt ustawy *„rozszerzył jej zastosowanie na wszystkie sektory gospodarki objęte projektowaną ustawą i wszystkie komponenty ICT”*. Oznacza to, że procedura HRV obejmie nie tylko telekomunikację, ale łącznie 18 kluczowych sektorów gospodarki – od energetyki i bankowości, po opiekę zdrowotną, produkcję żywności czy gospodarkę odpadami. Co więcej, dotyczyć będzie każdego elementu systemów informatycznych, a nie tylko infrastruktury krytycznej.

2.3.1. Naruszenie unijnej zasady skoordynowanej oceny ryzyka

Fundamentalną wadą procedury HRV, która podważa jej legalność i proporcjonalność, jest całkowite zignorowanie przez projektodawcę unijnego mechanizmu skoordynowanej oceny ryzyka, opisanego w **art. 22 oraz motywie 90 dyrektywy NIS2**.
Zgodnie z tymi przepisami, środki zarządzania ryzykiem w łańcuchu dostaw – zwłaszcza tak daleko idące jak wykluczenie dostawcy – powinny być stosowane wyłącznie do tych usług, systemów lub produktów ICT, które zostały uprzednio **zidentyfikowane jako krytyczne w ramach ogólnounijnej, skoordynowanej oceny ryzyka**. Co kluczowe, art. 22 ust. 2 NIS2 jednoznacznie wskazuje, że to **Komisja Europejska** (po konsultacjach z Grupą Współpracy i

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

ENISA), a nie pojedyncze państwo członkowskie, jest władna wskazać konkretne krytyczne usługi, systemy lub produkty ICT, które mogą być poddane takiej ocenie.
Do dnia dzisiejszego jedyna skoordynowana ocena ryzyka, która zakończyła się identyfikacją krytycznych elementów, została przeprowadzona **wyłącznie dla sektora telekomunikacji w zakresie sieci 5G** (w ramach tzw. 5G Toolbox). Dla pozostałych 17 sektorów Unia Europejska nie zidentyfikowała jeszcze żadnych krytycznych łańcuchów dostaw, usług ani produktów.
W świetle powyższego, polski projektodawca, rozszerzając mechanizm inspirowany 5G Toolbox na wszystkie 18 sektorów gospodarki, działa w sposób przedwczesny i nieproporcjonalny. Tworzy potężne narzędzie restrykcyjne dla obszarów, w których nie zidentyfikowano nawet przedmiotu ochrony na poziomie unijnym. Zgodnie z art. 21 ust. 3 NIS2, podmioty mają brać pod uwagę wyniki tych skoordynowanych ocen przy doborze środków bezpieczeństwa. Wprowadzenie procedury HRV bez oparcia jej o wymagane dyrektywą analizy stanowi zatem formę nadregulacji i rażące naruszenie zasady proporcjonalności, które podważa spójność wdrażania prawa UE.
W obecnym kształcie procedura ta jest niebezpiecznym narzędziem mogącym destabilizować rynek, co potwierdzają również uwagi kluczowych resortów i instytucji:

- arbitralność i brak przesłanek - jak słusznie zauważyło Rządowe Centrum Legislacji[6], projekt nie określa jasnych przesłanek wszczęcia postępowania. Przepisy pozwalają na jego wszczęcie w oparciu o ogólne klauzule, takie jak „ochrona bezpieczeństwa państwa", co pozostawia pole do arbitralnych decyzji i stwarza stan niepewności dla wszystkich firm na rynku. Mankament ten wcale nie został usunięty na ostatnim etapie prac – nadal postępowanie może zostać wszczęte w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, z urzędu albo na wniosek przewodniczącego Kolegium (tak art. 67b ust. 1), a zgodnie z ust. 15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa;

