Warszawa, 24 maja 2024 r.
KL/295/80/AM/2024

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu ds. Cyberbezpieczeństwa

Pan
Paweł Olszewski
Sekretarz Stanu
Ministerstwo Cyfryzacji

Szanowny Panie Premierze,
Szanowny Panie Ministrze,

Nawiązując do zaproszenia do udziału w konsultacjach projektu *ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw*, w załaczeniu, przesyłam stanoiwsko Konfederacji lewiatan do projektu ustawy.

Jesteśmy otwarci na współpracę i dalsze rozmowy z panem Premierem oraz z Panem Ministrem w sprawie szczegółowych rozwiązań zawartych w projekcie oraz ich wpływu na funkcjonowanie firm objetych projektem.

Z poważaniem

Maciej Witucki
Prezydent Konfederacji Lewiatan

Do wiadomości:
Pan Łukasz Wojewoda – Dyrektor Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Załącznik: Stanowisko Konfederacji Lewiatan wobec projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz o zmianie niektórych innych ustaw

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwagi wstępne

W imieniu Konfederacji Lewiatan niniejszym zgłaszamy uwagi do projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, opublikowanego do konsultacji publicznych.

W pierwszej kolejności **odnotowujemy, że część uwag zgłaszanych w toku poprzednich prac nad ustawą znalazła swoje odzwierciedlenie** w nowym tekście nowelizacji, mimo, że w ramach wcześniejszych prac uwagi te nie były uwzględniane. Odbieramy to jako zjawisko pozytywne. W szczególności, że część z tych kwestii dotyczy właśnie dialogu między stroną publiczną, a prywatną w ramach stosowania środków władczych w ramach krajowego systemu cyberbezpieczeństwa. W zakresie sektora telekomunikacyjnego, zauważamy także utrzymanie dotychczasowych przepisów działu VIIA ustawy Prawo telekomunikacyjne (w ustawie wprowadzającej PKE) do czasu wdrożenia NIS2. To również uznajemy za istotną poprawę wobec stanu wcześniejszego.

W drugiej kolejności dziękujemy za określenie 30-dniowego terminu konsultacji. Zabiegaliśmy o wydłużenie tego terminu, ale przyjmujemy argumenty dot. opóźnień w pracach nad wdrożeniem NIS2 na poziomie krajowym.

Zauważamy jednak, że **zakres projektu i jego skutków jest ogromny, co spowodowało, że skala wpływu na sektor telekomunikacyjny i teleinformatyczny nie mogła zostać w pełni oszacowana**. Dokładając należytej staranności przy analizie projektu napotkaliśmy na **liczne wątpliwości natury interpretacyjnej, a potencjalnie także kwestie wymagające poprawek oraz zwiększenia proporcjonalności**. Zakładamy, że w pozostałych sektorach objętych nowymi przepisami sytuacja jest podobna. Dlatego naszym ogólnym postulatem jest, aby po dokonaniu analizy zgłaszanych uwag **zorganizowana zostało spotkanie (lub seria spotkań) w ramach konsultacji społecznych**, w toku których ze strony Ministerstwa Cyfryzacji przedstawione zostałyby wyjaśnienia dotyczące praktycznych aspektów wdrażania projektowanych przepisów. Spotkania takie powinny odbyć się jeszcze przed skierowaniem projektu pod obrady komitetów Rady Ministrów. Uważamy, że jest to **niezwykle ważne dla zapewnienia właściwego, merytorycznego przebiegu konsultacji oraz wyjaśnienia wszelkich wątpliwości** interpretacyjnych. Dla objętych nowymi regulacjami firm jest to niezwykle istotne, aby właściwie planować przyszłe wdrożenia, w tym ich czaso- i kosztochłonność - które już teraz widać, że będą bardzo poważne.

Po trzecie – co wynika z doświadczeń z prac nad poprzednimi wersjami projektu – **wnioskujemy, aby w przypadku wprowadzania istotnych zmian mających wpływ na prawa i obowiązki regulowanych podmiotów, organizowane były także dodatkowe rundy**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

konsultacyjne. Niestety bowiem wielokrotnie byliśmy zaskakiwani wprowadzaniem do projektu całych nowych rozdziałów, które nie były przedmiotem pierwotnych konsultacji, a w sposób fundamentalny oddziaływały – często negatywnie – na sektor telekomunikacyjny.

Czwartą kwestią, która zauważamy w ramach uwag ogólnych, jest **brak aktów wykonawczych** do ustawy, a także brak aktów wykonawczych do samej dyrektywy NIS2. Powoduje to, że wiele kwestii jest wciąż niejasnych i nie jest tym samym możliwe dokonanie właściwej oceny wpływu regulacji na poszczególne typy działalności objętej nowymi przepisami. Z tego względu **postulujemy jak najszybsze opublikowanie projektów aktów wykonawczych do wstępnych chociaż konsultacji oraz wstrzymanie dalszych prac nad projektowaną ustawą do czasu ich przeprowadzenia**.

Ponadto, w naszej ocenie głębszego wyjaśnienia i przedstawienia praktycznych wytycznych wymagają relacje między NIS2 i DORA. Dotyczy to szczególnie podmiotów, które są jednocześnie regulowane w obu reżimach. Z jednej bowiem strony w art. 8i projektu ustawy wyłącza się stosowanie wobec podmiotów podlegających pod DORA rozdziału 3, ponieważ odpowiednie obowiązki należy wdrażać na bazie rozporządzenia DORA stosowanego bezpośrednio. Z drugiej jednak strony, przyjmuje się podejście wyrażone wyraźnie w uzasadnieniu: *Dyrektywa NIS 2 odeszła od wdrażania środków zapewniających bezpieczeństwo systemów informacyjnych tylko w zakresie świadczonych usług kluczowych. Podmiot ma dbać o bezpieczeństwo wszystkich swoich systemów wykorzystywanych do prowadzenia swojej działalności.* Przy tym podejściu, wyjaśnienia wymaga w jaki sposób np. podmiot kluczowy NIS2 (który miałby wdrożyć obowiązki we wszystkich swoich systemach), ma wdrażać obowiązki z NIS2 w swoich systemach służących także do działalności objętej rozporządzeniem DORA (a więc teoretycznie wyłączonej)?

Już na wstępie pragniemy także podkreślić konieczność głębokiej zmiany filozofii tego projektu, aby przyniósł on korzyści zarówno dla cyberbezpieczeństwa, jak i konkurencyjności polskich firm.
Doceniamy prace skoncentrowane na szybkiej implementacji dyrektywy NIS2. Niemniej zaproponowana treść przepisów, najbardziej restrykcyjna w porównaniu z innymi państwami członkowskimi w zakresie transpozycji dyrektywy NIS2. Warto zauważyć, że nadmierne regulacje mogą prowadzić do odwrotnych skutków niż zamierzone. Zamiast poprawiać bezpieczeństwo, mogą one skłaniać firmy do minimalizowania inwestycji w innowacje technologiczne oraz rozwój swoich systemów bezpieczeństwa, obawiając się wysokich kosztów i skomplikowanych procedur. W efekcie, może to paradoksalnie zwiększyć ryzyko cyberzagrożeń, zamiast je redukować. Ponadto, takie obciążenia mogą odstraszać potencjalnych inwestorów, którzy będą wybierać państwa o bardziej przyjaznym środowisku regulacyjnym.
Zasadne wydaje się zatem przyjęcie bardziej zrównoważonego podejścia, które nie tylko spełnia wymagania dyrektywy NIS2, ale również wspiera konkurencyjność i rozwój

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

gospodarczy. Wprowadzenie elastyczniejszych, mniej obciążających przepisów, które jednak zapewniają odpowiedni poziom bezpieczeństwa, przyniesie korzyści zarówno dla sektora prywatnego, jak i dla ogólnego poziomu cyberbezpieczeństwa w Polsce.

Projekt ustawy niesie ze sobą ogromne wyzwania i przekrojowo dotyka znacznej części polskich przedsiębiorców. W naszej ocenie projekt ustawy nie wyważa odpowiednio potrzeby zapewnienia państwu realnych narzędzi nadzoru i kontroli w obszarze cyberbezpieczeństwa z poszanowaniem i ochroną przedsiębiorczości oraz praw jednostki. Niestety, wiele elementów budzi głębokie wątpliwości z tego punktu widzenia. Przedsiębiorcy wyrażają swoje głębokie niezadowolenie, ponieważ projekt powtarza błędy poprzednich nowelizacji i dodatkowo rozszerza restrykcyjne regulacje na wszystkie 18 sektorów objętych dyrektywą NIS2, co stanowi ewenement w Unii Europejskiej. To podejście jest postrzegane jako nadmiernie obciążające dla polskich firm, zwiększając koszty i czasochłonność zgodności z przepisami i podkreślić należy, że spowoduje znaczne obniżenie atrakcyjności Polski, jako miejsca krajowych i zagranicznych inwestycji. Projekt ustawy nie zawiera nawet rzetelnie przeprowadzonej Oceny Skutków Regulacji, tak jak gdyby liczne obowiązki związane z cyberbezpieczeństwem miałyby pozostać bez wpływu na koszty prowadzenia działalności gospodarczej.

Szczególne zastrzeżenia budzi postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka (nie wynikające bezpośrednio z dyrektywy NIS2), które, spowoduje wykluczenie wielu dostawców z każdego z osiemnastu sektorów w Polsce, podczas ci sami dostawcy będą mogli bez przeszkód działać w innych krajach Unii Europejskiej). Zdaniem części firm zrzeszonych w Lewiatanie proponowana procedura uznania dostawcy za dostawcę wysokiego ryzyka nie jest zgodna z dyrektywą NIS2 i może być uznana za dyskryminującą, skupiając się bardziej na kryteriach politycznych niż technicznych, a zwłaszcza na państwie pochodzenia dostawców spoza Unii Europejskiej lub NATO. Niepokojące jest także, że władza nad tym procesem zostanie skupiona w zakresie kompetencji jednego ministra, który na podstawie niejawnych postępowań będzie mógł dowolnie wykluczać dostawców i ich rozwiązania z każdego sektora polskiej gospodarki. Taka koncentracja władzy budzi obawy o brak przejrzystości i potencjalne nadużycia, co może negatywnie wpływać na konkurencyjność i innowacyjność polskiej gospodarki. Ponadto, możliwość arbitralnego wykluczania dostawców bez jasnych i przejrzystych kryteriów może prowadzić do zmniejszenia zaufania inwestorów zagranicznych oraz do destabilizacji rynku technologicznego w Polsce.

Oczekujemy poważnych zmian w tekście projektowanych przepisów, które będą bardziej uwzględniać rzeczywiste potrzeby i możliwości polskiego rynku, przy jednoczesnym zachowaniu wysokiego poziomu cyberbezpieczeństwa, a także uwzględnia podejście innych krajów Unii Europejskiej. Istotne jest, aby nowe przepisy nie tylko spełniały wymogi dyrektywy NIS2, ale także wspierały rozwój gospodarczy i konkurencyjność polskich przedsiębiorstw. Izba nie neguje potrzeby i konieczności ochrony interesów Rzeczypospolitej Polskiej, jednak zwraca uwagę, że przyjęte rozwiązania powinny być proporcjonalne i dostosowane do specyfiki, a także uwzględniać skutki społeczne i ekonomiczne. Dlatego

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

wszelkie środki powinny być stosowane w odniesieniu do elementów krytycznych infrastruktury oraz związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa).
Jednocześnie część z firm zrzeszonych w Konfederacji Lewiatan nie widzi potrzeby zmian w treści projektu ustawy w zakresie odnoszącym się do procedury uznania danego przedsiębiorcy za dostawcę wysokiego ryzyka. Przedsiebiorcy Ci zwracają uwagę na to, że władze polskie, które odpowiadają za szeroko pojęte bezpieczeństwo państwa, muszą dysponować odpowiednimi narzędziami ograniczania realnych zagrożeń naszego bezpieczeństwa.
Implementacja dyrektywy NIS2 sama w sobie jest znaczącym wyzwaniem i prawdziwą rewolucją w obszarze cyberbezpieczeństwa. Wobec tak ambitnego zadania warto zastanowić się, czy czas na wprowadzanie dodatkowo restrykcyjnych przepisów, które wykraczają poza wymagania NIS2. Bardziej efektywne byłoby przyjęcie przepisów optymalnych, zgodnych z zasadą harmonizacji, a ewentualne korekty wprowadzać w zależności od sytuacji, co pozwoli na bardziej płynne dostosowanie do nowych regulacji. W kontekście samego zakresu nowelizacji należy także zwrócić uwagę, że sam projekt jest obszerniejszy, jeśli chodzi o treść i zawartość, niż sama ustawa o krajowym systemie cyberbezpieczeństwa. Zgodnie z § 84 Zasad techniki prawodawczej[1] *Jeżeli zmiany wprowadzane w ustawie miałyby być liczne albo miałyby naruszać konstrukcję lub spójność ustawy albo gdy ustawa była już poprzednio wielokrotnie nowelizowana, opracowuje się projekt nowej ustawy*. Ponadto pomimo relatywnie krótkiego, gdyż 6-letniego okresu obowiązywania, ustawa o krajowym systemie cyberbezpieczeństwa, była już wielokrotnie, bo aż 9 razy nowelizowana i ukazały się już 3 teksty jednolite. Przepis § 84 Zasad techniki prawodawczej wymienia alternatywnie trzy przyczyny, co oznacza, że zaistnienie tylko jednej z nich uzasadnia konieczność przygotowania nowej ustawy. W przypadku tej propozycji nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zachodzą dwie z trzech przyczyn wymienionych przez ten przepis, co uzasadnia przygotowanie nowej ustawy.
Apelujemy także o poszanowanie procesu legislacyjnego oraz o przeprowadzenie szerokich konsultacji, tak by uniknąć powtórzenia wadliwych rozwiązań zawartych w projekcie ustawy poprzedniego Rządu. Ważne jest, aby nowe przepisy były oparte na solidnych podstawach prawnych i uwzględniały rzeczywiste potrzeby oraz możliwości polskich przedsiębiorstw.
Apelujemy również o przeprowadzenie rzetelnej oceny skutków regulacji oraz analizy wpływu nowych obowiązków na koszty prowadzenia działalności w Polsce. Przedsiębiorcy już teraz borykają się z wieloma wyzwaniami, a nadmierne obciążenia regulacyjne mogą dodatkowo pogorszyć ich sytuację. Z tego powodu, konieczne jest, aby proces legislacyjny był przeprowadzany w sposób transparentny, z uwzględnieniem opinii wszystkich zainteresowanych stron, co pozwoli na wypracowanie przepisów, które będą zarówno skuteczne, jak i sprawiedliwe.

[1] Rozporządzenie z 20 czerwca 2002 r. Prezesa Rady Ministrów w sprawie „Zasad techniki prawodawczej" (t.j. Dz.U. z 2016 r. poz. 283)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

KL dostrzega znaczne potencjalne koszty oraz ryzyko nadregulacji związane z proponowanymi zmianami w ustawie o krajowym systemie cyberbezpieczeństwa. Obecny projekt ustawy wprowadza wiele kwestii wymagających dogłębnych konsultacji z różnymi sektorami gospodarki, również ze względu na szeroki zakres oddziaływania dyrektywy NIS2. Izba podkreśla, że szczególnie istotne jest unikanie tzw. "gold platingu", który prowadzi do niepotrzebnego obciążenia polskich przedsiębiorstw ponad wymagania dyrektywy NIS2, szczególnie w kontekście obecnych wyzwań makroekonomicznych, takich jak wzrost cen energii, inflacja oraz obciążenia podatkowe.

Proponowane regulacje wprowadzają znaczne obciążenia finansowe i operacyjne dla polskich firm, co może negatywnie wpłynąć na ich konkurencyjność oraz stabilność ekonomiczną. W związku z tym, Izba wyraża nadzieję na zorganizowanie konferencji uzgodnieniowej oraz warsztatów, które umożliwią szczegółowe omówienie i dopracowanie tych zmian z uwzględnieniem opinii i doświadczeń poszczególnych sektorów. Takie podejście pozwoli na wypracowanie bardziej zrównoważonych i efektywnych rozwiązań, które będą adekwatnie chronić bezpieczeństwo cybernetyczne kraju, nie powodując jednocześnie nadmiernych obciążeń dla przedsiębiorców.

Obawy dotyczące umocowania Ministra Cyfryzacji (koncepcja Superorganu ds. Cyberbezpieczeństwa)

Proponowane uprawnienia ministra ds. informatyzacji dają mu znaczny wpływ na całą polską gospodarkę, co budzi obawy o nadmierne kompetencje i potencjalne konflikty z Konstytucją RP. Szczególnie w sytuacji, gdy Minister Cyfryzacji jest organem jednoosobowym o charakterze politycznym. Minister będzie mógł usuwać z polskiego rynku dowolnego dostawcę (poprzez zakaz korzystania z jego rozwiązań), w drodze rekomendacji decydować o losach wszystkich zamówień publicznych, wydając polecenia zabezpieczające ograniczać i w praktyce zamykać działalność gospodarczą. Prerogatywy te są niespotykane w dotychczasowej legislacji – a powody tak silnych uprawnień nieznane. Takie uprawnienia mogą prowadzić do nieproporcjonalnej kontroli, co wymaga ponownej oceny, aby zapewnić zgodność z zasadami konstytucyjnymi, a w szczególności z prawami obywatelskimi.

Nadmierne regulacje specyficznych sektorów

Projekt ustawy nakłada dodatkowe obowiązki na sektory, które nie są objęte dyrektywą NIS2, takie jak wszystkie jednostki samorządu terytorialnego, sektor farmaceutyczny, w tym apteki i instytucje edukacyjne. Rozszerzenie zakresu na te podmioty jest nieuzasadnione i prowadzi do zbędnych obciążeń finansowych i administracyjnych. W szczególności dyrektywa NIS2 nie obejmuje w pełni sektora farmaceutycznego, jednak projekt ustawy klasyfikuje różne podmioty w tym sektorze jako kluczowe, co jest nadmierne i wprowadza niepotrzebne obciążenia regulacyjne.

Analiza rozwiązań zawartych w projekcie ustawy prowadzi również do konkluzji, że projektodawca przyjął rozwiązania jak najmniej proporcjonalne i nie uwzględniające specyfiki poszczególnych sektorów. W proponowanych przepisach nowelizacji nigdzie nie proponuje się podejścia opartego na kosztach. Artykuł 21 ust. 1 Dyrektywy NIS2 zobowiązuje

państwa członkowskie do zapewnienia, że podmioty kluczowe i ważne wdrażają odpowiednie i proporcjonalne środki techniczne, operacyjne oraz organizacyjne. Artykuł 8 ust. 1 pkt 2 projektu ustawy, który ma na celu implementację tych wymagań, nie zawiera odniesienia do kosztów wdrożenia jako kryterium oceny proporcjonalności środków. Stanowi to znaczącą różnicę w stosunku do dyrektywy, która podkreśla potrzebę uwzględniania tych kosztów w ocenie proporcjonalności środków zarządzania ryzykiem.

Potencjalna nadregulacja na tle innych państw członkowskich UE

Poniżej przedstawiono analizę poszczególnych implementacji dyrektywy NIS2 w niektórych krajach UE w zakresie stosowania nietechnicznych kryteriów oceny dostawców w łańcuchu dostaw.

Kraj	Status legislacji	Procedura DWR	Ocena nietechniczna w łańcuchach dostaw	Objęcie samorządu lokalnego	Objęcie instytucje edukacyjnych	Liczba podmiotów
Belgia	Ukończone	Nie	Nie	Nie	Nie	2K+
Węgry	Ukończone	Nie	Nie	Nie	Nie	N/D
Chorwacja	Ukończone	Nie	Nie	Tak	Tak	N/D
Niemcy	Przegląd rządowy	Nie	W trakcie dyskusji	Nie	Nie	35K+
Francja	Przegląd rządowy	Nie	Nie	Tak (ograniczone do 1% gmin)	Tak (ograniczone do funkcji badawczych)	15K+
Austria	Konsultacje publiczne	Nie	Nie	Nie	Nie	4K+
Finlandia	Konsultacje publiczne	Nie	Nie	Nie	Nie	N/D
Szwecja	Przegląd rządowy	Nie	Nie	Tak	Ograniczone do uniwersytetów	N/D

Implementacja dyrektywy NIS2 w krajach UE różni się znacząco pod względem liczby podmiotów objętych regulacjami. W Belgii, z populacją około 11,5 miliona i PKB wynoszącym 500 miliardów USD, dyrektywa obejmuje ponad 2,000 podmiotów. W Niemczech, liczących 83 miliony mieszkańców i z PKB około 4 bilionów USD, regulacje dotyczą ponad 35,000 podmiotów. We Francji, z populacją 67 milionów i PKB wynoszącym około 3 biliony USD,

dyrektywa obejmuje ponad 15,000 podmiotów. Austria, mająca około 9 milionów mieszkańców i PKB wynoszący 480 miliardów USD, ma ponad 4,000 podmiotów objętych dyrektywą. Polska, z populacją 38 milionów i PKB wynoszącym 740 miliardów USD, przyjęła szerokie podejście, obejmując około 38,000 podmiotów. Mimo że Polska jest znacznie mniejszym krajem i rynkiem niż Niemcy, to szerokie podejście skutkuje znacznymi wyzwaniami regulacyjnymi i kosztami dla polskich przedsiębiorców.

Szerokie podejście Polski do implementacji dyrektywy NIS2 może prowadzić do dużych obciążeń administracyjnych i finansowych dla polskich firm, które muszą spełniać liczne wymagania związane z bezpieczeństwem sieci i informacji. Dla porównania, Niemcy z większą populacją i znacznie wyższym PKB mają mniej podmiotów objętych dyrektywą, co wskazuje na bardziej wyważone podejście. W rezultacie polskie firmy mogą być zmuszone do poniesienia większych kosztów dostosowania się do nowych regulacji, co może wpłynąć na ich konkurencyjność na rynku europejskim. Podsumowując, Polska stoi przed wyzwaniem skutecznego wdrożenia dyrektywy NIS2 w sposób, który zapewni wysoki poziom bezpieczeństwa, ale jednocześnie nie zahamuje rozwoju gospodarczego i innowacji. Wymaga to strategicznego podejścia oraz wsparcia dla przedsiębiorców w adaptacji do nowych wymogów.

Obecnie trwają prace nad implementacją Dyrektywy NIS2 w Czechach, w których główne elementy proponowanej oceny obejmują ocenę dostawców w czterech kluczowych sektorach: telekomunikacja, rząd, energia i transport. W telekomunikacji szczególną uwagę poświęca się funkcjom krytycznym. Brak jest jednak standardów oceny ryzyka dostawców opartych na kraju pochodzenia. Krajowa Agencja Bezpieczeństwa Cybernetycznego (NOUGHKIB) ma możliwość oceny ryzyka dostawców na podstawie zagrożeń dla bezpieczeństwa Czech lub porządku publicznego.

Projekt ustawy o cyberbezpieczeństwie spotkał się z krytyką Rady Legislacyjnej Rządu (LRV), która zażądała jego modyfikacji. Problemy dotyczą m.in. szerokiego mandatu agencji oraz braku jasnych podstaw prawnych i ograniczeń dla wydawanych dekretów. Natomiast Polska zamierza zastosować procedury oceny dostawców wysokiego ryzyka dla wszystkich 18 sektorów objętych dyrektywą NIS2, w przeciwieństwie do Czech, które skupiają się tylko na czterech sektorach. Polski plan obejmuje każdą kategorię urządzeń i oprogramowania.

Procedury dla dostawców wysokiego ryzyka

Za całkowicie nieproporcjonalne uważamy objęcie procedurą dla dostawców wysokiego ryzyka wszystkich osiemnastu sektorów, co stanowi duży krok wstecz, w stosunku do, i tak powszechnie krytykowanego, przedłożenia poprzedniego Rządu. Co więcej, również sama analiza przeprowadzona przez Ministerstwo Cyfryzacji dołączona do OSR prowadzi do wniosku, że projektodawca proponuje unikalne w całej Unii Europejskiej rozwiązanie, zgodnie z którym procedura wykluczenia dostawcy obejmie wszystkie osiemnaście sektorów. Proponowana procedura uznania dostawcy za dostawcę wysokiego ryzyka nie jest zgodna z dyrektywą NIS2 i może być uznana za dyskryminującą, skupiając się bardziej na kryteriach politycznych niż technicznych. Procedura ta może prowadzić do znaczących skutków ekonomicznych, w tym wzrostu cen i zakłóceń rynkowych. Taka procedura, umocowana

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

właściwie w arbitralnej decyzji ministra ds. informatyzacji, w oparciu o niejawną opinię Kolegium ds. Cyberbezpieczeństwa budzi poważne zastrzeżenia z punktu widzenia zasady praworządności. Izba nie neguje potrzeby i konieczności ochrony interesów Rzeczypospolitej Polskiej, jednak zwraca uwagę, że przyjęte rozwiązania powinny być proporcjonalne i dostosowane do specyfiki, a także uwzględniać skutki społeczne i ekonomiczne. Dlatego wszelkie środki powinny być stosowane w odniesieniu do elementów krytycznych infrastruktury oraz związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa).

Elastyczność w zakresie funkcji krytycznych i infrastruktury

Aby ustawa nadążała za rozwojem technologii i dynamiką zagrożeń w cyberbezpieczeństwie, środki cyberbezpieczeństwa oraz zakres infrastruktury krytycznej muszą być łatwo dostosowywane. Wzorem Niemiec oraz Finlandii, funkcje krytyczne oraz infrastruktura krytyczna powinny być regulowane w aktach wykonawczych przez odpowiednie organy ds. cyberbezpieczeństwa dla każdego sektora, a nie sztywno określone w ustawie. Uważamy, że załącznik nr 3 powinien zostać usunięty, a oceny takich funkcji prowadzone przez Grupę Współpracy we współpracy z Komisją Europejską i ENISA, a nie przez ministra ds. informatyzacji.

Polecenia zabezpieczające

Natychmiastowa wykonalność poleceń zabezpieczających bez możliwości odwołania się narusza podstawowe zasady prawne. Te polecenia mogą prowadzić do znacznych przerw w działalności oraz obciążeń finansowych dla podmiotów, które muszą się do nich dostosować, bez przewidzianego odszkodowania. W wyniku poszerzenia zakresu jego obowiązywania – polecenia zabezpieczające może w zasadzie w każdej chwili sparaliżować działalność danego podmiotu, włączonego w system cyberbezpieczeństwa.

Podsumowanie

Konfederacja Lewiatan zdecydowanie rekomenduje ponowne rozważenie proponowanych zmian, aby zrównoważyć potrzeby w zakresie cyberbezpieczeństwa z praktycznymi realiami poszczególnych sektorów. Zapewnienie elastyczności w regulacji funkcji krytycznych i infrastruktury krytycznej pomoże uniknąć nadmiernych regulacji i związanych z nimi kosztów. Ponadto, kompetencje ministra ds. informatyzacji powinny zostać dokładnie przeanalizowane, aby zapobiec nadmiernej kontroli i zapewnić, że regulacje będą efektywne i proporcjonalne. Izba liczy na dalsze konsultacje i współpracę, aby dopracować przepisy w sposób wspierający zarówno cyberbezpieczeństwo, jak i stabilność ekonomiczną.

Poniżej przedstawiono szczegółowe uwagi podzielone na dziesięć kluczowych obszarów.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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. **<u>Bezpieczeństwo systemów informacyjnych</u>**

Jednostka redakcyjna: Art. 2 pkt 3c – bezpieczeństwo systemów informacyjnych

Nowa definicja bezpieczeństwa systemów informacyjnych określa je jako: *odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*.

Odpowiednia definicja w dyrektywy NIS2 wskazuje natomiast, że *bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, **<u>przy danym poziomie zaufania</u>**, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem*

Różnica polega w szczególności na pominięciu w krajowej definicji zwrotu „przy danym poziomie zaufania". Zmieniono także kolejność wylistowania atrybutów bezpieczeństwa. W pierwszej kolejności wnosimy o wyjaśnienie dla dokonania takich modyfikacji wobec dyrektywy NIS2, szczególnie, że w samym uzasadnieniu wskazano, że *Wprowadzone zmiany zapewnią spójność siatki pojęciowej wykorzystywanych we wszystkich krajach Unii Europejskiej.*

Pominięcie w definicji stwierdzenia „*na danym poziomie pewności*" zmienia istotę tego wymagania i może nie pozostawać bez wpływu na zakres obowiązków dostawcy usług, a w konsekwencji może również wpłynąć na zakres jego odpowiedzialności. Z tego względu wnioskujemy o uzupełnienie tego braku.

2. **Definicja dostawcy sieci dostarczania treści obejmuje przedsiębiorców telekomunikacyjnych**

Jednostka redakcyjna: art. 2 pkt 4b) projektu KSC

Jednostka redakcyjna NIS2: art. 6 pkt 32)

Uwaga: Definicja dostawcy sieci dostarczania treści (CDN) mówi o "osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej, która dostarcza sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług". Istnieją kluczowe elementy tej definicji, które mogą umożliwić zaliczenie operatorów telekomunikacyjnych do kategorii dostawców CDN:

a) "*Dostarcza sieci rozproszonych geograficznie serwerów*" - operator telekomunikacyjny zazwyczaj zarządza rozległą infrastrukturą sieciową, która obejmuje serwery i inne urządzenia telekomunikacyjne rozmieszczone geograficznie w różnych lokalizacjach, aby zapewnić pokrycie sieci i usług na dużą skalę. Choć głównym celem jest zapewnienie dostępu do sieci,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

infrastruktura ta technicznie spełnia kryterium "sieci rozproszonych geograficznie serwerów".

b) "*Służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania*" - w ramach swojej działalności operator telekomunikacyjny często oferuje usługi, które zapewniają dostęp do cyfrowych treści i usług (np. dostęp do internetu, usługi streamingowe, hosting). Infrastruktura ta jest kluczowa w utrzymaniu wysokiej dostępności i wydajności dostarczania tych usług, co jest zgodne z rolą CDN w kontekście szybkiego dostarczania treści.

c) "*Na rzecz użytkowników internetu w imieniu dostawców treści i usług*" - operator telekomunikacyjny świadczy usługi, które umożliwiają dostarczanie treści od dostawców treści do użytkowników końcowych. Operator działa jako kluczowe ogniwo w łańcuchu dostarczania treści od producentów do konsumentów.

Zaproponowana definicja może prowadzić do wniosku, że operator telekomunikacyjny spełnia niektóre z kluczowych kryteriów definiujących dostawcę CDN. Definicja jest na tyle szeroka, że technicznie obejmuje działalność operatora telekomunikacyjnego w kontekście zarządzania i dystrybucji cyfrowych treści i usług.

Wprowadzona w projekcie nowelizacji definicja dostawcy sieci dostarczania treści (CDN) jest niezwykle szeroka, co może prowadzić do niezamierzonych konsekwencji. Zgodnie z proponowanym art. 2 pkt 4b, każdy podmiot świadczący usługi CDN, niezależnie od stopnia technicznego zaangażowania w proces ich tworzenia, może zostać uznany za podmiot kluczowy. Taka sytuacja stawia pod znakiem zapytania m.in. status dostawców treści rozrywkowych, takich jak platformy VOD, które z założenia nie zajmują się zarządzaniem infrastrukturą krytyczną. Klasyfikacja tych podmiotów jako kluczowych nałoży na nie obowiązki typowe dla sektora ochrony infrastruktury krytycznej, takie jak rygorystyczne wymogi bezpieczeństwa czy obowiązkowe audyty, co może być nieadekwatne do charakteru ich działalności. Zaleca się dokładniejsze określenie kryteriów klasyfikacji dostawców CDN, by ograniczyć tę definicję tylko do tych podmiotów, które faktycznie odpowiadają za kluczowe aspekty infrastruktury krytycznej, unikając nadmiernego obciążenia podmiotów, których główna działalność nie wiąże się bezpośrednio z zagrożeniami dla cyberbezpieczeństwa.

3. Zbędna definicja dostawcy internetowej platformy handlowej

Jednostka redakcyjna: art. 2 pkt 4d) projektu KSC
Jednostka redakcyjna NIS2: art. 6 pkt 28)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwaga: Nie ma konieczności tworzenia autonomicznej definicji dostawy internetowej platformy handlowej, ponieważ jest już ona zdefiniowana w art. 2 pkt 9 ustawy o prawach konsumenta. Z tego samego założenia wychodzi ustawodawca europejski, odsyłając w tym zakresie do postanowień Dyrektywy 2005/29/WE. W tym przypadku nie ma potrzeby stosowania § 146 ust. 1 pkt 4) Zasad techniki prawodawczej, ponieważ nie ma potrzeby ustalania nowego znaczenia danego określenia.

4. **Definicja incydentu, niezgodna z analogiczną definicją zawartą w NIS2, skutkująca znaczącym rozszerzeniem obowiązków raportowania**

Jednostka redakcyjna: art. 2 pkt 5) projektu KSC
Jednostka redakcyjna NIS2: art. 6 pkt 6)

Uwaga: Zgodnie z art. 6 pkt 6) NIS2, incydent oznacza zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem. Natomiast projektodawca proponuje definicję, zgodnie z którą incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych. Proponowana definicja jest na tyle ogólna, że potencjalnie każde zdarzenie, które w jakikolwiek sposób wpłynie lub mogłoby wpłynąć na systemy informacyjne, może być uznane za incydent. To prowadzi do sytuacji, w której trudno odróżnić rzeczywiste incydenty od zdarzeń. Brak wyraźnych kryteriów dotyczących tego, co dokładnie stanowi naruszenie bezpieczeństwa, może utrudniać efektywne zarządzanie incydentami. Organizacje oraz organy odpowiedzialne za cyberbezpieczeństwo mogą mieć trudności z określeniem, które zdarzenia wymagają zgłoszenia i jakie działania należy podjąć. Definicja, która może obejmować niemal każde zdarzenie, również zwiększa ryzyko nadmiernego obciążenia organizacji obowiązkiem raportowania. Może to prowadzić do zbyt dużej liczby raportów, co obciąża zarówno raportujące podmioty, jak i organy nadzorcze, a także może rozmywać uwagę od bardziej krytycznych zagrożeń. Dlatego konieczne jest dostosowanie definicji incydentu w projekcie do standardów NIS2, aby zapewnić jasność i precyzję w zakresie obowiązków raportowania oraz efektywne zarządzanie incydentami.

5. **Definicja incydentu poważnego niezgodna z NIS2, skutkująca znaczącym rozszerzeniem zakresu regulacji**

Jednostka redakcyjna: art. 2 pkt 7) projektu KSC
Jednostka redakcyjna NIS2: art. 23 ust. 2

Uwaga: Projektodawca proponuje rozszerzenie definicji incydentu poważnego, określonego w art. 23 ust. 2 dyrektywy NIS2. Zgodnie z NIS2, incydent uznaje się za poważny, jeżeli ma on poważne skutki operacyjne lub finansowe dla danego podmiotu oraz jeśli wpływa na inne

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe. Wprowadzona definicja poszerza zakres, obejmując nie tylko skutki operacyjne i finansowe, ale również poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi (art. 2 pkt 7 projektu KSC). Nowe sformułowanie, jakim jest "poważne obniżenie jakości", wprowadza większą subiektywność i może być trudne do jednoznacznego określenia. Taka zmiana w definicji daje możliwość klasyfikacji szerokiej gamy zdarzeń jako incydentów poważnych, nawet jeśli ich wpływ nie jest bezpośrednio porównywalny z tym, co przewiduje dyrektywa NIS2. Przyjęcie takiej definicji może prowadzić do nadregulacji, zwiększając obciążenia dla przedsiębiorców, którzy będą zobowiązani do zgłaszania nawet mniejszych awarii technicznych. Choć takie incydenty mogą wpływać na jakość usługi, niekoniecznie prowadzą one do poważnych zakłóceń operacyjnych czy znaczących strat finansowych. Może to skutkować nieproporcjonalnym zwiększeniem liczby zgłoszeń, co obciąży zarówno przedsiębiorców, jak i organy nadzorujące, potencjalnie odwracając ich uwagę od rzeczywistych incydentów. Dlatego konieczne jest dostosowanie definicji incydentu poważnego w polskim projekcie do standardów NIS2, aby uniknąć nadmiernych obciążeń i skupić się na rzeczywistych zagrożeniach.

6. Szeroka odpowiedzialność kierowników podmiotów kluczowych lub podmiotów ważnych, niewymagana przez NIS2

Jednostka redakcyjna: art. 2 pkt 8a) projektu KSC
Jednostka redakcyjna NIS2: art. 20 ust. 2

Uwaga: W art. 2 pkt 8a) projektu KSC proponuje się zdefiniowanie kierownika podmiotu kluczowego lub podmiotu ważnego poprzez odesłanie do przepisów art. 3 pkt 6) ustawy o rachunkowości. Odesłanie jest błędne, gdyż powinno odsyłać do art. 3 ust. 1 pkt 6 ustawy o rachunkowości. Definicja ta posiada istotne znaczenie pod kątem obowiązków kierowników oraz zasad ich odpowiedzialności. Zastosowanie bardzo szerokiej definicji z ustawy o rachunkowości skutkuje tym, że odpowiedzialność o charakterze penalnym, zamiast być ściśle ograniczona, obejmuje wszystkie osoby odpowiedzialne za zarządzanie danym podmiotem, nawet w sytuacji, gdy z okoliczności prawnych lub faktycznych wynika, że nie są one w ogóle odpowiedzialne za kwestie cyberbezpieczeństwa. W tym zakresie projektodawca powinien raczej zastosować konstrukcję prawną znaną z ustawy – Prawo telekomunikacyjne, tj. wykorzystanie pojęcia "osoba kierująca przedsiębiorstwem" (tak art. 209 ust. 2 ustawy – Prawo telekomunikacyjne). Takie podejście będzie również bardziej adekwatne w stosunku do terminu "organ zarządzający podmiotem kluczowym i podmiotem ważnym", do którego odwołuje się art. 20 ust. 1 i 2 NIS2. Ponadto, odesłanie może być nieadekwatne, ponieważ nie wszystkie podmioty stosują ustawę o rachunkowości. Na marginesie również budzi wątpliwości odesłanie akurat do tej ustawy, w kontekście materii regulowanej projektem KSC. W związku z powyższym, zaleca się zrewidowanie definicji kierownika podmiotu kluczowego lub podmiotu ważnego w projekcie KSC, aby

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

odpowiedzialność była precyzyjnie określona i adekwatna do zakresu obowiązków związanych z cyberbezpieczeństwem.