- ograniczenie konkurencji- stanowisko MRiT[7] trafnie wskazuje, że nacisk na kryteria geograficzne (wykluczenie dostawców spoza EOG i NATO) uderzy w konkurencję, podniesie ceny i negatywnie wpłynie na polski eksport. Jak słusznie zauważyło Ministerstwo Spraw Zagranicznych, regulacja ta może objąć również dostawców z państw sojuszniczych Polski, które nie należą do UE i NATO[8];

- naruszenie prawa do obrony i proporcjonalności - jak alarmuje Rzecznik Praw Obywatelskich[9], rygor natychmiastowej wykonalności *ex lege*, iluzoryczna procedura

[6] Tak pismo Rządowego Centrum Legislacji znak: RCL.DISIP.550.5.2024 z 23.05.2024 r.
[7] Protokół rozbieżności z uzgodnień projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32), str. 1. Link: dokument695597.pdf
[8] Tak pismo Ministerstwa Spraw Zagranicznych znak: DPB.900.1.2024 / 1 z 21.10.2024 r.
[9] Pismo Rzecznika Praw Obywatelskich znak: BDG-WP.071.1.2022 z 24.05.2024 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

odwoławcza bez możliwości rozprawy (wyrok doręczany skarżącemu bez informacji niejawnych, a w pełnej wersji ministrowi) i brak gwarancji odszkodowania za błędne decyzje stanowią rażące naruszenie zasad proporcjonalności i prawa do skutecznego środka odwoławczego;

- dyskryminacja i naruszenie prawa UE - projektowany art. 67b ust. 4 w sposób rażący narusza traktatowe zasady jednolitego rynku, w szczególności swobodę świadczenia usług oraz swobodę przedsiębiorczości[10]. Przepis ten ogranicza bowiem prawo do przystąpienia do postępowania na prawach strony wyłącznie do przedsiębiorców telekomunikacyjnych **mających siedzibę na terytorium Rzeczypospolitej Polskiej**. Taka konstrukcja wprost dyskryminuje przedsiębiorców z innych państw członkowskich UE, którzy świadczą usługi na polskim rynku, ale ich siedziba znajduje się np. w Niemczech czy Czechach. **Jest to niedopuszczalna bariera i forma dyskryminacji ze względu na miejsce siedziby, zakazana na gruncie Traktatu o Funkcjonowaniu Unii Europejskiej.**

Skutkiem uznania dostawcy za HRV będzie obowiązek wycofania jego sprzętu i oprogramowania przez potencjalnie dziesiątki tysięcy podmiotów, co ww. raport EY szacuje na około 38 tysięcy firm. Wiąże się to z ogromnymi, nieplanowanymi kosztami nabycia nowego sprzętu oraz wdrożenia, co znacząco podnosi ogólne koszty prowadzenia działalności (tzw. *compliance costs*). Taka niepewność regulacyjna i ryzyko przymusowej, kosztownej wymiany infrastruktury IT drastycznie obniża atrakcyjność inwestycyjną Polski.

2.4. Znaczące osłabienie gwarancji prawnych dla przedsiębiorców uznanych za dostawcę wysokiego ryzyka

Z największym niepokojem przyjmujemy kierunek zmian w projekcie ustawy, który w naszej ocenie stanowi systemowy demontaż gwarancji prawnych chroniących przedsiębiorców. Proponowane przepisy w sposób nieuzasadniony i nieproporcjonalny wzmacniają pozycję organów państwa, jednocześnie osłabiając fundamentalne prawa podmiotów gospodarczych i wprowadzając osobistą, dotkliwą odpowiedzialność finansową dla kadry zarządzającej.