7. Definicja podmiotu krytycznego

Jednostka redakcyjna: art. 2 pkt 11c) projektu KSC
Jednostka redakcyjna NIS2: art. 2 ust. 5

Uwaga: Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557, podobnie jak każda inna dyrektywa, co do zasady obowiązuje tylko państwa członkowskie. Z tej przyczyny nieprawidłowym może być odsyłanie do definicji podmiotu krytycznego w art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE. Szczególnie, gdy zgodnie z art. 7 ust. 8 projektu KSC informację o wyznaczeniu takiemu podmiotowi przekazuje ministrowi właściwemu do spraw informatyzacji dyrektor Rządowego Centrum Bezpieczeństwa. Aby uniknąć nieprawidłowości i zapewnić jasność przepisów, zaleca się sformułowanie definicji podmiotu krytycznego bezpośrednio w ustawie KSC, zamiast odsyłania do definicji zawartej w dyrektywie. W ten sposób zapewni się, że definicja jest w pełni zrozumiała i zgodna z krajowymi regulacjami oraz praktykami. Ustawa może odsyłać do dyrektywy, ale należy pamiętać, że dyrektywy jako takie nie mają bezpośredniego zastosowania w prawie krajowym – wymagają transpozycji, czyli wdrożenia poprzez krajowe akty prawne.

8. Brak dostosowania przepisów do projektu ustawy Prawo Komunikacji Elektronicznej przyjęte przez Radę Ministrów 7.05.2024

Jednostka redakcyjna: art. 2 pkt 11g) projektu KSC; art. 5 projektu ustawy,
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: 7 maja 2024 r. Rada Ministrów przyjęła projekt ustawy Prawo komunikacji elektronicznej. Niemniej, opublikowana wersja projektu KSC zakłada odwołanie się do obowiązującej ustawy – Prawo telekomunikacyjne, która zostanie uchylona przez ustawę wdrażającą Prawo komunikacji elektronicznej. Na tym etapie brak odwołania do Prawa komunikacji elektronicznej uniemożliwia całościową analizę proponowanych przepisów z uwzględnieniem stanu prawnego po wejściu w życie ustawy – Prawo komunikacji elektronicznej (planowane po 1 stycznia 2025 r.).

9. System informacyjny.

Jednostka redakcyjna: Art. 2 pkt 14 – system informacyjny
Jednostka redakcyjna NIS2: art. 6 pkt 1)

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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. 2 pkt 14) projektu KSC projektodawca definiuje system teleinformatyczny jako:

a) system teleinformatyczny, o którym mowa w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307) lub

b) urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych

– wraz z danymi przetwarzanymi w postaci elektronicznej.

W definicji systemu informacyjnego dodawane jest sformułowanie *„urządzenie lub grupę połączonych urządzeń elektrycznych lub elektronicznych i oprogramowania zaprogramowanych w celu przetwarzania danych”*. W uzasadnieniu wskazano, że intencją jest przesądzenie objęcia definicją systemów OT. Taka redakcja powoduje jednak, że jako system informacyjny może być klasyfikowany także pojedyncze urządzenie, jak np. laptop czy telefon, które wydają się same w sobie nie wyczerpywać pojęcia „systemu”. Wnosimy o ponowne rozważenie tej kwestii.

10. <u>Potencjalne zdarzenie dla cyberbezpieczeństwa</u>

Jednostka redakcyjna: Art. 2 pkt 11e - potencjalne zdarzenie dla cyberbezpieczeństwa
Jednostka redakcyjna NIS2: art. 6 pkt 5)

11e) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych

Zauważamy, że definicja jest odmienna od definicji zawartej w NIS2. W szczególności pominięto w niej wskazanie, że jest to zdarzenie *„któremu udało się jednak zapobiec lub które jednak nie wystąpiło;”*.
Art. 6 pkt 5 NIS2 skupia się na konkretnych aspektach bezpieczeństwa danych i systemów informatycznych, takich jak dostępność, autentyczność, integralność i poufność. Uwzględnia zdarzenia, które mogły naruszyć te aspekty, ale którym udało się zapobiec lub które ostatecznie nie wystąpiły. Natomiast propozycja projektodawcy jest bardziej ogólna i obejmuje każde zdarzenie, które może mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych. Nie ogranicza się do konkretnych aspektów bezpieczeństwa danych, co otwiera możliwość interpretacji każdego zdarzenia jako potencjalnego zagrożenia. Szerokie i nieprecyzyjne określenie "potencjalne zdarzenie" może prowadzić do nadmiernego obciążenia organizacji obowiązkiem raportowania nawet mało znaczących zdarzeń. To z kolei może prowadzić do zwiększenia biurokracji i rozmycia uwagi od rzeczywiście istotnych zagrożeń. Podmioty kluczowe i ważne mogą borykać się z problemem ustalenia, które zdarzenia faktycznie stanowią zagrożenie wymagające zgłoszenia, co może prowadzić do

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

przeciążenia systemów raportowania i rozproszenia uwagi od zagrożeń wymagających natychmiastowej interwencji.

11. Aktualna definicja ryzyka

Jednostka redakcyjna: w art. 2 pkt 12

12) ryzyko - kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

Zauważamy, że aktualna definicja używa niezdefiniowanego pojęcia *„zdarzenia niepożądanego*". Jest też odmienna od definicji ryzyka z NIS2 używającej pojęć zdefiniowanych:

„„ryzyko" oznacza możliwość wystąpienia strat lub zakłóceń spowodowanych incydentem, wyrażoną jako wypadkową wielkości takiej straty lub takich zakłóceń oraz prawdopodobieństwo wystąpienia takiego incydentu;"

12. Niejasne uprawnienia podmiotów krajowego systemu cyberbezpieczeństwa w zakresie dokonywania analizy ruchu sieciowego w kontekście tajemnicy telekomunikacyjnej (a także tajemnicy korespondencji).

Jednostka redakcyjna: art. 3a projektu KSC
Jednostka redakcyjna NIS2: art. 21 ust. 2 pkt b)

„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług.";

W uzasadnieniu wskazano, że *„Przepisy ustawy przesądzają, że w ramach obsługi incydentu dotknięty nim podmiot może wykrywać źródło ataku oraz czasowo ograniczyć ruch sieciowy z adresów IP lub adresów URL. Uprawnienia te są niezbędne dla zapewnienia skutecznej reakcji na incydent, a w praktyce sprawiają one problemy praktyczne. Wykrycie źródła ataku często jest niezbędne do jego powstrzymania i przywrócenia normalnego funkcjonowania systemów. Równocześnie te działania mogą prowadzić do ewentualnego naruszenia uprawnień innych podmiotów. Do tej pory istniały wątpliwości na ile takie działania mogą być podejmowane. W związku z tym konieczne jest wprowadzenie wyraźnej podstawy prawnej do takich działań."*

Zaproponowany zapis naszym zdaniem zakreśla węższy zakres uprawnień niż ten, o którym mowa w uzasadnieniu. W szczególności pominięto słowo „ataku" co jednak można uznać za zabieg celowy. Co jednak istotniejsze, projektowany przepis nie zawiera przywołanego w uzasadnieniu uprawnienia do „czasowego ograniczania ruchu sieciowego z adresów IP lub

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

adresów URL”. Jeśli więc cel określony w uzasadnieniu miałby zostać osiągnięty, przepis należy rozszerzyć.

Uwaga. Dodatkowo art. 3a projektu KSC proponuje, aby podmioty krajowego systemu cyberbezpieczeństwa mogły podejmować działania w celu wykrywania źródła lub dokonywania analizy ruchu sieciowego powodującego wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usług. Niemniej, przepis ten jest zbyt ogólny i nie określa jednoznacznie zakresu uprawnień tych podmiotów. Brak precyzyjnego ograniczenia tych uprawnień może prowadzić do kolizji z normami zawartymi w art. 159 ustawy – Prawo telekomunikacyjne, który chroni tajemnicę telekomunikacyjną, obejmującą m.in. treść indywidualnych komunikatów oraz dane transmisyjne i lokalizacyjne. Szerokie i nieokreślone uprawnienia mogą prowadzić do naruszenia tajemnicy telekomunikacyjnej i korespondencji, co jest niedopuszczalne. Z uwagi na powyższe, przepis art. 3a projektu KSC powinien zostać doprecyzowany, aby jasno określał granice uprawnień podmiotów krajowego systemu cyberbezpieczeństwa w zakresie analizy ruchu sieciowego.

Poza powyższym, zauważamy, że wraz z uchyleniem rzdz. VIIA uPT usunięty zostanie także przepis art. 175c przewidujący szczególne uprawnienia przedsiębiorców telekomunikacyjnych w zakresie podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym:

1) eliminacji przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług;

2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług.

Wnosimy o rozważenie utrzymania tego uprawnienia w projektowanym brzmieniu uKSC.

13. Objęcie nowymi obowiązkami w zakresie cyberbezpieczeństwa podmiotów, które nie powinny zostać nimi objęte zgodnie z NIS2. Zakres stosowania określany wg GBER

Jednostka redakcyjna: art. 5 projektu KSC; załącznik nr 1; załącznik nr 2
Jednostka redakcyjna NIS2: art. 3

NIS2 wskazuje na dokonywania oceny wielkości przedsiębiorstwa na podstawie art. 2 załącznika do zalecenia 2003/361/WE natomiast projekt ustawy w art. 5 ust. 1 pkt 1, ust.2, odnosi się wprost do art. 2 załącznika 2 rozporządzenia GBER, ale już art. 5 ust. 1 pkt 2 odnosi się do całego GBER.

W uzasadnieniu wyjaśniono, że wynika to z zasad techniki prawodawczej i konieczności odwołania się do obowiązujących przepisów prawnych.
Wyjaśnienia wymaga czy dla oceny wielkości przedsiębiorstwa należy uwzględniać jedynie pułapy określone w art. 2 załącznika 2 GBER czy także pozostałe przepisy załącznika 2 GBER dot. powiązań między przedsiębiorstwami. Z uwagi na wprowadzenie w ust. 3 wyłączenia art. 3 ust. 4 załącznika GBER wydaje się, że intencją jest stosowanie wszystkich zapisów załącznika oprócz wyłączonych. Niezrozumiała jest jednocześnie wyżej wskazana różnica w sposobie odwołania do rozporządzenia GBER.

W porównaniu z NIS2 projekt ustawy nakłada dodatkowe obowiązki na sektory, które nie muszą podlegać tak rygorystycznym regulacjom**.** Po pierwsze projekt ustawy klasyfikuje jako podmioty kluczowe podmioty ważne, zgodnie z dyrektywą NIS2, co wiąże się z podwyższeniem stopnia nadzoru nad tymi podmiotami. Takie działanie zostało podjęte w sektorach takich jak produkcja, wytwarzanie i dystrybucja chemikaliów; produkcja, przetwarzanie i dystrybucja żywności; produkcja w tym podsektor produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro, podsektor produkcji komputerów, wyrobów elektronicznych i optycznych, podsektor produkcji urządzeń elektrycznych, podsektor produkcji maszyn i urządzeń, gdzie indziej niesklasyfikowana, oraz podsektor produkcji pojazdów samochodowych, przyczep i naczep. Nie można obciążać polskich przedsiębiorców dodatkowymi wymaganiami, co powoduje dalsze koszty, zwłaszcza w kontekście polityki energetycznej, wzrostu cen, inflacji oraz wzrostu obciążeń podatkowych.
Po drugie dyrektywa NIS2 nie obejmuje co do zasady jednostek samorządu terytorialnego i instytucji edukacyjnych (brak obligatoryjności). Dyrektywa NIS2 nie nakłada obowiązku regulacji na jednostki samorządu terytorialnego oraz instytucje edukacyjne jako takie. Natomiast rządowy projekt ustawy rozszerza zakres podmiotów kluczowych o jednostki samorządu terytorialnego oraz instytucje edukacyjne prowadzące działalność badawczą, co odbiega od postanowień dyrektywy NIS2. W świetle przepisów dyrektywy, jednostki na poziomie regionalnym mogą zostać uznane za podmioty administracji publicznej tylko wtedy, gdy świadczą usługi o znaczącym wpływie społeczno-gospodarczym, co powinno być potwierdzone oceną ryzyka. Jednakże, projekt ustawy nie uwzględnia tego warunku, co prowadzi do nieuzasadnionych obciążeń dla jednostek samorządu terytorialnego oraz instytucji edukacyjnych, takich jak domy kultury czy muzea. Co więcej zgodnie z art. 2 ust. 5 dyrektywy NIS2, państwa członkowskie mogą zdecydować o włączeniu do zakresu dyrektywy lokalnych jednostek administracji publicznej lub instytucji edukacyjnych, pod warunkiem, że prowadzą one działalność badawczą o krytycznym znaczeniu. Jednakże, projekt ustawy krajowej generalizuje to rozszerzenie na wszystkie publiczne uczelnie i instytucje kulturalne, niezależnie od charakteru ich działalności, co stoi w sprzeczności z intencją dyrektywy i generuje niepotrzebne koszty.
Po trzecie Dyrektywa NIS2 nie obejmuje w całości sektora farmaceutycznego, w tym aptek: Projekt ustawy kwalifikuje jako podmioty kluczowe hurtownie farmaceutyczne,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

przedsiębiorców posiadających pozwolenie na dopuszczenie do obrotu produktu leczniczego, importerów i wytwórców produktów leczniczych/substancji czynnych, importerów równoległych, dystrybutorów substancji czynnej oraz apteki. Tymczasem, zgodnie z załącznikiem nr 1 do NIS2, status podmiotów kluczowych przysługuje tylko tym podmiotom, które prowadzą działalność badawczo-rozwojową w zakresie produktów leczniczych, podmiotom produkującym podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, a także podmiotom produkującym wyroby medyczne uznane za mające krytyczne znaczenie podczas stanu zagrożenia zdrowia publicznego.

Poniżej przedstawiono szczegółową informację w tym zakresie:

Lista podmiotów, które nie zostały wskazane w załączniku I do Dyrektywy NIS2, a które umieszczono w załączniku nr 1 do projektu ustawy co oznacza objęcie obowiązkami wynikającymi z ustawy podmiotów, które nie muszą pod nią podlegać:

1. Sektor energia
    a. Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane.
    b. Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.
2. Sektor bankowość i infrastruktura rynków finansowych
    a. Administratorzy kluczowych wskaźników referencyjnych.
3. Sektor ochrona zdrowia:
    a. Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301, 605, 650, 1859 i 1938).
    b. Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.
    c. Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
    d. Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
    e. Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
    f. Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
    g. Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
4. Sektor administracja publiczna:
    a. jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w tym:

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

i. jednostki samorządu terytorialnego oraz ich związki;
ii. związki metropolitalne;
iii. jednostki budżetowe;
iv. samorządowe zakłady budżetowe
v. uczelnie publiczne;
vi. Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;
vii. państwowe i samorządowe instytucje kultury;

b. instytuty badawcze

Lista podmiotów, które nie zostały wskazane w załączniku I do Dyrektywy NIS2, a które umieszczono w załączniku nr 1 do projektu ustawy zamiast w załączniku nr 2 do ustawy(podwyższenie wymogów minimalnych wynikających z Dyrektywy NIS2, poprzez sklasyfikowanie niektórych sektorów jako podmiotów kluczowych, zamiast jako podmiotów ważnych):

1. Sektor produkcja, wytwarzanie i dystrybucja chemikaliów
   a. Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady.
   b. Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady.
2. Sektor produkcja, przetwarzanie i dystrybucja żywności
   a. Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady, zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem.
3. Sektor produkcja:
   a. podsektor produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro:
      i. Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745.
      ii. Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego.
   b. podsektor produkcja komputerów, wyrobów elektronicznych i optycznych
      i. Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.).

c. podsektor produkcja urządzeń elektrycznych
    i. Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2.
d. podsektor produkcja maszyn i urządzeń, gdzie indziej niesklasyfikowana
    i. Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 28 klasyfikacji NACE Rev. 2.
e. podsektor produkcja pojazdów samochodowych, przyczep i naczep
    i. Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2.
f. podsektor produkcja pozostałego sprzętu transportowego
    i. Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2.

14. Definicja Podmiotu Kluczowego (art. 5 UKSC) – zmiana zakresu podmiotowego projektowanej ustawy, objęcie ustawą jedynie podmiotów świadczących publicznie dostępne usługi

Jednostka redakcyjna: art. 5

W ramach projektowanej nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa, znacznemu poszerzeniu ulega krąg podmiotów, do których zastosowanie będą miały przepisy ustawy co nie znajduje uzasadnienia we wdrażanej dyrektywie NIS2. Zgodnie z dyrektywą NIS2 nowymi obowiązkami dotyczącymi cyberbezpieczeństwa miały zostać objęte jedynie podmioty, które świadczą usługi o charakterze publicznym.
Przepisy nowelizacji ustawy o KSC, przy zaproponowanych szerokich definicjach przedsiębiorcy komunikacji elektronicznej oraz przedsiębiorcy telekomunikacyjnego wychodzą znacząco ponad wskazania zawarte w NIS 2, która wskazuje w swoim Załączniku I jako sektory kluczowe jedynie dostawców **publicznych** sieci łączności elektronicznej oraz dostawców **publicznie dostępnych** usług łączności elektronicznej. Definicje zaproponowane w nowelizowanej ustawie KSC powodują, że krąg podmiotów objętych ustawą jest znacznie szerszy i obejmuje również podmioty, których usługi nie mają charakteru publicznego, są świadczone okazjonalnie i jedynie np. dla podmiotów z grupy kapitałowej, do której należą. Nakładanie na takie podmioty nowych obowiązków związanych z dostosowaniem ich

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

infrastruktury, koniecznością zaprojektowania nowych procesów czy zatrudnienia nowych osób jest całkowicie nieuzasadnione ekonomiczne i sprzeczne z wymogami dyrektywy NIS2.
Zgodnie z proponowanym w nowelizacji art. 1 ust. 8 Podmiotem Kluczowym, do którego będą miały zastosowanie przepisy nowelizowanej ustawy są m.in. przedsiębiorcy komunikacji elektronicznej, którzy co najmniej spełniają wymogi dla średniego przedsiębiorcy. W zakresie definicji przedsiębiorcy komunikacji elektronicznej projekt nowelizacji ustawy posługuje się pojęciem zbieżnym z siatką pojęciową, którą posługuje się procedowany aktualnie w Sejmie projekt nowego Prawa Komunikacji Elektronicznej. Zgodnie z definicją przedsiębiorcy komunikacji elektronicznej, krąg ten obejmuje przedsiębiorcę telekomunikacyjnego, oraz podmiot świadczący usługi komunikacji interpersonalnej niewykorzystującej numerów.
Wątpliwości budzi w szczególności interpretacja definicji przedsiębiorcy telekomunikacyjnego zawarta w nowelizowanej ustawie PKE, która obejmuje: podmioty, które wykonują działalność gospodarczą polegającą na dostarczaniu **publicznych sieci telekomunikacyjnych**, *świadczeniu powiązanych usług* lub **świadczeniu publicznie dostępnych usług telekomunikacyjnych**. Wśród wymienionych podmiotów znajduje się podmioty świadczące usługi powiązane, które zgodnie z literalnym brzmieniem definicji nie muszą mieć charakteru usługi publicznej – co jest sprzeczne z wytycznymi dyrektywy NIS2.
W związku z tym, aby zapewnić zgodność z wprowadzaną dyrektywą NIS2, definicje dodawane projektowanym art. 2 dotyczące dostawców usług (od pkt 4b do pkt 4i) jak również definicje znajdujące się w procedowanym w Sejmie PKE, powinny zostać zmodyfikowane w taki sposób, **żeby odnosiły się tylko do podmiotów, które świadczą wskazane usługi w sposób publicznie dostępny**. Ewentualnie powinno zostać dodatkowe wyłączenie, które wskaże, że w zakres definicji świadczenia usług nie będą wchodziły usługi świadczone na rzecz jednostek powiązanych z dostawcą w rozumieniu Ustawy o rachunkowości z dnia 29 września 1994 r. Oczekiwany skutek można również uzyskać odpowiednio modyfikując propozycję definicji przedsiębiorcy telekomunikacyjnego zawartą w nowelizowanym PKE.

15. Nieuzasadnione włączenie całych grup kapitałowych jako podmiotów kluczowych i ważnych

Jednostka redakcyjna: art. 5 ust. 1 pkt 1 i 2 oraz ust. 2 pkt 1 ustawy KSC
Jednostka redakcyjna NIS2: art. 2 ust. 1

Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa wprowadza problematyczne i niejasne kryteria klasyfikacji podmiotów kluczowych i ważnych, w tym odwołanie do art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014. Zastosowanie tego przepisu prowadzi do sytuacji, w której całe grupy kapitałowe lub holdingi mogą zostać zakwalifikowane jako podmioty objęte ustawą, niezależnie od rzeczywistej

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

wielkości poszczególnych spółek, ich obrotów czy liczby zatrudnionych pracowników. Jest to podejście niewspółmierne. Kluczowym czynnikiem decydującym o zakwalifikowaniu przedsiębiorstwa jako podmiotu kluczowego lub ważnego staje się jedynie fakt przynależności do grupy kapitałowej, a nie rzeczywista działalność i wpływ na infrastrukturę krytyczną. Ignorowanie w projektowanej nowelizacji motywu (16) dyrektywy NIS2, który sugeruje konieczność analizy powiązań między przedsiębiorcami w celu uniknięcia niewłaściwego klasyfikowania podmiotów, jest poważnym zaniedbaniem. Podejście to może prowadzić do niewłaściwego alokowania zasobów na środki ochrony, które w rzeczywistości mogą nie przyczyniać się do zwiększenia poziomu bezpieczeństwa cybernetycznego. Takie rozwiązanie jest nie tylko absurdalne, ale też szkodliwe, gdyż obciąża firmy niepotrzebnymi kosztami i wymogami administracyjnymi, co jest sprzeczne z ideą efektywnej ochrony cyberbezpieczeństwa.[2].

16. Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa

Jednostka redakcyjna: Art. 5 ust. 1 pkt 3 lit. b

Zauważamy wykroczenie poza ramy dyrektywy NIS2 i nadmiarowe wobec niej zakwalifikowanie wszystkich dostawców usług zarządzanych w zakresie cyberbezpieczeństwa do kategorii podmiotów kluczowych niezależnie od ich wielkości. W uzasadnieniu wyjaśniono, że zabieg ten jest celowy i wynika z faktu, że takie podmioty świadczą usługi dla innych podmiotów. Wydaje się jednak, że włączenie wszystkich takich podmiotów byłoby bardziej proporcjonalne, gdyby było uzależnione od tego czy faktycznie świadczą usługi podmiotom KSC czy nie.

17. Nieproporcjonalny obowiązek rejestracji i rygorystyczne terminy samorejestracji dla podmiotów kluczowych i ważnych

Jednostka redakcyjna: art. 5 ust. 3 projektu KSC

[2]Zgodnie z motywem (16): Stosując art. 6 ust. 2 załącznika do zalecenia 2003/361/WE, państwa członkowskie mogą uwzględnić stopień niezależności podmiotu w stosunku do jego przedsiębiorstw partnerskich lub powiązanych, aby uniknąć uznawania podmiotów, które mają przedsiębiorstwa partnerskie lub które są przedsiębiorstwami powiązanymi, za podmioty kluczowe lub ważne, gdyby było to nieproporcjonalne. W szczególności państwa członkowskie mogą uwzględnić fakt, że dany podmiot jest niezależny od przedsiębiorstw partnerskich lub powiązanych pod względem sieci i systemów informatycznych, z których korzysta przy świadczeniu usług, a także pod względem świadczonych przez siebie usług. Na tej podstawie, w stosownych przypadkach, państwa członkowskie mogą uznać, że taki podmiot nie kwalifikuje się jako średnie przedsiębiorstwo na podstawie art. 2 załącznika do zalecenia 2003/361/WE, ani nie przekracza określonych dla średniego przedsiębiorstwa pułapów, określonych w ust. 1 tego artykułu, jeżeli po uwzględnieniu stopnia niezależności tego podmiotu nie zostałby on uznany za kwalifikujący się jako średnie przedsiębiorstwo lub przekraczający te pułapy, w przypadku gdy uwzględniono tylko jego własne dane. Nie wpływa to na określone w niniejszej dyrektywie obowiązki przedsiębiorstw partnerskich i powiązanych, które są objęte zakresem jej stosowania.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Jednostka redakcyjna NIS2: art. 3 ust. 3

Uwaga: Zgodnie z przepisami, przedsiębiorstwa, które przekroczą określone progi zatrudnienia lub obrotu, mają zaledwie 2 miesiące na dokonanie wpisu do tego wykazu, co może być szczególnie problematyczne. Taki krótki termin stawia sektor przed wyzwaniem szybkiego dostosowania się do nowych wymogów, nawet przed zamknięciem roku obrachunkowego i przed sporządzeniem sprawozdania finansowego. Dodatkowo, wymóg składania oświadczenia o statusie pod rygorem odpowiedzialności karnej (art. 5 ust. 10 ustawy KSC) zwiększa ryzyko dla przedsiębiorstw, które mogą nieświadomie naruszyć ten obowiązek. W efekcie, firmy są zmuszane do prowadzenia ciągłej i często skomplikowanej samooceny, aby uniknąć sankcji karnych za niezłożenie wymaganej deklaracji w odpowiednim terminie. Takie podejście nie tylko generuje dodatkowe, często nieuzasadnione obciążenia dla przedsiębiorstw, ale również potencjalnie odciąga zasoby, które mogłyby być wykorzystane na rzeczywiste wzmocnienie bezpieczeństwa cybernetycznego. Absurdalność tej sytuacji polega na tym, że zamiast faktycznego zwiększania bezpieczeństwa, projekt nowelizacji wprowadza mechanizmy, które skupiają się na spełnianiu formalnych wymogów, zamiast na rzeczywistym adresowaniu zagrożeń cybernetycznych.

18. Wykaz podmiotów kluczowych i ważnych

Jednostka redakcyjna: Art. 7

Przepis przewiduje obowiązek wpisu do wykazu przez podmiot kluczowy i ważny. Wnosimy o wyraźne rozstrzygnięcie sposobu w jaki powinny dokonywać wpisu podmioty, których działalność obejmuje kilka rodzajów usług kluczowych lub ważnych.
Wnioskujemy o jak najszybsze udostępnienie testowej wersji systemu służącego do dokonywania zgłoszeń do rejestru. Sygnalizujemy również, że w zakresie niektórych punktów mogą wystąpić trudności w ich zgłoszeniu: np. pkt 12 (w dużych firmach nie istnieje jeden numer telefonu, inny niż infolinia), pkt 15 (nie każdy podmiot zawrze takie umowy), pkt 17 (nie każdy podmiot zawrze takie porozumienie).

19. Wpis z urzędu

Jednostka redakcyjna: Art. 7 ust. 16

Wyjaśnienia wymaga, w jakich okolicznościach Minister może wpisać określony podmiot z urzędu i czy podmiot może zaprzeczyć istnieniu podstaw do dokonania wpisu. Zastrzeżenie dot. rygoru kary pieniężnej wydaje się zbędne, w przypadku, gdy projekt ustawy zawiera wydzielone przepisy dot. kar. Nie jest zupełnie jasna relacja tego przepisu do

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

projektowanego art. 7a, który również mówi o wpisie do wykazu przez organ właściwy podmiotu.

20. Brak zastosowania zasady proporcjonalności wynikającej z NIS2 przy konstruowaniu wymagań dla zarządzania ryzykiem przez podmioty ważne i kluczowe.

Jednostka redakcyjna: art. 8 ust. 1 pkt 2 projektu KSC
Jednostka redakcyjna NIS2: 21 ust. 1

Uwaga: Artykuł 21 ust. 1 Dyrektywy NIS2 zobowiązuje państwa członkowskie do zapewnienia, że podmioty kluczowe i ważne wdrażają odpowiednie i proporcjonalne środki techniczne, operacyjne oraz organizacyjne. Wykorzystując najnowszą wiedzę oraz normy europejskie i międzynarodowe, podmioty mają zapewnić poziom bezpieczeństwa adekwatny do istniejącego ryzyka. Istotnym elementem jest tutaj uwzględnienie kosztów wdrożenia tych środków przy ocenie ich proporcjonalności, biorąc pod uwagę wielkość podmiotu oraz prawdopodobieństwo wystąpienia incydentów. Artykuł 8 ust. 1 pkt 2 projektu ustawy, który ma na celu implementację tych wymagań, nie zawiera odniesienia do kosztów wdrożenia jako kryterium oceny proporcjonalności środków. Stanowi to znaczącą różnicę w stosunku do dyrektywy, która podkreśla potrzebę uwzględniania tych kosztów w ocenie proporcjonalności środków zarządzania ryzykiem. Ominięcie rozważań dotyczących kosztów może prowadzić do sytuacji, w której podmioty są zobowiązane do realizacji potencjalnie kosztownych inicjatyw bez względu na ich ekonomiczną wykonalność. Może to nałożyć nadmierne obciążenie finansowe na przedsiębiorstwa, zwłaszcza mniejsze, które mogą nie posiadać zasobów pozwalających spełnić takie rygorystyczne standardy bez kompromisów w innych obszarach działalności.

21. Polityki tematyczne

Jednostka redakcyjna: Art. 8 pkt 2 lit a

Przyjmujemy, że wymóg posiadania *„polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne*” stanowi przeniesienie art. 21 ust. 2 lit. a) NIS2 wskazującego na „politykę analizy ryzyka i bezpieczeństwa systemów informatycznych;”. Wnosimy jednak o wyjaśnienie dodanego wobec dyrektywy sformułowania *„w tym polityki tematyczne*”. Nie zostało ono zdefiniowane, a dla precyzji przepisów wydaje się to niezbędne.

22. Łańcuch dostaw

Jednostka redakcyjna: Art. 8 pkt 2 lit. d

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Projektowany przepis zawiera istotne rozszerzenie zakresu badania łańcucha dostaw, wymaganego zgodnie z dyrektywą NIS2 i wprowadza tym samym nadmiarowe obciążenie.
Dyrektywa NIS2 wskazuje na *„bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego **bezpośrednimi** dostawcami lub usługodawcami”*
Wnosimy o przyjęcie następującego brzmienia projektu:
*d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy **bezpośrednim** dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym*

23. Katastrofa

Jednostka redakcyjna: Art. 8 pkt 2 lit e

W doprecyzowaniu dotychczasowego przepisu dodano *„oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie”*.
Sformułowanie „po katastrofie” nie zostało zdefiniowane. Sugerujemy jego usunięcie lub zdefiniowanie, co może być jednak problematyczne. Możliwe jest też jego zastąpienie zwrotem *„po przerwaniu ciągłości jego działania”*.
Z uwagi na potencjalne kary pieniężne konieczne jest zachowanie maksymalnej precyzji pojęć używanych do opisu wymagań.

24. Mapowanie PN

Jednostka redakcyjna: Art. 8 ust. 3

Wnioskujemy o jak najszybsze opublikowanie mapowania wymogów PN na obowiązki wynikające z ustawy i przyszłych rozporządzeń. Wydaje się jednocześnie, że do tego typu zadania nie jest konieczne szczególne upoważnienie ustawowe.

25. Dostawca

Jednostka redakcyjna: Art. 8 ust. 4

Wnosimy o wprowadzenie zmian w pkt 1:
1) *podatności związane z dostawcą sprzętu lub oprogramowania, **o ile zostaną zidentyfikowane w ramach szacowania ryzyka***

Wnosimy o wprowadzenie zmiany w pkt 3:
3) *wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

*wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555", **o ile zostang wydane.***

Wydanie skoordynowanych ocen jest fakultatywne.

26. Uszczegółowienie wymagań

Jednostka redakcyjna: Art. 8a

Odnotowujemy, że w związku z brakiem publikacji projektów rozporządzeń nie jest możliwe odniesienie do ewentualnego dalszego uszczegółowienia wymagań. Tym samym nie jest możliwe dokonanie oceny przyszłych wymagań. W szczególności jednak dalsze uszczegółowienia wymagań w drodze rozporządzenia nie powinny uniemożliwiać stosowania projektowanego art. 8 ust. 2, który wskazuje, że *„Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarzadzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301"*.
Apelujemy, aby projekty rozporządzeń zostały opublikowane jak najszybciej.
Podkreślamy jednocześnie, że przyjęte podejście musi uwzględniać sytuację podmiotów, które będą kwalifikowały się jako kluczowe lub ważne w ramach kilku rodzajów działalności. W upoważnieniu przewiduje się natomiast możliwość wydania różnych rozporządzeń np. wobec działalności telekomunikacyjnej, chmury obliczeniowej lub centrów danych, które często będą łączone w ramach jednego podmiotu. Ewentualne zróżnicowanie wymagań szczegółowych może poważnie utrudniać wdrożenie. W naszej ocenie należy przede wszystkim unikać zróżnicowania wymagań w ramach poszczególnych sektorów.
Poza powyższym, zauważamy również, że zgodnie z samą dyrektywą NIS2: *Do 17 października 2024 r. Komisja przyjmuje akty wykonawcze określające wymogi techniczne i metodykę dotyczącą środków, o których mowa w ust. 2, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych oraz platform sieci społecznościowych i dostawców usług zaufania. Komisja może przyjąć akty wykonawcze określające wymogi techniczne i metodykę, a w razie potrzeby również wymogi sektorowe dotyczące środków, o których mowa w ust. 2, w odniesieniu do podmiotów kluczowych i ważnych innych niż te, o których mowa w akapicie pierwszym niniejszego ustępu.*

Powyższe oznacza, że na obecnym etapie nie jest możliwe odniesienie się do szczegółowych wymagań, a sam projekt ustawy nie dostarcza informacji istotnie wykraczających poza same ogólne sformułowania dyrektywy NIS2. W praktyce ogranicza

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

to możliwość rozpoczęcia przygotowań zorientowanych na osiągnięcie oczekiwanych regulacyjnie efektów.

27. Spółki obrotu

Jednostka redakcyjna: Art. 8b

Projektowany przepis wprowadza obowiązek podmiotów objętych tzw. rozporządzeniem systemowym do stosowania zasad *dotyczących aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, w tym zasad dotyczących wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego odpowiednio*.
Zauważamy, że rozporządzenie obejmuje także spółki obrotu, których dotyczy rzdz. 3 pt. *Sposób prowadzenia obrotu energią elektryczną.* Przepisy te nie dotyczą kwestii cyberbezpieczeństwa w transgranicznych przepływach. Wydaje się, że stosowanie tych wymagań do spółek obrotu jest nieadekwatne i powinno zostać wyraźnie wyłączone.

28. Zakres szkoleń personelu

Jednostka redakcyjna: Art. 8d pkt 4

Projektowany przepis wymaga, aby kierownik zapewniał „*że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna przepisy prawa oraz wewnętrzne regulacje podmiotu w tym zakresie*".
W naszej ocenie przepis ten jest zdecydowanie nadmiarowy i zupełnie pomija specyfikę działania firm, a w szczególności dużych organizacji. Taka redakcja przepisu może być adekwatna jedynie w przypadku podmiotów o ścisłej specjalizacji, gdzie faktyczna wiedza prawna (sic!) jest wymagana dla prawidłowej realizacji obowiązków. Szeroko rozumianym personelem pracowników są też osoby zupełnie niezwiązane z systemami informatycznymi i usługami kluczowymi lub krytycznymi. Wymaganie od nich posiadania specjalistycznej wiedzy prawnej w obszarze cyberbezpieczeństwa jest skrajnie nieuzasadnione. Przyjmujemy oczywiście, że ogólna wiedza o cyberbezpieczeństwie jest istotna z uwagi na różne wektory ataków, ale musi ona być dostosowywana do konkretnych potrzeb na różnych stanowiskach pracy.
W motywie 89 NIS2, wskazano: „*szkolenia dla pracowników oraz szerzyć wiedzę na temat cyberzagrożeń, phishingu lub technik inżynierii społecznej*.". W art. 20 ust. 2 wskazano natomiast, aby państwa członkowskie „***zachęcały** podmioty kluczowe i ważne do oferowania podobnych* (jak kierownikom) *szkoleń ich pracownikom*.".
Z tych względów proponujemy poniższe brzmienie:

4) *zapewnia, że personel podmiotu **ma dostęp do szkoleń dotyczących cyberzagrożeń, phishingu lub technik inżynierii społecznej,** ~~jest świadomy~~ obowiązków z zakresu*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

*cyberbezpieczeństwa**, i zna** przepisów prawa oraz wewnętrznych regulacji podmiotu w tym zakresie;*

29. Brak karalności

Jednostka redakcyjna: Art. 8f ust. 1

Poważne niejasności budzi wymóg potwierdzania niekaralności wszystkich osób wykonujących zadania, o których mowa w art. 8 i 11. W pierwszej kolejności zauważamy, że wymóg ten nie wynika z dyrektywy NIS2 i jest wobec niej nadmiarowy.
Zauważamy, że z uwagi na bardzo rozległy zakres zadań realizowanych na podstawie art. 8 i 11 zadania te będą wykonywane w niektórych organizacjach przez znaczną liczbę osób, a wobec części z nich wymaganie „zaświadczenia", tj. zapewne zaświadczenia z Krajowego Rejestru Karnego będzie nieproporcjonalne.
Postulujemy wprowadzenie wymagania zgodnego z normą ISO 27001, do której odnosi się uzasadnienie projektu. Przewiduje ona środek kontrolny wskazujący, że *Przed dołączeniem do organizacji i na bieżąco należy przeprowadzać badanie przeszłości wszystkich kandydatów na pracowników, z uwzględnieniem obowiązujących przepisów prawa, regulacji i zasad etycznych, a także proporcjonalnie do wymagań działalności, klasyfikacji informacji, do których pracownik ma mieć dostęp, oraz postrzeganego ryzyka*.
W szczególności wymagania dot. potwierdzenia niekaralności powinny zostać ograniczone do zakresu kluczowego personelu definiowanego przez pracodawcę.