2.4.1. Ograniczenie praw przedsiębiorcy w trakcie kontroli

Pozytywnie oceniamy usunięcie art. 54 ust. 2 w projekcie ustawy w zakresie, w jakim wyłączał on przepisy ustawy Prawo przedsiębiorców. Niemniej nowo dodany art. 59c wprowadza instytucję „kontroli doraźnej", która może być zarządzona w niejasno określonych przypadkach „uzasadnionych charakterem sprawy lub pilnością". Co kluczowe, art. 59c ust. 4 stanowi, że kontrola taka może być prowadzona bez wcześniejszego powiadomienia

[10] Por. także uwagi Ministerstwa Klimatu i Środowiska (załącznik do pisma znak: BM-WR.0221.620.2024.DW z 15.05.2024 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

przedsiębiorcy. To rozwiązanie, w połączeniu z art. 65a (wyłączającym stosowanie art. 47 i 53 Prawa przedsiębiorców), w praktyce likwiduje fundamentalne prawo przedsiębiorcy do bycia uprzedzonym o zamiarze wszczęcia kontroli. Projekt ustawy, pod pozorem utrzymania standardów, w rzeczywistości likwiduje kluczowe zabezpieczenia, które do tej pory chroniły firmy przed paraliżem w wyniku działań kontrolnych[11], może w praktyce uniemożliwić normalne funkcjonowanie przedsiębiorstwa.

2.4.2. Nadmierne uprawnienia organów i ograniczenie prawa do sądu

Projekt ustawy przyznaje organom administracji uprawnienia, które nie tylko wykraczają poza standardy dyrektywy NIS 2, ale również naruszają konstytucyjne prawo do obrony swoich interesów przed sądem. Zmieniony art. 53 ust. 9 oraz nowy art. 53e wprowadzają katalog niezwykle dotkliwych środków, jakie organ może zastosować w przypadku niewykonania jego poleceń. Organ właściwy do spraw cyberbezpieczeństwa może m.in. **wstrzymać w całości albo w części działalność podmiotu** lub **zakazać pełnienia funkcji zarządczych przez kierownika**. Co najbardziej alarmujące, zgodnie z art. 53e ust. 10, od decyzji w sprawie zastosowania tych środków **nie przysługuje skarga do sądu administracyjnego**, co stanowi rażące naruszenie prawa do sądu i pozbawia przedsiębiorcę możliwości obrony przed potencjalnie arbitralnymi i niszczącymi dla biznesu decyzjami.

2.4.3. Wprowadzenie osobistej odpowiedzialności finansowej menedżerów

Projekt ustawy w bezprecedensowy sposób zaostrza reżim odpowiedzialności, przenosząc ciężar finansowy z podmiotu gospodarczego bezpośrednio na osoby fizyczne pełniące funkcje zarządcze.

- **wprowadzenie odpowiedzialności osobistej kadry kierowniczej -** nowe przepisy (art. 8c i 73a) wprowadzają **bezpośrednią odpowiedzialność kierownika podmiotu** za szeroki katalog obowiązków z zakresu cyberbezpieczeństwa. Co istotne, w przypadku organów wieloosobowych odpowiedzialność ponoszą solidarnie wszyscy jego członkowie, a odpowiedzialności tej nie można skutecznie scedować na inną osobę;

- **dotkliwe kary finansowe dla menedżerów -** art. 73a przewiduje możliwość nałożenia na kierownika podmiotu kary pieniężnej w wysokości **do 300% jego wynagrodzenia**. Takie rozwiązanie tworzy ogromne, osobiste ryzyko finansowe dla kadry zarządzającej i może zniechęcać do podejmowania funkcji kierowniczych w podmiotach objętych ustawą.

Podsumowując, powyższe zmiany stanowią nieuzasadnione i niebezpieczne wzmocnienie aparatu państwa kosztem praw nabytych przez przedsiębiorców, wprowadzając klimat niepewności prawnej i nadmiernego ryzyka, co w długofalowej perspektywie negatywnie odbije się na polskiej gospodarce.

[11] Por. uwaga Ministra Rozwoju i Technologii nr 11 w Protokole rozbieżności z uzgodnień projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).

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

2.5. Brak oceny skutków regulacji

Uwagi Ministerstwa Finansów[12] oraz Ministerstwa Infrastruktury[13] demaskują fundamentalne braki w Ocenie Skutków Regulacji oraz wprowadzają poważne wątpliwości co do stabilności finansowania całego systemu.