30. Wymiana informacji

Jednostka redakcyjna: Art. 8h

W naszej ocenie w ust. 1 należy wprowadzić fakultatywność wymiany informacji, w miejsce aktualnego bezwzględnego obowiązku. Początek ust. 1 powinien więc brzmieć: „*Podmioty kluczowe i podmioty ważne **mogą wymieniać** ~~wymieniają~~ między sobą informacje dotyczące cyberbezpieczeństwa (…)*".

31. Brak zwolnienia sektora bankowego i rynków finansowych z obowiązków wynikających z ustawy KSC wbrew dyrektywie NIS2

Jednostka redakcyjna: art. 8i
Jednostka redakcyjna NIS2: art. 2 ust. 10, załącznik nr 1

Uwaga: Projekt ustawy o krajowym systemie cyberbezpieczeństwa wprowadza zasadniczą różnicę w stosunku do dyrektywy NIS2, która zwalnia sektor bankowy i rynki finansowe z obowiązków dyrektywy. W projekcie ustawy KSC, sektor ten jest zobowiązany do

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

przestrzegania ustawy KSC w zakresie, w jakim nie stosuje on rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554. Tymczasem, zgodnie z art. 2 ust. 10 dyrektywy NIS2, podmioty te są całkowicie wyłączone z obowiązków wynikających z dyrektywy na podstawie zwolnienia. Zgodnie z tym przepisem: *Niniejsza dyrektywa nie ma zastosowania do podmiotów, które państwa członkowskie zwolniły z zakresu stosowania rozporządzenia (UE) 2022/2554 zgodnie z art. 2 ust. 4 tego rozporządzenia.*

To rozwiązanie wydaje się być nie tylko sprzeczne z duchem dyrektywy NIS2, ale także wprowadza dodatkowe, potencjalnie zbędne obciążenia dla sektora bankowego i rynków finansowych. Sektory te są już wysoko regulowane i objęte ścisłymi przepisami dotyczącymi cyberbezpieczeństwa, co czyni obowiązki wynikające z ustawy KSC w najlepszym przypadku redundantnymi, a w najgorszym — generującymi dodatkowe, niepotrzebne koszty administracyjne i operacyjne. Takie podejście nie tylko nie przyczynia się do rzeczywistego wzrostu poziomu cyberbezpieczeństwa, ale może również prowadzić do nadmiernego skomplikowania procesów regulacyjnych w sektorze.

32. Termin rozpoczęcia korzystania z S46

Jednostka redakcyjna: Art. 9

Projektowany przepis wskazuje na rozpoczęcie korzystania z S46 w 2 tygodnie od wpisu do rejestru. Projektowany art. 46 ust. 4 określa, że rozpoczęcie korzystania następuje po wpisie, bez wskazania na termin 2 tygodni. Z kolei z art. 15 ustawy nowelizującej wynika, że *minister właściwy do spraw informatyzacji ogłasza komunikat określający harmonogram rozpoczęcia korzystania* z S46. Co więcej komunikat ten może być *zmieniany jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z* S46.
Poza tym, wątpliwości budzi wskazanie, że podmiot korzysta z s46 w pełnym zakresie funkcji określonych w art. 46 ust. 1. Wśród nich znajdują się takie, które wydają się wykraczać poza jego możliwości, jak np.: *generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa* czy *szacowanie ryzyka na poziomie krajowym.*
Nowe funkcjonalności S46 wynikające z pkt 6 i 7, mają być jednocześnie uruchomione dopiero w okresie do roku od wejścia w życie ustawy, co wynika z art. 16.
Z uwagi na potencjalną karę pieniężną związaną z korzystaniem z S46 kwestia ta wymaga jednoznacznego wyjaśnienia w przepisach ustawy. Wnosimy również o przedstawienie założeń funkcjonowania nowego S46 w ramach spotkania warsztatowego.

33. Dokumentacja

Jednostka redakcyjna: Art. 10

W art. 10 ust. 4 wskazano, że dokumentacja może być prowadzona elektronicznie ALBO papierowo. Wydaje się, że właściwym byłoby użycie alternatywy łącznej, tj. LUB.

34. Obligatoryjny wymóg stosowania norm technicznych

Jednostka redakcyjna: art. 10 ust. 3 pkt 1 i 3 projektu KSC
Jednostka redakcyjna NIS2: art. 21 ust. 1

Uwaga: Zgodnie z art. 10 ust. 3 pkt 1 i 3 projektu ustawy podmioty kluczowe i ważne zobowiązane są do stosowania dokumentacji dotyczącej systemu zarządzania:

(a) bezpieczeństwem informacji wytworzonej zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej;

(b) ciągłością działania usługi wytworzonej zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej.

Jednakże, zgodnie z art. 25 dyrektywy NIS2 normy techniczne nie powinny być stosowane obligatoryjnie. Państwa członkowskie powinny zachęcać do ich stosowania, ale nie wymagać tego. Co więcej, normy techniczne ulegają szybkiej dezaktualizacji, co oznacza, że każda zmiana norm w tym zakresie będzie wymagała przejścia przez cały proces legislacyjny w ramach nowelizacji ustawy. Takich dylematów nie posiada ustawodawca unijny, który odwołuje się do najnowszego stanu wiedzy i odpowiednich norm europejskich (por. art. 21 dyrektywy NIS2, motyw 79).

35. Dokonywanie zgłoszeń do CSIRT sektorowych

Jednostka redakcyjna: Art. 11

Zalecamy utworzenie jednego punktu przyjmowania zgłoszeń incydentów na poziomie krajowym, zwłaszcza w kontekście nowych wymogów dotyczących zgłaszania incydentów w ramach CRA, zamiast oddzielnych „sektorowych" punktów przyjmowania zgłoszeń. Ważne jest, aby uniknąć fragmentacji, podwójnego raportowania i niepotrzebnego obciążenia zarówno dla branży, jak i organów publicznych.

36. Zbyt krótki termin zgłoszeń incydentów dla przedsiębiorców telekomunikacyjnych

Jednostka redakcyjna: Art. 11 ust. 1a

Projekt ustawy przewiduje, że przedsiębiorcy komunikacji elektronicznej mają być zobowiązani do zgłaszania wczesnych ostrzeżeń o incydencie poważnym niezwłocznie, nie później niż w ciągu 12 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego, stanowiąc w ten sposób nieuzasadniony wyjątek od terminu wynoszącego 24 godziny, który mają na zgłoszenie pozostałe podmioty kluczowe i ważne. Wnioskujemy o wykreślenie art.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

11 ust. 1a jako nadmiernego zaostrzenia reżimu raportowania wobec jedynej wybranej grupy, tj. przedsiębiorców telekomunikacyjnych. Zgodnie z NIS2 prawie wszystkie podmioty mają identyczny termin zgłoszenia wczesnego ostrzeżenia, tj. 24 godziny, a jedyny wyjątek przewidziano dla dostawców usług zaufania, którzy w 24 godziny zgłaszają incydent poważny, a nie wczesne ostrzeżenie. Jednocześnie w NIS2 dla żadnej z kategorii nie wprowadzono terminu 12-godzinnego. Zauważamy również, że na gruncie aktualnie obowiązujących przepisów PT nie został określony sztywny termin dokonywania zgłoszeń, a ustalona praktyka współpracy z UKE wskazuje, że obowiązek niezwłocznego zgłoszenia naruszenia uznaje się za spełniony, jeśli zgłoszenie nastąpi w okresie 4-5 dni roboczych.
Raportowanie w terminie 12-godzinnym jest obowiązkiem nieproporcjonalnym. Skoro na poziomie UE nie uznano za zasadne zaostrzania tych wymagań, tym bardziej nie jest uzasadnione jego dokonywania na poziomie krajowym.
Ponadto, zróżnicowanie terminów będzie problematyczne w przypadku operatorów, którzy klasyfikują się także wg innych kategorii usług kluczowych lub ważnych. Oznaczałoby to trudności w ustaleniu właściwego terminu raportowania, tj. czy w związku z tym, że operator jako podmiot kluczowy jako przedsiębiorca telekomunikacyjny, ale też np. jako operator punktu wymiany ruchu powinien raportować w ciągu 12 czy 24 godzin. Także z tego względu, właściwym rozwiązaniem jest wprowadzenie jednolitych wymagań na poziomie 24 godzin.

37. Progi incydentu poważnego

Jednostka redakcyjna: Art. 11 ust. 4

Wnioskujemy o pilne przedstawienie projektu rozporządzenia dot. progów incydentów. Bez jego tekstu nie jest możliwe odniesienie się do potencjalnej uciążliwości wdrożenia obowiązków, ich kosztu oraz czasu niezbędnego na dostosowanie.
Sygnalizujemy, że na etapie prac nad poprzednimi projektami nowelizacji zgłaszaliśmy liczne uwagi dot. uszczegółowienia progów raportowania w ówczesnym projekcie rozporządzenia. Skutkowałyby one ogromnym zwiększeniem liczby incydentów, których większość – w naszej ocenie – nie byłaby faktycznie incydentami zasługującymi na klasyfikację jako incydenty poważne. Liczymy, że uwagi te zostaną uwzględnione w toku prac nad nowym projektem rozporządzenia.
Ponadto zgłaszamy wątpliwości co do obligatoryjnego charakteru upoważnienia w związku z art. 23 ust. 11 NIS2, który wskazuje, że: ***Do dnia 17 października 2024 r. Komisja**, w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych, **przyjmuje akty wykonawcze doprecyzowujące przypadki, w których incydent uznaje się za poważny** zgodnie z ust. 3. Komisja może przyjąć takie akty wykonawcze w odniesieniu do innych podmiotów kluczowych i ważnych.*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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 przypadku wydania w tym samym zakresie przepisów krajowych może wystąpić kolizja norm.

38. Wczesne ostrzeżenie
Jednostka redakcyjna: Art. 12 ust. 1 pkt 5

W art. 12 ust. 1 pkt 5 wskazano, że należy przekazać: *„wskazanie czy incydent poważny wyczerpuje znamiona przestępstwa*". Wymóg ten wymaga przeformułowania zgodnie z brzmieniem NIS2. Dyrektywa wskazuje w tym zakresie następująco*: „w którym w stosownych przypadkach wskazuje się, czy poważny incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze".*
Podmioty kluczowe lub ważne, a w szczególności podmioty prywatne, nie posiadają żadnych uprawnień do dokonywania klasyfikacji czynów jako przestępstw. Takie podmioty mogą natomiast informować o swoich przypuszczeniach lub podejrzeniach co do ew. nieuprawnionego naruszenia ich dóbr, w tym poprzez ew. dokonanie czynności o charakterze przestępstwa. Klasyfikacji zdarzeń jako przestępstw powinny zaś dokonywać uprawnione do tego służby państwowe.

39. Parametry
Jednostka redakcyjna: Art. 12 ust. 3

Art. 12 ust. 3 projektu ustawy zawiera bardzo szczegółowy zestaw parametrów, które należy udostępnić w ramach zgłoszenia incydentu. Zalecamy unikanie takich specyfikacji, ponieważ szablony i rodzaje informacji, które mają być udostępniane, zostaną ujednolicone w całej UE w nadchodzącym akcie wykonawczym dotyczącym zgłaszania incydentów. Ujednolicenie szablonów zgłoszeń w całej UE pomaga w zapewnieniu kompatybilności zgłoszeń, ułatwiając tym samym transgraniczną wymianę i analizę informacji. Pomaga to również firmom, które działają w dwóch lub więcej krajach UE, uniknąć zamieszania prawnego i niepotrzebnych inwestycji zasobów w celu radzenia sobie z różnymi systemami sprawozdawczości.

40. Art. 12 ust. 3 pkt 1 lit. f w zw. z ust. 2
Jednostka redakcyjna: Art. 12 ust. 3 pkt 1 lit. f

Sygnalizujemy, że powtórzona została ta sama norma w dwóch przepisach dot. zgłoszenia incydentu.

f) przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi

2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

41. Brak odpowiedniego zabezpieczenia tajemnicy przedsiębiorstwa w sprawozdaniu końcowym

Jednostka redakcyjna: art. 12a i art. 12b
Jednostka redakcyjna NIS2: 23 ust. 4 lit d)

Uwaga: Art. 12a projektu KSC wymaga, aby sprawozdanie końcowe dotyczące incydentu poważnego zawierało:

- szczegółowy opis incydentu, w tym spowodowane zakłócenia i szkody;
- rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu;
- zastosowane i wdrażane środki ograniczające ryzyko;
- w odpowiednich przypadkach transgraniczne skutki incydentu.

Art. 12b ust. 1 i 2 projektu KSC określają obowiązek składania sprawozdań okresowych i końcowych w przypadku, gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego.
Obowiązek przedstawienia szczegółowego opisu incydentu może wymagać ujawnienia informacji, które są kluczowe dla funkcjonowania przedsiębiorstwa, w tym danych dotyczących jego infrastruktury technicznej, procedur bezpieczeństwa oraz potencjalnych słabych punktów systemu. Takie informacje mogą stanowić tajemnicę przedsiębiorstwa zgodnie z definicją zawartą w art. 11 ust. 4 ustawy o zwalczaniu nieuczciwej konkurencji, która chroni informacje techniczne, technologiczne oraz organizacyjne przedsiębiorstwa, jeżeli nie są one powszechnie znane i mają wartość gospodarczą. Ujawnienie rodzaju zagrożenia lub przyczyny incydentu może odsłonić wrażliwe informacje dotyczące mechanizmów zabezpieczeń stosowanych przez przedsiębiorstwo oraz potencjalnych luk, które mogły zostać wykorzystane przez atakujących. Tego typu informacje, jeśli staną się publiczne, mogą zostać wykorzystane przez konkurencję lub osoby trzecie w sposób szkodliwy dla przedsiębiorstwa. Wymóg raportowania zastosowanych środków ograniczających ryzyko narusza zasadę ochrony tajemnicy przedsiębiorstwa, gdyż może prowadzić do ujawnienia szczegółowych informacji na temat strategii zabezpieczeń, technologii oraz procesów wewnętrznych przedsiębiorstwa. Takie dane mogą być strategicznie istotne i ich ujawnienie może osłabić konkurencyjność firmy oraz zwiększyć ryzyko przyszłych ataków. Art. 51 ust. 2 Konstytucji RP stanowi, że "władze publiczne nie mogą uzyskiwać, gromadzić ani udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym". Ochrona tajemnicy przedsiębiorstwa jest fundamentalnym elementem wolności gospodarczej i praw własności. Przepisy Art. 12a i Art. 12b nie uwzględniają jednak mechanizmów zabezpieczających przed nieuprawnionym dostępem do informacji, które mogą stanowić tajemnicę przedsiębiorstwa.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

42. W Dyrektywie NIS2 wymóg regularnych audytów bezpieczeństwa nie ma zastosowania do podmiotów ważnych

Jednostka redakcyjna: art. 15 ust.1 projektu KSC
Jednostka redakcyjna NIS2: art. 32 ust. 2 lit. b)

Uwaga: Art. 32 ust. 4 lit. b) Dyrektywy NIS2 wprowadza obowiązek objęcia podmiotów kluczowych regularnymi, ukierunkowanymi audytami bezpieczeństwa, które prowadzone są przez niezależną instytucję lub właściwy organ. Audyty te opierają się na oszacowaniach ryzyka przeprowadzonych przez właściwy organ lub badany podmiot, bądź na innych dostępnych informacjach dotyczących ryzyka. Propozycja implementacji tego przepisu w polskim ustawodawstwie rozszerza ten obowiązek na podmioty ważne, co stanowi rozszerzenie w stosunku do wymagań Dyrektywy. Ponadto zgodnie z proponowanymi przepisami, audyt jest obligatoryjny dla wszystkich tych podmiotów, co dwa lata, bez względu na wcześniejsze oszacowanie ryzyka. Oznacza to, że polskie przepisy implementują przepisy NIS2 w sposób nadmierny w tym zakresie. Jest to również istotne dla jednostek samorządu terytorialnego, gdyż nowe przepisy obejmą także te podmioty obowiązkowymi audytami – sam OSR wymienia prawie 28 000 podmiotów jako podmioty z sektora administracji publicznej.

43. Nieprawidłowa forma wpisu operatorów usług kluczowych do wykazu podmiotów kluczowych i ważnych

Jednostka redakcyjna: art. 15 ust. 2 projektu KSC
Jednostka redakcyjna NIS2: 3 ust. 2

Uwaga: Zgodnie z art. 15 ust. 2 projektu KSC, organ właściwy do spraw cyberbezpieczeństwa wpisuje z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych. Niemniej jest to czynność o charakterze materialnym, tj. umieszczenie w wykazie podmiotów ważnych i kluczowych ma charakter materialny, kształtujący prawa i obowiązki operatorów usług kluczowych. Treść tego przepisu pozwala uznać, że wpis stanowi czynność materialno-techniczną, która należą do czynności faktycznych administracji, służących bezpośredniej i praktycznej realizacji konkretnych zadań administracji. Niemniej fakt wpisania do wykazu powinien być realizowany w formie decyzji administracyjnej, ponieważ wpływa na prawa i obowiązki jej adresata. Wpisanie operatora usług kluczowych do wykazu podmiotów kluczowych i ważnych determinuje jego obowiązki i uprawnienia wynikające z ustawy, co jednoznacznie wskazuje na konieczność wydania decyzji administracyjnej, aby zapewnić przejrzystość, pewność prawa i możliwość odwołania się od takiej decyzji. Obecna forma przepisu jest zbyt uproszczona i nie uwzględnia konieczności formalnego uregulowania wpływu na prawa i obowiązki operatorów usług kluczowych.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

44. Niekonstytucyjna forma komunikatu dla harmonogramów złożenia wniosków o wpis do wykazu podmiotów kluczowych i ważnych

Jednostka redakcyjna: art. 15 w zw. z art. 14 ust. 2 projektu KSC
Jednostka redakcyjna NIS2: art. 3 ust. 3

Uwaga: W art. 15 projektu KSC przewiduje się określenie harmonogramu złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych oraz rozpoczęcia korzystania przez te podmioty z systemu S46 w formie komunikatu. Niemniej, regulowanie terminu na realizację obowiązku ustawowego powinno mieć formę rozporządzenia, a nie komunikatu, który nie stanowi źródła prawa. Komunikat nie może bowiem decydować o obowiązkach obywateli i przedsiębiorców. Zgodnie z art. 87 ust. 1 Konstytucji RP, źródłami powszechnie obowiązującego prawa Rzeczypospolitej Polskiej są: Konstytucja, ustawy, ratyfikowane umowy międzynarodowe oraz rozporządzenia. W tym kontekście warto przywołać orzeczenie Trybunału Konstytucyjnego z 9 maja 2023 r. (sygn. akt SK 81/19), w którym stwierdzono niezgodność z ustawą zasadniczą komunikatów określających Program Szczepień Ochronnych na dany rok.[3]. Komunikaty nie mogą bowiem kształtować praw jednostek. Do takiego kształtowania praw dojdzie w sytuacji, gdy określone daty graniczne wpisu do wykazu podmiotów kluczowych i podmiotów ważnych będą regulowane właśnie w formie komunikatu, a nie rozporządzenia. Konieczne jest zatem ograniczenie i doprecyzowanie przepisu art. 15 projektu KSC, aby zapewnić zgodność z konstytucyjnymi wymogami dotyczącymi źródeł powszechnie obowiązującego prawa.[4].

45. Realizacja obowiązków od dnia wpisu do wykazu

Jednostka redakcyjna: art. 16 ust. 1

„art. 16 otrzymuje brzmienie:

„Art. 16. 1. Podmiot kluczowy i podmiot ważny:

1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy,

[3] Zgodnie z tym wyrokiem: Art. 17 ust. 11 ustawy z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi (Dz.U. z 2022 r. poz. 1657, ze zm.) w związku z § 5 rozporządzenia Ministra Zdrowia z dnia 18 sierpnia 2011 r. w sprawie obowiązkowych szczepień ochronnych (Dz.U. z 2022 r. poz. 2172) w zakresie, w jakim termin wymagalności obowiązkowych szczepień ochronnych, jak i liczba dawek poszczególnych obowiązkowych szczepień ochronnych, określone są w Programie Szczepień Ochronnych na dany rok, ogłaszanym przez Głównego Inspektora Sanitarnego w formie komunikatu, a nie przez ministra właściwego do spraw zdrowia, w drodze rozporządzenia, jest niezgodny z art. 47 w związku z art. 31 ust. 3 w związku z art. 87 Konstytucji Rzeczypospolitej Polskiej.

[4]Vide ust. 4 art. 15, zgodnie z którym: *W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych i podmiotów ważnych.*

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 12 miesięcy

– od dnia dokonania wpisu do wykazu, o którym mowa w art. 7 ust. 1.

Z uwagi na objęcie przepisami bardzo szerokiego katalogu podmiotów, także niebędących dotychczas podmiotami krajowego systemu cyberbezpieczeństwa postulujemy wydłużenie terminów na implementację do 12 miesięcy na wdrożenie obowiązków oraz 24 miesiące na przeprowadzenie pierwszego audytu.
Potencjalne podmioty kluczowe lub podmioty ważne nie są w stanie przewidzieć na etapie składania wniosku czy zostaną jako takie podmioty zidentyfikowane, a w przypadku zaniechania samorejestracji – czy nie zostaną wpisane do wykazu z urzędu. Również możliwość dokonania takiego wpisu w dowolnym czasie wymusza konieczność zmiany brzmienia powyższego przepisu

Proponujemy też wskazanie daty dokonania wpisu do wykazu jako daty rozpoczynającej bieg terminu na realizację wymagań. Jest to data pewna, która nie będzie rodziła wątpliwości na etapie ewentualnych kontroli realizacji obowiązków.

46. Działania techniczne i udostępnianie informacji

Jednostka redakcyjna: art. 32 projektu KSC
Jednostka redakcyjna NIS2: art. 10

Uwaga: Art. 32 ust. 1 CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego i incydentu krytycznego. Choć jest to zrozumiałe w kontekście zapewnienia bezpieczeństwa, przepisy nie określają szczegółowo granic tych uprawnień ani warunków, które muszą być spełnione przy wykonywaniu takich działań. Brak precyzyjnych wytycznych może prowadzić do nadużyć i naruszeń praw podmiotów kontrolowanych.
Zgodnie z art. 32 ust. 2 projektu KSC w trakcie koordynacji obsługi incydentu poważnego lub krytycznego, CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego. Problemem jest brak przewidzianej ścieżki odwoławczej od takiego wezwania. Podmioty kluczowe i ważne nie mają możliwości zaskarżenia decyzji, co narusza zasadę prawa do obrony i do sprawiedliwego procesu (art. 45 Konstytucji RP).
Zgodnie z art. 32 ust. 3 projektu KSC CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do podmiotu kluczowego lub podmiotu ważnego o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu. Takie żądanie może

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

obejmować informacje stanowiące tajemnicę przedsiębiorstwa, co może naruszać prawa podmiotów kontrolowanych do ochrony informacji poufnych i własności intelektualnej (art. 64 Konstytucji RP). Ponadto, przepisy nie precyzują, w jaki sposób zapewniona będzie ochrona udostępnionych informacji oraz jakie będą konsekwencje ich nieuprawnionego ujawnienia.
Zgodnie z art. 32 ust. 4 projektu KSC CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5 ustawy KSC, uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach. Choć przekazywanie takich informacji jest zrozumiałe z punktu widzenia poprawy bezpieczeństwa, brak jest gwarancji ochrony przed nadużyciem tych informacji przez osoby trzecie oraz zabezpieczeń przed ich niewłaściwym wykorzystaniem.
Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wykonywania działań technicznych oraz udostępniania informacji technicznych związanych z incydentami poważnymi i krytycznymi, budzą poważne wątpliwości co do ich zgodności z konstytucyjnymi standardami ochrony praw i wolności jednostek. Przede wszystkim, brak przewidzianej ścieżki odwoławczej dla podmiotów kontrolowanych narusza zasadę prawa do obrony i do sprawiedliwego procesu. Ponadto, możliwość żądania udostępnienia informacji stanowiących tajemnicę przedsiębiorstwa bez odpowiednich zabezpieczeń może naruszać prawa do ochrony informacji poufnych i własności intelektualnej.
Niezbędne jest wprowadzenie zmian, które zapewnią zgodność z konstytucyjnymi standardami, w tym mechanizmów ochrony prawnej, transparentności działań oraz poszanowania praw podmiotów kontrolowanych. W szczególności, konieczne jest wprowadzenie procedury odwoławczej oraz ścisłych zabezpieczeń dotyczących ochrony udostępnianych informacji, aby przepisy te mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.

47. Badanie produktów, usług, procesów ICT. Badanie oprogramowania bez gwarancji zabezpieczenia podmiotów, u których badanie miałoby następować

Jednostka redakcyjna: art. 33 projektu KSC
Jednostka redakcyjna NIS2: 20 ust. 1

Z uwagi na potencjalne skutki prowadzenia badania, w tym także przerwanie lub zakłócenie działania usług, wnioskujemy o doprecyzowanie przepisów w zakresie ograniczenia możliwości prowadzenia takiego badania urządzeń lub oprogramowania wobec działających systemów teleinformatycznych służących do świadczenia określonych usług. Wydaje się, że intencją jest prowadzenie tego typu badań w warunkach laboratoryjnych, tudzież systemów wydzielonych na potrzeby badania, a nie zasobów działających w warunkach produkcyjnych i służących świadczeniu usług.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Wnosimy o doprecyzowanie, że badanie, o którym mowa w art. 33 nie jest wykonywane wobec funkcjonujących systemów podmiotów krajowego systemu cyberbezpieczeństwa, ale w środowisku testowym zapewnianym przez dokonujący badania CSIRT.
Jeśli natomiast takie działania miałyby być dopuszczalne, konieczne jest wprowadzenie przepisów dot. odpowiedzialności organu prowadzącego badanie za ew. przerwanie lub zakłócenie działania usługi, w tym dot. odpowiedzialności finansowej, także wobec stron trzecich.

Projektowane przepisy pozwalają na przeprowadzanie badań urządzeń informatycznych i oprogramowania na tzw. "żywym systemie", czyli w środowisku produkcyjnym, co może prowadzić do znaczących zakłóceń w jego działaniu. Przepisy nie przewidują dodatkowych warunków ani zabezpieczeń dotyczących takich działań, co budzi poważne wątpliwości co do ich zgodności z zasadami ochrony praw i wolności jednostek. Zgodnie z art. 33 ust. 1 projektu KSC, CSIRT MON, CSIRT NASK lub CSIRT GOV mogą przeprowadzić badanie urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, mających wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie badania urządzeń i oprogramowania budzą poważne wątpliwości co do ich zgodności z konstytucyjnymi standardami ochrony praw i wolności.
Przepisy przyznają CSIRT szerokie uprawnienia do stosowania technik mających na celu: obserwację i analizę pracy urządzenia lub oprogramowania, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie kodu programowego, translację jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, oraz identyfikację podatności i nieudokumentowanych funkcji.
Tak szerokie uprawnienia mogą prowadzić do naruszenia prawa do prywatności (art. 47 Konstytucji RP) oraz ochrony danych osobowych (art. 51 Konstytucji RP). Przełamywanie zabezpieczeń systemów informacyjnych bez odpowiednich gwarancji ochrony prawnej budzi poważne wątpliwości co do zgodności z konstytucyjnymi standardami ochrony danych osobowych oraz integralności systemów informacyjnych. Ponadto, takie działania mogą naruszać prawa do ochrony własności intelektualnej (art. 64 Konstytucji RP) oraz prawa autorskie.
Przepis ten stwierdza, że CSIRT prowadząc badanie, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, które ograniczałyby możliwość przeprowadzenia badania. Takie sformułowanie budzi wątpliwości co do zgodności z zasadą ochrony własności (art. 64 Konstytucji RP) oraz zasadą rzetelnej legislacji (art. 2 Konstytucji RP). Naruszenie warunków umów licencyjnych bez zgody stron może prowadzić do poważnych konsekwencji prawnych i gospodarczych dla właścicieli oprogramowania oraz usług ICT.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Przepis ten twierdzi, że badanie nie narusza autorskich praw osobistych oraz majątkowych oraz nie wymaga zgody licencjodawcy lub dysponenta produktu ICT, usługi ICT lub procesu ICT. Takie sformułowanie może być sprzeczne z art. 64 ust. 1 Konstytucji RP, który gwarantuje ochronę praw majątkowych, w tym praw autorskich. Pominięcie konieczności uzyskania zgody licencjodawcy na przeprowadzanie badań może naruszać umowne prawa stron oraz prowadzić do naruszeń prawa autorskiego i własności intelektualnej.
Przepis ten stwierdza, że postanowienia umów sprzeczne z przepisami ust. 1–1d są nieważne. Taka generalna klauzula może prowadzić do niepewności prawnej i podważać zaufanie do państwa i jego prawa (art. 2 Konstytucji RP). Ograniczenie możliwości swobodnego zawierania umów i określania ich warunków może być sprzeczne z zasadą wolności gospodarczej (art. 20 i art. 22 Konstytucji RP).
Projektowane przepisy dotyczące uprawnień CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie badania urządzeń i oprogramowania mogą prowadzić do poważnych naruszeń konstytucyjnych praw i wolności jednostek. Przede wszystkim, szerokie uprawnienia do przełamywania zabezpieczeń, uzyskiwania dostępu do danych i analizowania kodu programowego bez odpowiednich gwarancji ochrony prawnej budzą poważne wątpliwości co do zgodności z prawem do prywatności, ochrony danych osobowych oraz własności intelektualnej.
Brak związania CSIRT umowami licencyjnymi i postanowienia o nieważności sprzecznych postanowień umów mogą prowadzić do niepewności prawnej i podważać zasady wolności gospodarczej oraz ochrony własności. Niezbędne jest wprowadzenie zmian, które zapewnią zgodność z konstytucyjnymi standardami, w tym mechanizmów ochrony prawnej, transparentności działań oraz poszanowania praw majątkowych i autorskich podmiotów kontrolowanych. Tylko wtedy przepisy te będą mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.

48. Nieograniczony i potencjalnie niewłaściwy dostęp do systemów informatycznych przez CSIRT-y

Jednostka redakcyjna: rozdział rozdział 6a projektu ustawy KSC
Jednostka redakcyjna NIS2: art. 20 ust. 1

Uwaga: Propozycja zawarta w rozdziale 6a ustawy KSC, umożliwiająca CSIRT MON, CSIRT NASK i CSIRT GOV przeprowadzanie dowolnych badań oprogramowania lub sprzętu w celu identyfikacji podatności, bez przestrzegania wymogów licencyjnych, budzi poważne zastrzeżenia. W świetle proponowanych przepisów, te jednostki będą mogły m.in. odtwarzać źródłową postać oprogramowania, powielać kod programowy, przełamywać zabezpieczenia, czy identyfikować nieudokumentowane funkcje. Brak w przepisach jakiejkolwiek odpowiedzialności Skarbu Państwa za potencjalne zniszczenie systemów lub danych podczas takich działań jest kolejnym aspektem, który budzi wątpliwości. To zaniechanie legislacyjne może prowadzić do poważnych konsekwencji finansowych i operacyjnych dla

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

przedsiębiorstw posiadających kluczowe i ważne systemy informatyczne. Ostatecznie, brak odpowiednich zabezpieczeń i gwarancji, zarówno prawnych, jak i technicznych, dotyczących postępowania z uzyskanymi materiałami, pozostaje poważnym niedociągnięciem, które może osłabić zaufanie do krajowego systemu cyberbezpieczeństwa oraz prowadzić do dalszych nadużyć i szkód – przecież zespoły nie będą za każdym razem niszczyć dysków na których przechowywały dane materiały (co do zasady tylko fizyczne zniszczenie danych, daje gwarancje braku dostępu do nich).

49. Oceny bezpieczeństwa naruszające podstawowe zasady państwa prawa

Jednostka redakcyjna: Art. 36a – 36d
Jednostka redakcyjna NIS2: art. 20 ust. 1

Uwaga: Projektowane przepisy dotyczące oceny bezpieczeństwa systemów informacyjnych, zawarte w art. 36a–36d, budzą liczne wątpliwości pod względem ich zgodności z konstytucyjnymi standardami ochrony praw i wolności jednostek.

Przede wszystkim, art. 36b ust. 1 pkt 2 pozwala na przeprowadzenie oceny bezpieczeństwa systemu informacyjnego na zlecenie organu właściwego do spraw cyberbezpieczeństwa, bez konieczności uzyskania zgody podmiotu kontrolowanego. Taki poziom ingerencji może naruszać konstytucyjnie chronione prawa do prywatności (art. 47 Konstytucji RP) oraz prawa do ochrony własności (art. 64 Konstytucji RP). Przeprowadzanie testów bezpieczeństwa, które mogą obejmować przełamywanie zabezpieczeń systemów informacyjnych, stwarza ryzyko naruszenia integralności i poufności danych. To jest szczególnie niepokojące, ponieważ art. 36b ust. 4 i 5 projektu KSC zezwalają CSIRT na używanie urządzeń i programów komputerowych do przełamywania zabezpieczeń systemów informacyjnych. Brak odpowiednich mechanizmów ochrony prawnej i kontroli nad użyciem takich narzędzi może prowadzić do nieuzasadnionych naruszeń praw jednostek i podmiotów gospodarczych, co może być sprzeczne z zasadą ochrony prawnej prywatności i własności.

Projektowane przepisy nie przewidują także mechanizmów odszkodowawczych w przypadku wystąpienia szkód wynikających z przeprowadzenia oceny bezpieczeństwa. Art. 36b ust. 2 projektu KSC stwierdza, że ocena bezpieczeństwa nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym. Niemniej jednak, przepisy nie określają mechanizmu odszkodowawczego w przypadku, gdyby takie zniszczenie jednak miało miejsce. Brak takiego mechanizmu może być uznany za sprzeczny z art. 77 ust. 1 Konstytucji RP, który gwarantuje prawo do wynagrodzenia szkody wyrządzonej przez niezgodne z prawem działanie organów władzy publicznej.

Kolejnym problemem jest brak transparentności w przepisach dotyczących trybu i warunków przeprowadzania oceny bezpieczeństwa. Art. 36b ust. 3 projektu KSC przewiduje, że CSIRT uzgadnia z podmiotem kontrolowanym tryb i ramowe warunki przeprowadzania oceny bezpieczeństwa, jednak brak jest precyzyjnych wytycznych dotyczących tego procesu. Brak transparentności może prowadzić do nadużyć i naruszeń praw podmiotów kontrolowanych,

co może być sprzeczne z zasadą zaufania obywateli do państwa i jego prawa, wynikającą z art. 2 Konstytucji RP.
Przepisy dotyczące używania urządzeń i programów komputerowych do przełamywania zabezpieczeń systemów informacyjnych (art. 36b ust. 4 i 5 projektu KSC) mogą również prowadzić do naruszenia prawa do prywatności oraz ochrony danych osobowych. Przełamywanie zabezpieczeń bez odpowiednich gwarancji ochrony prawnej budzi poważne wątpliwości co do zgodności z art. 51 Konstytucji RP, który chroni dane osobowe i zobowiązuje organy publiczne do ochrony prywatności jednostki.
Dodatkowo, informowanie o wykrytych podatnościach, jak przewiduje art. 36c ustawy o KSC, może prowadzić do naruszenia tajemnicy przedsiębiorstwa i innych chronionych informacji. Przepisy nie zawierają wystarczających zabezpieczeń, aby chronić te informacje przed nieuprawnionym ujawnieniem, co może być sprzeczne z art. 61 Konstytucji RP, gwarantującym prawo dostępu do informacji publicznej, ale z wyłączeniem informacji chronionych prawem.
Podsumowując, projektowane przepisy dotyczące oceny bezpieczeństwa systemów informacyjnych wymagają istotnych zmian, aby zapewnić zgodność z konstytucyjnymi standardami ochrony praw i wolności jednostek. Niezbędne jest wprowadzenie mechanizmów odszkodowawczych, szczegółowych procedur gwarantujących transparentność i zgodność działań z obowiązującymi przepisami oraz mechanizmów weryfikacji poprawności działań kontrolnych. Tylko wtedy przepisy te będą mogły skutecznie chronić interesy podmiotów kontrolowanych i zapewnić zgodność z zasadami konstytucyjnymi.

50. Nieproporcjonalne uprawnienia Ministra Cyfryzacji do dostępu do wrażliwych danych osobowych (art. 39a ustawy KSC)

Jednostka redakcyjna: art. 39a KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Art. 39a ustawy KSC, który upoważnia Ministra Cyfryzacji do dostępu do danych osobowych o szczególnie wrażliwym charakterze, budzi poważne obawy dotyczące prywatności i ochrony danych osobowych. Mowa tutaj o danych, których przetwarzanie jest szczegółowo regulowane przez art. 9 ust. 1 i art. 10 RODO, obejmujących informacje o rasie, orientacji seksualnej, poglądach politycznych, przekonaniach religijnych, przynależności do związków zawodowych, a także dane genetyczne, biometryczne oraz zdrowotne. Chociaż koncepcja serwisu umożliwiającego użytkownikom weryfikację, czy ich dane zostały w sposób nieuprawniony ujawnione, jest wartościowa, to jednak zapisy pozwalające na dostęp do tak delikatnych informacji przez organ administracji publicznej, bez wyraźnych, restrykcyjnych zabezpieczeń i ograniczeń, są niepokojące. Jest to szczególnie problematyczne w świetle wymagań RODO, które nakłada na państwa członkowskie

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

obowiązek zapewnienia wysokiego poziomu ochrony danych osobowych, w szczególności tych o wrażliwym charakterze.

Brak jasnych mechanizmów kontrolnych, przejrzystości działań oraz odpowiednich środków zabezpieczających te dane przed nadużyciem stanowi realne zagrożenie dla praw i wolności obywateli, co może prowadzić do nadmiernej inwigilacji i naruszenia prywatności przez państwo. Tego typu uprawnienia powinny być otoczone szczególną ostrożnością i zabezpieczone solidnymi gwarancjami proceduralnymi oraz nadzorcami, aby zapobiec jakimkolwiek nadużyciom.