- naruszenie dyscypliny finansów publicznych - MF zgłasza aż 8 krytycznych uwag, wskazując m.in. na tworzenie wyłomu w systemie poprzez przekierowywanie kar do Funduszu Cyberbezpieczeństwa zamiast do budżetu państwa, niezgodne z prawem zasady niedokonywania zwrotu dotacji, czy wątpliwości co do samego funkcjonowania Funduszu;

- nierealne i nieprzejrzyste szacunki kosztów - MF kwestionuje potrzebę tworzenia 371 nowych etatów przy istniejących wakatach oraz brak uzasadnienia dla planowanych podwyżek. Wskazuje na brak dostępnej przestrzeni finansowej i konieczność optymalizacji kosztów;

- pominięcie kluczowych podmiotów - MI alarmuje, że w budżecie nie przewidziano środków dla strategicznych instytucji jak Wody Polskie i IMGW na realizację nowych, kosztownych obowiązków, co grozi paraliżem ich zdolności do zapewnienia cyberbezpieczeństwa.

Taki stan rzeczy dowodzi, że projekt jest przygotowany w pośpiechu, bez rzetelnej analizy finansowej, co grozi jego niewydolnością już na starcie.

2.6. Brak notyfikacji technicznej TRIS

Projekt ustawy zawiera przepisy techniczne, w tym te wykraczające poza minimalne wymogi dyrektywy NIS2, a w związku z tym podlega obowiązkowi notyfikacji Komisji Europejskiej zgodnie z dyrektywą (UE) 2015/1535 ustanawiającą procedurę udzielania informacji w dziedzinie przepisów technicznych[14]. Trybunał Sprawiedliwości Unii Europejskiej w fundamentalnym orzeczeniu CIA Security International SA przeciwko Signalson SA i Securitel SPRL z dnia 30 kwietnia 1996 r. (C-194/94) jednoznacznie stwierdził, że naruszenie obowiązku notyfikacji stanowi poważne uchybienie proceduralne, powodujące bezskuteczność spornych przepisów technicznych wobec jednostek. Wcześniej, w wyroku z dnia 2 sierpnia 1993 r. w sprawie Komisja przeciwko Republice Włoskiej (C-139/92), TSUE potwierdził, że naruszenie obowiązku notyfikacji stanowi samodzielną podstawę stwierdzenia uchybienia przez państwo zobowiązaniom traktatowym. Skutkiem braku notyfikacji jest obowiązek sądów krajowych odmowy zastosowania nienotyfikowanych przepisów technicznych, co oznacza, że jednostki mogą skutecznie podnosić zarzut braku notyfikacji, a przepisy te nie mają mocy obowiązującej wobec osób prywatnych. W

[12] Uwagi do Oceny Skutków Regulacji, str. 11 i następne w SRKM II – protokół rozbieżności.
[13] Ibidem.
[14] https://www.gov.pl/web/rozwoj/notyfikacja-przepisow-technicznych

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

konsekwencji, projekt ustawy wprowadzający dodatkowe wymogi cyberbezpieczeństwa **wykraczające poza dyrektywę NIS2 wymagają uprzedniej notyfikacji pod rygorem ich bezskuteczności w stosunkach z jednostkami.**