51. Kontrowersje wokół możliwości powierzenia funkcji CSIRT sektorowego państwowym osobom prawnym (art. 44a ustawy KSC)

Jednostka redakcyjna: art. 44a projektu KSC
Jednostka redakcyjna NIS2: art. 15

Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który zakłada możliwość powierzenia funkcji CSIRT sektorowego różnorodnym państwowym osobom prawnym, wzbudza poważne wątpliwości co do skuteczności i właściwości takiego rozwiązania. Zgodnie z art. 44a ustawy KSC, funkcję tę mogą pełnić m.in. agencje wykonawcze, instytucje kultury, jednostki naukowe Polskiej Akademii Nauk, uczelnie publiczne oraz parki narodowe. Przykładowo mogą to być takie podmioty jak: Polski Instytut Sztuki Filmowej; Narodowy Instytut Fryderyka Chopina; Zakład Narodowy imienia Ossolińskich; Akademia Kopernikańska; uczelnia publiczna; Instytut Współpracy Polsko-Węgierskiej im. Wacława Felczaka; Instytut Rozwoju Języka Polskiego im. świętego Maksymiliana Marii Kolbego; czy dowolne przedsiębiorstwo państwowe. Przekazanie odpowiedzialności za cyberbezpieczeństwo sektora tak zróżnicowanym podmiotom, które często nie mają odpowiednich kompetencji, doświadczenia, ani struktur do efektywnego zarządzania kwestiami bezpieczeństwa informacyjnego, stawia pod znakiem zapytania racjonalność i efektywność takiego rozwiązania. Cyberbezpieczeństwo wymaga specjalistycznej wiedzy i narzędzi, a także szybkiej reakcji na incydenty, co w przypadku wielu wymienionych instytucji może być trudne do osiągnięcia. Nawet potencjalna możliwość powierzenia takich funkcji może budzić poważne zastrzeżenia.

52. Zakres korzystania z S46 przez podmioty kluczowe i ważne

Jednostka redakcyjna: Art. 46 ust. 4

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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. 46 ust. 4 wskazano ogólnie, że: *Podmioty kluczowe i podmioty ważne, inne niż w ust. 2, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, po uzyskaniu wpisu w wykazie podmiotów kluczowych i podmiotów ważnych*.
W naszej ocenie przepis ten wymaga doprecyzowania w świetle faktycznych obowiązków podmiotów kluczowych i ważnych wynikających z przepisów art. 8-15. W szczególności podmioty takie nie są uprawnione/zobowiązane do realizacji poniższych zadań przypisanych do S46:

> *2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;*
> *4) szacowanie ryzyka na poziomie krajowym;*
> *5) ostrzeganie o cyberzagrożeniach;*
> *6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;*

53. Termin dostosowania do S46

Jednostka redakcyjna: Art. 46 ust. 6

Niejasna jest relacja wymagań technicznych, do których należy się dostosować w ciągu 3 miesięcy od ich publikacji do terminu rozpoczęcia korzystania z systemu w ciągu 2 tygodni od wpisu do wykazu (wyżej uwagi do art. 9), a także art. 46 ust. 4 (korzystanie po wpisie) oraz art. 15 dotyczącego komunikatu o harmonogramie rozpoczęcia korzystania.
W szczególności nie jest jasne czy przed spełnieniem wymagań technicznych (które zostaną opublikowane w nieznanym terminie po wejściu w życie ustawy) możliwe będzie prawidłowe korzystanie z S46.
Kwestie te nie zostały wyjaśnione w uzasadnieniu i w naszej ocenie wymagają jednoznacznego rozstrzygnięcia.
Ponadto sygnalizujemy, że na obecnym etapie nie jest możliwe odniesienie się do tego czy 3 miesięczny termin na wdrożenie wymagań będzie wystarczający. Nie są bowiem znane jakiekolwiek założenia techniczne (poza tym, że ma to być wersja chmurowa) dot. nowej wersji S46 i tym samym nie jest jasne jakiego rodzaju zmian będzie wymagało dostosowanie. Zauważamy, że dokonywanie istotnych zmian w systemach informatycznych dużych podmiotów jest wielokrotnie zadaniem skomplikowanych, które wymaga wielomiesięcznych przygotowań oraz zapewnienia odpowiedniego budżetu.
Z tego względu wnioskujemy o wydłużenie terminu na dostosowanie do 6 miesięcy, z możliwością ewentualnego wcześniejszego zgłoszenia gotowości.

54. Zastosowanie procedur zawieszenia działalności bez zachowania gwarancji proceduralnych znanych z NIS2

Jednostka redakcyjna: art. 53 projektu KSC
Jednostka redakcyjna NIS2: art. 32 ust. 5

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwaga: Zgodnie z art. 32 ust. 5 dyrektywy NIS2, tymczasowe zawieszenie lub zakaz prowadzenia działalności powinno być stosowane z zachowaniem odpowiednich gwarancji proceduralnych, zgodnych z ogólnymi zasadami prawa Unii Europejskiej oraz z Kartą Praw Podstawowych Unii Europejskiej. Do tych gwarancji należą prawo do skutecznej ochrony prawnej, rzetelny proces sądowy, domniemanie niewinności oraz prawo do obrony. Zaproponowana implementacja tego przepisu w art. 53 ust. 8 i kolejnych projektu ustawy nie zawiera takich gwarancji proceduralnych. Trudno uznać za gwarancję proceduralną samą możliwość przedstawienia swojego stanowiska przed organem do spraw cyberbezpieczeństwa, gdyż to ten sam organ (lub inny działający na jego wniosek) podejmuje decyzję o cofnięciu, zawieszeniu odpowiedniej koncesji lub wykreśleniu z rejestru.

55. Nadmiarowe przepisy w zakresie nadzoru, naruszające normy konstytucyjne w zakresie proporcjonalności

Jednostka redakcyjna: art. 53 projektu KSC
Jednostka redakcyjna NIS2: art. 33

Uwaga: Art. 53 ust. 2 pkt 1 projektu KSC nie przewiduje przeprowadzania kontroli doraźnych przez organy właściwe do spraw cyberbezpieczeństwa – a żaden inny przepis nie przewiduje takiej kontroli (także przepisy ustawy – Prawo przedsiębiorców). Zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa. Brak wskazania kontroli doraźnych w przepisach podważa możliwość powołania się na te przepisy.
Art. 53 ust. 2 pkt 3 projektu KSC przewiduje ocenę bezpieczeństwa systemu informacyjnego podmiotów ważnych jako nadzór o charakterze ex ante, a nie ex post. W konsekwencji, podmioty mogą być niepotrzebnie obciążane dodatkowymi obowiązkami, co narusza ich prawo do swobodnego prowadzenia działalności gospodarczej (art. 22 Konstytucji RP). Dyrektywa NIS2, w szczególności motyw 58 oraz art. 29, przewiduje nadzór ex post wobec podmiotów ważnych, co podkreśla, że nadzór ten powinien być stosowany głównie po wystąpieniu incydentu lub naruszenia, a nie przed (jak proponuje się to w art. 53 ust. 2 pkt 3 projektu KSC).
Projekt ustawy nie precyzuje formy poszczególnych czynności, takich jak zlecenie CSIRT, wniosek o udzielenie dostępu do danych, czy postanowienia. Brak jasności w tej kwestii narusza zasadę pewności prawa (art. 2 Konstytucji RP), która wymaga, aby przepisy były precyzyjne i przewidywalne. Nieokreśloność formy czynności administracyjnych może prowadzić do arbitralności działań administracji, co jest sprzeczne z zasadą demokratycznego państwa prawa. W szczególności art. 53 ust. 5 pkt 1 projektu KSC przewiduje możliwość nakazania podjęcia określonych czynności dotyczących obsługi incydentu bez formy decyzji administracyjnej. Takie rozwiązanie narusza prawo do ochrony praw majątkowych (art. 64 Konstytucji RP) oraz prawo do sądu (art. 45 Konstytucji RP), ponieważ podmioty nie mają możliwości zaskarżenia takiego nakazu. Nakazy ingerujące w podstawowe swobody

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

prowadzenia działalności gospodarczej powinny być wydawane w formie decyzji administracyjnej, aby zapewnić podmiotom prawo do obrony i kontroli sądowej.
Brak możliwości złożenia wniosku o ponowne rozpatrzenie sprawy, przewidziany w art. 53 ust. 7 projektu KSC, budzi wątpliwości w kontekście art. 78 Konstytucji RP, który gwarantuje każdemu prawo do zaskarżenia decyzji wydanej w pierwszej instancji. Ograniczona rola sądownictwa administracyjnego i brak kompetencji do zajmowania się kompleksową tematyką cyberbezpieczeństwa dodatkowo potęgują te wątpliwości, ponieważ podmioty nie mają realnej możliwości obrony swoich praw w pełnym postępowaniu administracyjnym.
Wymóg przedstawienia wstępnego stanowiska w ciągu 7 dni, o którym mowa w art. 53 ust. 11-12 projektu KSC, nie zastępuje rzetelnego, sprawiedliwego postępowania administracyjnego, w którym podmiot ma prawo do obrony swoich praw.

56. Nieproporcjonalność nadzoru i rygory sankcji

Jednostka redakcyjna: art. 53 ust. 8 projektu KSC
Jednostka redakcyjna NIS2: art. 20 ust. 1

Uwaga: Artykuł 53 ust. 8 ustawy KSC wprowadza niezmiernie surowe sankcje, pozwalające organom nadzoru cyberbezpieczeństwa na zawieszenie, ograniczenie lub cofnięcie koncesji do czasu usunięcia przez podmiot kluczowy lub ważny stwierdzonych uchybień lub zaprzestania naruszeń. Co więcej, umożliwia to również wykreślenie podmiotu z rejestru (np. z rejestru przedsiębiorców telekomunikacyjnych Prezesa Urzędu Komunikacji Elektronicznej), co w praktyce może oznaczać natychmiastowe i całkowite zaprzestanie prowadzenia działalności przez danego przedsiębiorcę, jak na przykład w przypadku przedsiębiorcy telekomunikacyjnego, który musiałby natychmiast przerwać świadczenie usług telekomunikacyjnych.

Tak drastyczne uprawnienia nadzorcze mogą prowadzić do nadmiernie surowych konsekwencji dla podmiotów, których naruszenia mogą być stosunkowo niewielkie, jak na przykład nieprzeprowadzenie audytu bezpieczeństwa. Wprowadzenie takiego mechanizmu, który może efektywnie „zamknąć" działalność podmiotu na podstawie stwierdzenia administracyjnego bez adekwatnego procesu sądowego lub bez możliwości skutecznego odwołania, jest wysoce nieproporcjonalne.

Przewidziane sankcje mogą nie tylko nieodwracalnie zaszkodzić firmom, które z różnych przyczyn mogą czasowo nie spełniać określonych wymogów, ale również destabilizować sektory gospodarki, wpływając na gospodarkę narodową i bezpieczeństwo usług. Odpowiednie byłoby zatem przemyślenie skali sankcji oraz wprowadzenie bardziej zrównoważonych i proporcjonalnych środków naprawczych, które pozwoliłyby na kontynuację działalności przy jednoczesnym zapewnieniu odpowiednich działań naprawczych, zamiast automatycznego i drastycznego zakończenia działalności.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

57. Brak szczegółowego uzasadnienia podjętych lub planowanych środków w ramach procedury wstępnego informowania i uzasadnienie działań w zakresie zawieszenia działalności

Jednostka redakcyjna: art. 53 ust. 11
Jednostka redakcyjna NIS2: art. 32 ust. 8

Uwaga: Artykuł 53 ust. 11 projektu ustawy proponuje procedurę wstępnego informowania o działaniach mających na celu wydanie decyzji lub podjęcie działań polegających na tymczasowym zawieszeniu działalności. Jednakże zgodnie z art. 32 ust. 8 NIS2, istnieje wymóg szczegółowego uzasadnienia zastosowanych środków z zakresu egzekwowania przepisów. W związku z tym nie jest jasne, w jakim stopniu działania organów właściwych do spraw cyberbezpieczeństwa będą należycie uzasadniane, co stanowi bezwzględny warunek umożliwiający polemikę z danym rozstrzygnięciem.

58. Termin przekazania danych, informacji i dokumentów

Jednostka redakcyjna: Art. 53c ust. 2 pkt 5

W związku z potencjalnie szerokim zakresem niezbędnych do zgromadzenia i przekazania danych wnioskujemy o dookreślenie, że wskazanie terminu jest proporcjonalne do zakresu żądania, a minimalny termin jest określany na 14 dni, a nie 7 jak w projekcie.

59. Uprawnienia urzędnika monitorującego

Jednostka redakcyjna: Art. 53d ust. 1

Z uwagi na bardzo szerokie, projektowane uprawnienia urzędnika monitorującego, wnioskujemy, aby w szczególności w przypadku pkt 1 (swobodny wstęp i poruszanie się po terenie bez obowiązku uzyskania przepustki) oraz pkt 5 (przeprowadzenie oględzin), czynności te odbywały się po wcześniejszym zawiadomieniu podmiotu kluczowego. Jest to istotne w celu umożliwienia prawidłowego wykonywania czynności urzędnika.

60. Tłumaczenia na język polski

Jednostka redakcyjna: Art. 56 ust. 3

Wnioskujemy o doprecyzowanie przepisu o wskazanie, że tłumaczenia są przygotowywane na uzasadniony wniosek organu kontrolującego, w którym wskazany jest związek wniosku z faktycznym zakresem kontroli oraz zakres w jakim dany dokument miałby zostać przetłumaczony.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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 naszej ocenie wyłączone z tego zakresu powinny zostać dokumenty zawierające normy techniczne. Tłumaczenie tego typu dokumentów (których często nie realizuje nawet PKN wdrażając normy europejskie) byłoby obowiązkiem bardzo kosztownym i czasochłonnym dla podmiotu kontrolowanego. W powszechnym obrocie często wykorzystywane są wersje w języku angielskim.

61. Zbyt krótki termin na wniesienie zastrzeżeń do protokołu kontroli

Jednostka redakcyjna: art. 58 ust. 4 projektu KSC
Jednostka redakcyjna NIS2: 32

Uwaga: Zgodnie z art. 58 ust. 4 projektu KSC, "*Kontrolowany ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu go do podpisu*." Wydłużenie terminu na zgłoszenie zastrzeżeń do protokołu kontroli do minimum 14 dni jest uzasadnione z uwagi na złożoność materii kontroli, potrzebę konsultacji i zbierania informacji oraz porównanie z analogicznymi przepisami w innych ustawach. Dodatkowo, projektowane przepisy powinny uwzględniać bardziej szczegółowe procedury odwoławcze, dostęp do informacji, mechanizmy kontrolne oraz kwestie proceduralne, aby skutecznie zagwarantować prawa podmiotów kontrolowanych. Proponowany termin 7 dni jest zbyt krótki, aby kontrolowany podmiot mógł dokładnie przeanalizować protokół, skonsultować się z odpowiednimi specjalistami oraz przygotować umotywowane zastrzeżenia. Wydłużenie tego terminu jest niezbędne dla zapewnienia rzetelności procesu kontroli oraz ochrony praw kontrolowanych podmiotów.

62. *Superfluum* ustawowe w zakresie upoważnienia dyrektora, zastępcy dyrektora departamentu lub naczelnika wydziału

Jednostka redakcyjna: art. 61 ust. 6 projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Z Zgodnie z art. 268a Kodeksu postępowania administracyjnego (kpa), organ administracji publicznej, któremu przysługuje prawo do wydawania decyzji administracyjnych, może upoważnić do tego inną osobę. Upoważnienie takie musi być wyraźnie określone w przepisach prawa lub wynikać z upoważnienia ustawowego. Oznacza to, że delegowanie kompetencji musi być jasno sprecyzowane i wynikać bezpośrednio z norm prawnych. Art. 268a kpa już teraz precyzyjnie reguluje możliwość delegowania kompetencji w ramach administracji publicznej. Wprowadzenie dodatkowych przepisów, które pozwalają pełnomocnikowi ds. cyberbezpieczeństwa upoważniać dyrektora, zastępcę dyrektora lub naczelnika do realizacji swoich zadań, jest zbędne, ponieważ art. 268a kpa wystarczająco normuje te kwestie. Przepis art. 61 ust. 6 projektu KSC jest więc zbędny, gdyż dodaje regulacje, które są już wystarczająco uregulowane w istniejących przepisach prawa. Przepis ten powinien zostać ograniczony lub usunięty, aby uniknąć nadmiarowości legislacyjnej i zapewnić przejrzystość regulacji prawnych.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

63. Brak ograniczenia zakresu uprawnień Pełnomocnika do żądania pomocy

Jednostka redakcyjna: art. 61 ust. 7 projektu KSC
Jednostka redakcyjna NIS2: 32

Uwaga: Proponowany przepis nie precyzuje ograniczeń zakresu pomocy, jaką organy administracji rządowej oraz jednostki organizacyjne mają obowiązek udzielać Pełnomocnikowi. Przykładem bardziej precyzyjnego sformułowania jest art. 9 ustawy o obronie ojczyzny, który wskazuje, że pomoc ma być udzielana "w zakresie swojego działania". Brak takiego ograniczenia może prowadzić do niejasności i nadmiernego obciążenia tych organów obowiązkami, które mogą wykraczać poza ich podstawowe zadania i kompetencje. Przepis ten, w obecnym brzmieniu, może kolidować z innymi regulacjami prawnymi dotyczącymi ochrony danych osobowych, tajemnicy służbowej czy poufności informacji. Bez odpowiednich ograniczeń, organy administracji rządowej mogą być zmuszone do udostępniania informacji, które są chronione innymi przepisami prawa, co może prowadzić do naruszeń prawa i sankcji. Dodatkowo, przepis ten nie zawiera żadnych mechanizmów kontrolnych ani proceduralnych, które zapewniałyby właściwe zarządzanie udzielaniem pomocy. Wprowadzenie takich mechanizmów pozwoliłoby na lepsze monitorowanie i koordynowanie działań oraz zapobieganie potencjalnym nadużyciom. Obecny brak precyzyjnych ograniczeń i mechanizmów kontrolnych może prowadzić do niejasności i potencjalnych problemów w praktycznym stosowaniu tego przepisu.