2.7. Naruszenie prawa zamówień publicznych i zasad jednolitego rynku UE

Projekt ustawy w sposób niedopuszczalny ingeruje w reżim prawny zamówień publicznych, tworząc nowe, obligatoryjne podstawy odrzucenia oferty, które są sprzeczne z duchem i literą prawa unijnego – na co zwrócił uwagę również Minister ds. Unii Europejskiej[15]. Zgodnie z projektowanym art. 17 projektu ustawy, zmieniającym ustawę Prawo zamówień publicznych (PZP), zamawiający będzie zobowiązany do odrzucenia oferty, jeżeli obejmuje ona produkty, usługi lub procesy ICT pochodzące od dostawcy uznanego za dostawcę wysokiego ryzyka (nowy art. 226 ust. 1 pkt 1 PZP) lub wskazane w negatywnej rekomendacji Pełnomocnika ds. Cyberbezpieczeństwa (zmieniony art. 226 ust. 1 pkt 17 PZP).
Takie rozwiązanie stoi w jawnej sprzeczności z art. 58 dyrektywy 2014/24/UE, który przyznaje instytucjom zamawiającym szeroki zakres swobody i uznania w określaniu kryteriów kwalifikacji wykonawców. Celem dyrektywy jest umożliwienie zamawiającemu elastycznego doboru warunków, które są proporcjonalne i adekwatne do przedmiotu zamówienia, tak aby wybrać ofertę gwarantującą najwyższą jakość. Projektowane przepisy odbierają zamawiającym tę swobodę, narzucając im automatyczny obowiązek odrzucenia oferty na podstawie zewnętrznej decyzji administracyjnej, bez możliwości samodzielnej oceny ryzyka w kontekście konkretnego postępowania.
Argument, jakoby zmiany te mieściły się w ramach wyjątku dotyczącego ochrony podstawowych interesów bezpieczeństwa państwa (art. 15 ust. 2 dyrektywy 2014/24/UE), jest nie do obrony. Zgodnie z utrwalonym orzecznictwem Trybunału Sprawiedliwości UE (m.in. w sprawie *Teckal*, C-107/98), wszelkie wyjątki od stosowania dyrektyw zamówieniowych muszą być interpretowane w sposób ścisły i zawężający. Tymczasem polski projektodawca posługuje się niezwykle szerokimi i ocennymi przesłankami, takimi jak *„zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego*" czy „negatywny wpływ na bezpieczeństwo publiczne". Takie klauzule generalne wykraczają daleko poza wąsko rozumiane interesy bezpieczeństwa państwa i otwierają drogę do arbitralnego wykluczania wykonawców z rynku, co narusza zasady uczciwej konkurencji i równego traktowania, stanowiące fundament jednolitego rynku.

2.8. Brak uwzględnienia Opinii Europejskiego Banku Centralnego

Pragniemy zwrócić szczególną uwagę na fakt, że projekt ustawy w obecnym kształcie wciąż nie adresuje fundamentalnych zastrzeżeń podniesionych w opinii Europejskiego Banku Centralnego z dnia 20 stycznia 2025 r. (CON/2025/2). Najważniejsza uwaga EBC dotyczy objęcia Narodowego Banku Polskiego zakresem ustawy jako podmiotu kluczowego, co, jak jednoznacznie stwierdził Bank, „wykracza poza dyrektywę (UE) 2022/2555, która wyłącza banki centralne (...) z definicji podmiotu administracji publicznej". Utrzymanie tego zapisu w

[15] Pismo Ministra do Spraw Unii Europejskiej znak: DPUE.720.508.2024(8) z 03.06.2024 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

polskim projekcie ma poważne konsekwencje, ponieważ kluczowe infrastruktury rynku finansowego będące własnością i prowadzone przez Eurosystem, takie jak polski komponent systemu TARGET, nie będą korzystały z wyłączenia przewidzianego dla banków centralnych. Stwarza to ryzyko kolizji z zharmonizowanymi ramami prawnymi Eurosystemu i może naruszać niezależne wykonywanie przez NBP jego zadań statutowych , w tym wspierania sprawnego funkcjonowania systemów płatniczych. Chociaż doceniamy utrzymanie w projekcie pewnych zabezpieczeń, takich jak wyłączenie NBP z procedury dostawcy wysokiego ryzyka czy wymóg uzyskania jego zgody na ocenę bezpieczeństwa, to nadrzędny problem poddania niezależnego banku centralnego krajowemu reżimowi nadzoru w zakresie cyberbezpieczeństwa, w sposób sprzeczny z duchem dyrektywy NIS2, pozostaje nierozwiązany i stanowi poważne ryzyko systemowe.

KL/241/77/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