64. Brak udziału Prezesa Urzędu Komunikacji Elektronicznej w pracach Kolegium ds. Cyberbezpieczeństwa a także w pracach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa

Jednostka redakcyjna: art. 62a i 66 projektu KSC
Jednostka redakcyjna NIS2: 13 ust. 1

Uwaga: Zgodnie z art. 66 ustawy o krajowym systemie cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa stanowi organ doradczy w sprawach dotyczących krajowego systemu cyberbezpieczeństwa. Kolegium to ma na celu koordynację działań na rzecz poprawy cyberbezpieczeństwa na poziomie krajowym oraz zapewnienie spójności działań podejmowanych przez różne podmioty zaangażowane w ochronę cyberprzestrzeni.
Prezes Urzędu Komunikacji Elektronicznej (UKE) posiada szczególne kompetencje oraz wiedzę w zakresie zarządzania i regulacji rynku telekomunikacyjnego. Jego doświadczenie i znajomość specyfiki sektora telekomunikacyjnego są nieocenione w kontekście tworzenia i wdrażania polityki cyberbezpieczeństwa. Prezes UKE będzie odpowiedzialny za nadzór nad procesem wymiany urządzeń i infrastruktury telekomunikacyjnej dostawcy uznanego za dostawcę wysokiego ryzyka. W ramach tego zadania, Prezes UKE będzie musiał współpracować z podmiotami krajowego systemu cyberbezpieczeństwa, aby zapewnić, że wymiana ta nie wpłynie negatywnie na ciągłość działania sieci oraz na poziom

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

bezpieczeństwa telekomunikacyjnego. Włączenie Prezesa UKE w prace Kolegium ds. Cyberbezpieczeństwa umożliwi skuteczniejszą koordynację tych działań oraz szybsze reagowanie na potencjalne zagrożenia.
Zgodnie z art. 192 ustawy Prawo telekomunikacyjne, Prezes UKE jest odpowiedzialny za podejmowanie działań mających na celu zapewnienie bezpieczeństwa publicznego oraz ochrony interesów użytkowników końcowych. Jego udział w Kolegium ds. Cyberbezpieczeństwa jest więc naturalnym rozszerzeniem jego obowiązków i kompetencji w zakresie ochrony infrastruktury krytycznej telekomunikacyjnej. Obecność Prezesa UKE w Kolegium ds. Cyberbezpieczeństwa pozwoli na zapewnienie spójności działań podejmowanych przez różne podmioty w zakresie cyberbezpieczeństwa. Prezes UKE, jako członek Kolegium, będzie mógł lepiej koordynować działania telekomunikacyjne z innymi obszarami cyberbezpieczeństwa, co jest kluczowe w przypadku złożonych zagrożeń cybernetycznych, które często obejmują wiele sektorów.
Artykuł 66 ustawy o krajowym systemie cyberbezpieczeństwa przewiduje możliwość powoływania do Kolegium przedstawicieli różnych organów administracji publicznej, którzy mają istotne znaczenie dla bezpieczeństwa cyberprzestrzeni. Biorąc pod uwagę kluczową rolę Prezesa UKE w nadzorze nad telekomunikacją oraz jego zaangażowanie w działania związane z bezpieczeństwem tej infrastruktury, włączenie go do Kolegium jest w pełni uzasadnione.
Włączenie Prezesa Urzędu Komunikacji Elektronicznej do Kolegium ds. Cyberbezpieczeństwa oraz do Połączonego Centrum Operacyjnego Cyberbezpieczeństwa jest nie tylko logiczne, ale również niezbędne dla zapewnienia skutecznej i spójnej ochrony cyberprzestrzeni w Polsce. Jego doświadczenie, kompetencje oraz nowe obowiązki związane z nadzorem nad wymianą urządzeń i infrastruktury telekomunikacyjnej dostawców wysokiego ryzyka stanowią silne argumenty za jego udziałem w tych pracach. Zapewni to lepszą koordynację działań, zwiększy efektywność podejmowanych środków oraz przyczyni się do podniesienia poziomu bezpieczeństwa telekomunikacyjnego w kraju.

65. Wiążąca forma rekomendacji Pełnomocnika pomimo rzekomo niewiążącej formy

Jednostka redakcyjna: art. 67a projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: W myśl przepisów Konstytucji RP, obywatelom przysługuje prawo do sądu, a także prawo do odwołania się od decyzji organów administracyjnych. Art. 45 Konstytucji RP stanowi, że każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy przez właściwy, niezależny, bezstronny i niezawisły sąd. Przepisy zawarte w art. 67a ustawy o krajowym systemie cyberbezpieczeństwa nie przewidują jednak żadnej ścieżki odwoławczej od wydawanych przez Pełnomocnika rekomendacji. Brak możliwości odwołania się od decyzji organu publicznego stanowi naruszenie fundamentalnego prawa do sądu.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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. 67a ust. 1 projektu KSC umożliwia bowiem Pełnomocnikowi wydawanie rekomendacji, które określają środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych. Przepisy nie precyzują jednak, w jakiej formie mają być wydawane te rekomendacje, co może prowadzić do niejasności i niejednoznaczności w ich interpretacji. Konstytucja RP w art. 2 zapewnia, że Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej, co wymaga, aby przepisy prawa były jasne, precyzyjne i zrozumiałe dla obywateli. Brak jednoznacznej formy rekomendacji może prowadzić do ich dowolnej interpretacji i stosowania. Zgodnie z art. 78 Konstytucji RP, każda ze stron ma prawo do zaskarżania orzeczeń i decyzji wydanych w pierwszej instancji. Tymczasem art. 67a projektu KSC nie przewiduje obowiązku doręczania rekomendacji podmiotom krajowego systemu cyberbezpieczeństwa. Udostępnianie rekomendacji jedynie w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika może być niewystarczające do skutecznego powiadomienia zainteresowanych podmiotów, co stanowi naruszenie prawa do rzetelnej informacji i możliwości odwołania się od wydanych rekomendacji. Art. 67a ust. 1 projektu KSC pozwala Pełnomocnikowi na wydawanie rekomendacji dotyczących szerokiego spektrum środków technicznych i organizacyjnych związanych z bezpieczeństwem systemów informacyjnych. Ogólnikowa forma tych rekomendacji sprawia, że mogą one dotyczyć praktycznie każdego aspektu związanego z cyberbezpieczeństwem. Tak szeroko zakrojona kompetencja Pełnomocnika bez szczegółowych wytycznych i ograniczeń może prowadzić do nadużyć oraz braku przejrzystości w funkcjonowaniu systemu cyberbezpieczeństwa. Konstytucja RP w art. 7 stanowi, że organy władzy publicznej działają na podstawie i w granicach prawa, co oznacza, że kompetencje organów administracyjnych muszą być wyraźnie określone i ograniczone.

66. Przegląd decyzji HRV

Jednostka redakcyjna: Art. 67b

Postulujemy, aby wprowadzić zasadę cyklicznego przeglądu wydanych decyzji dot. dostawcy wysokiego ryzyka. Przykłady takiego podejścia podano w samym załączniku nr do OSR, gdzie przywołano taką instytucję funkcjonującą w Słowenii (przegląd co 2 lata). Także w przypadku Wielkiej Brytanii wskazano, że *Designated vendor directions mają być przeglądane, co jakiś czas*.
Kwestia ta wydaje się bardzo ważna, z uwagi na bardzo doniosłe skutki wydania decyzji HRV, a także dynamikę zmian technicznych i poza-technicznych mogących skutkować zmianą okoliczności będących podstawą do wydania pierwotnej decyzji.

67. Notyfikacja techniczna

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Jednostka redakcyjna: Art. 67b

Wyjaśnienia wymaga wyrażone w uzasadnieniu utrzymanie założenia dot. braku uzasadnienia dla dokonania notyfikacji technicznej w zakresie przepisów wprowadzających możliwość uznania danego dostawcy za dostawcę wysokiego ryzyka. Zauważamy, że w biegu prac nad poprzednią nowelizacją uznawano taką potrzebę, a dopiero na finalnym etapie podejście to zostało zmodyfikowane bez przedstawienia szerszego uzasadnienia. Z uwagi na doniosłość projektowanych przepisów uważamy, że kwestia ta powinna zostać w pełni wyjaśniona, szczególnie, że odnotowaliśmy, że część krajów UE takich notyfikacji dokonywała, w tym: Belgia, Estonia, Finlandia, Francja, Hiszpania, Słowenia. Wnosimy więc uzupełnienie uzasadnienia o wskazanie przyczyn uznania braku zasadności notyfikacji.

68. Podmioty, do których może być kierowana decyzja HRV

Jednostka redakcyjna: Art. 67b ust. 1

Według projektu skutki decyzji dot. dostawcy wysokiego ryzyka mogą zostać skierowane do podmiotów kluczowych lub ważnych, z wyłączeniem podsektora komunikacji elektronicznej lub do przedsiębiorców telekomunikacyjnych.
W ten sposób precyzyjnie wyłączone zostały *podmioty świadczące usługę komunikacji interpersonalnej niewykorzystującej numerów*, które należą do podsektora komunikacji elektronicznej, ale mogą nie być przedsiębiorcami telekomunikacyjnymi.
Uzasadnienie nie odnosi się do tego czy jest to zabieg celowy i z jakich wynika przesłanek. Należy więc wprost przesądzić o objęciu wszystkich podmiotów podsektora komunikacji elektronicznej potencjalnymi skutkami wydania decyzji dot. dostawcy wysokiego ryzyka.

69. Termin na wycofanie

Jednostka redakcyjna: Art. 67c ust. 2

Zasadniczym terminem na wycofanie zasobów wskazanych w decyzji jest 7 lat. Obowiązywał będzie on wszystkie podmioty z najbardziej krytycznych sektorów krajowej gospodarki, w tym z sektorów energetyki czy transportu. Termin ten został uznany za adekwatny i właściwy, także w świetle ich podstawowego wręcz znaczenia dla bezpieczeństwa państwa i usług niezbędnych do funkcjonowania firm i obywateli. Jednocześnie warto zauważyć, że dotyczył on będzie podmiotów w dużej mierze będących własnością lub współwłasnością Skarbu Państwa.
Jednocześnie, **wyłącznie wobec przedsiębiorców telekomunikacyjnych** – i to tylko tych wdrażających sieć 5G – zdecydowano o wprowadzeniu **terminu istotnie krótszego, tj. 4-**

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

letniego. Skrócono więc nawet dotychczas projektowany termin mający wynieść 5 lat. W uzasadnieniu wskazano jedynie, że *„Takie skrócenie okresu na wycofanie jest spowodowane szczególnym znaczeniem dla bezpieczeństwa państwa usług telekomunikacyjnych, szczególnie sprzętu lub oprogramowania wykorzystywanych do realizowania funkcji krytycznych dla bezpieczeństwa sieci i usług określonych w załączniku nr 3 do ustawy.*”. Z drugiej jednak strony (na str. 71 uzasadnienia) dokonano już bardziej racjonalnej (niż wynika to z samego projektu) oceny wskazując następująco: *W proponowanych przepisach jest mowa o 5–7 latach – termin ten jest często uznawany za średni okres użytkowania sprzętu lub oprogramowania, czyli tzw. cykl życia urządzenia. Raport BEREC wskazuje, że w przypadku sprzętu 5G wykorzystywanego w radiowej sieci dostępowej (RAN) cykl życia urządzenia wynosi w większości przypadku od 5 do 10 lat.*

Wobec pozostałych podmiotów – których usługi są w naszej ocenie są co najmniej tak samo istotne jak sieć 5G – wskazano*: Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów ICT, usług ICT lub procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.* Nie jest dla nas zrozumiałe tak daleko idące zróżnicowanie oceny dot. możliwości dokonania wymiany oraz ryzyka zaprzestania świadczenia usług.

Już z samego tego względu - w pierwszej kolejności - wnosimy o równe traktowanie różnych podmiotów w takich samych sytuacjach faktycznych - poprzez określenie identycznych terminów wycofania zasobów wskazanych w decyzji.

Dalej – odnosząc się już wprost do **terminu 4-letniego wskazujemy, że będzie to czas zbyt krótki na dokonanie wymiany**. Wynika to ze względów technicznych, organizacyjnych, a także samego rynku usług i dostaw.

Wskazujemy, że w przypadku dużych przedsiębiorców telekomunikacyjnych, skutki wydania decyzji HRV wpłyną bardzo istotnie na strategiczne i kluczowe procesy funkcjonowania tych podmiotów, włączając w to wygenerowanie ryzyka dotyczącego ciągłości świadczenia usług telekomunikacyjnych. Wskazujemy dodatkowo, że okres amortyzacji, jaki jest przyjmowany dla urządzeń sieciowych wynosi przeważnie 10 lat.

W zakres zasobów objętych potencjalnymi decyzjami może wejść zarówno obszar sieci radiowej oraz sieci rdzeniowej. Nie mając wiedzy o tym, którzy dostawcy mogliby zostać objęci decyzjami, musimy wskazać, że potencjalnie decyzje mogłoby obejmować tysiące obiektów w całym kraju. Niezbędne do wykonania prace obejmowałyby m.in. prace instalacyjne wymagające wyspecjalizowanych podwykonawców robót telekomunikacyjnych. Szacujemy, że sama te kwestia będzie problematyczna, szczególnie uwzględniając, że w najbliższych latach spodziewamy się ogromnego obciążenia podwykonawców realizacją projektów inwestycyjnych z udziałem środków Krajowego Planu Odbudowy i programu Fundusze Europejskie na Rozwój Cyfrowy o łącznej wartości ponad 10 mld zł.

Istotne w tym zakresie jest, że w tak krótkim czasie łańcuch dostaw może okazać się niewydolny do zrealizowania tego wymogu na racjonalnych warunkach – szczególnie jeśli zakres decyzji obejmowałby istotną część takich zasobów. Jakiekolwiek ograniczenia występujące w tym względzie – niezależnie od ich uzasadniania – będą negatywnie

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

oddziaływały przede wszystkim na przedsiębiorców telekomunikacyjnych oraz ich ryzyko poniesienia wysokich kar finansowych z tytułu naruszenia ustawowego terminu wymiany.
Z perspektywy przedsiębiorców telekomunikacyjnych zobowiązanych do dokonania wymiany w nieprzekraczalnym terminie 4 lat będzie to miało ogromny **wpływ na faktyczne warunki prowadzenia procedur zakupowych i potencjalne zaburzenia możliwości negocjacyjnych** wobec wykonawców i dostawców. Będzie to miało szczególne znaczenie w warunkach już teraz istniejącego ograniczonego poziomu konkurencji. Liczymy, że przewidziany w nowym projekcie ustawy udział Prezesa UOKiK w procesie wydawania opinii Kolegium będzie zapewniał dogłębne zbadane także tego obszaru, jeszcze przed wydaniem decyzji.
Powyższe okoliczności będą z kolei miały niebagatelny **wpływ na koszty przeprowadzenia ewentualnej wymiany**, które będą musiały zostać potencjalnie poniesione przez przedsiębiorców telekomunikacyjnych. Warto w tym miejscu odnotować, że już teraz trwają kosztowne inwestycje związane z realizacją zobowiązań inwestycyjnych w ramach rezerwacji pasma C, a także szerokie inwestycje w sieci VHCN, w tym wspierane ze środków unijnych. W tych okolicznościach, uważamy, że **ustalane teraz warunki dokonywania ew. wymiany powinny szeroko uwzględniać niemożliwe do uniknięcia skutki dla kondycji sektora telekomunikacyjnego**, świadczącego przecież usługi dla szerokiego grona odbiorców.
Podsumowując, przeprowadzenie (po wydaniu decyzji) na dużą skalę szeregu procesów w ramach międzynarodowego łańcucha dostaw obejmujących m.in. procedury przetargowe, zakupowe, produkcję, demontaż, instalację, integrację i uruchomienie wielu tysięcy specjalistycznych urządzeń rozproszonych w całym kraju może nie być możliwe do zrealizowania w okresie zaledwie 4 lat, szczególnie biorąc pod uwagę niewielką dostawców alternatywnych, którzy w tym okresie zapewne spotkają się ze zwiększonym popytem ze strony rynku i wydłużonymi terminami dostaw.
Kwestią, która również zasługuje na uwzględnienie jest fakt, że projektowany w ustawie 4-letni termin jest istotnie krótszy niż przewidziany w wydanych już decyzjach rezerwacyjnych dla pasma C, a rozpoczęcie jego biegu również jest różne na poziomie projektu ustawy oraz decyzji rezerwacyjnych. Wprowadzenie tak istotnego zaostrzenia na etapie po wydaniu decyzji rezerwacyjnych jest w naszej ocenie nieproporcjonalne i rodzi znaczące obiekcje wobec braku stabilności otoczenia prawno-regulacyjnego działalności telekomunikacyjnej.
Wreszcie musimy również wskazać na - zapewne znane Ministerstwu Cyfryzacji - doświadczenia z innych krajów, gdzie wprowadzone zostały nakazy wymiany określonych zasobów sieciowych. W Wielkiej Brytanii termin na wymianę urządzeń w sieci rdzeniowej został przesunięty o niemal rok, a i tak okazał się nierealizowalny dla największego operatora[5]. W Stanach Zjednoczonych, istotnych opóźnień doznaje także program wymiany zasobów „lokalnych operatorów", w którym zabrakło publicznych środków finansujących zmiany w sieciach[6]. Może to – wg FCC – grozić upadkiem niektórych firm

[5] https://www.ft.com/content/54d46cf2-5e24-49d4-9939-63a564c27ca6
[6] DOC-402312A1.pdf (fcc.gov)

telekomunikacyjnych oraz niewystarczającym zasięgiem sieci na części obszarów. W naszej ocenie pokazuje to jak ważne jest, aby warunki wykonywania ewentualnych decyzji były proporcjonalne i szeroko uwzględniające warunki rynkowe. Szczególnie, że projekt ustawy nie przewiduje żadnych form rekompensaty w tym zakresie.

Podsumowując, wnosimy o:

wprowadzenie dla wszystkich podmiotów jednolitego terminu wycofania wynoszącego 7 lat.

Zarówno uzasadnienie do Projektu KSC jak i OSR nie wskazuje na podstawowy problem związany z Procedurą DWR dla podmiotów, których dotyczy Załącznik nr 3 do projektu, mianowicie nie zwrócono uwagi, że wymiana sprzętu dla sieci 5G wymaga wymiany sprzętu również dla 4G (wykorzystywana obecnie konfiguracja 5G non-standalone), nie tylko na tych samym lokalizacjach ale de facto w całej sieci. W konsekwencji jest to dużo bardziej złożony projekt niż budowa sieci 5G obejmujący wielokrotnie więcej lokalizacji fizycznych. Skala inżynieryjna projektu jest tak duża, że próba jego realizacji w ciągu 4 lat będzie ograniczona ze względu na brak dostępności wyspecjalizowanych ekip instalacyjnych (podkreślenia wymaga, że wymiany będą dokonywane przez kilku przedsiębiorców telko równolegle).

Wymiana sprzętu zaś to uruchomienie bardzo dużego programu obejmującego nie jeden, ale co najmniej kilka projektów, dotyczących równolegle zmiany kilku systemów w tym samym czasie oraz dostosowanie pozostałych systemów do współpracy z nowym rozwiązaniem. Podkreślić, należy że ryzyko nie dotrzymania wskazanego w Projekcie KSC terminu z art. 67c może być całkowicie niezależne od przedsiębiorcy telekomunikacyjnego w sytuacji gdy, pozostali dostawcy oferujący dany typ rozwiązania (ilość ich jest również ograniczona), nie będą w stanie wywiązać się z zamówień od nowych klientów w określonym czasie.

70. Niezgodność procedury uznania dostawcy za dostawcę wysokiego ryzyka („Procedura DWR") z Dyrektywą NIS2

Jednostka redakcyjna: art. 67b – 67f projektu KSC
Jednostka redakcyjna NIS2: 20 ust.1; art. 21 ust 1 w zw. z ust.2 w zw. z ust. 3

Uwaga: Sama Procedura DWR nie została przewidziana w dyrektywie NIS2. W szczególności, nie zakłada się, by ryzyko związane z danym dostawcą było badane odgórnie przez organy wyłącznie ze względu na okoliczności dotyczące samego dostawcy, bez związku z cechami konkretnego podmiotu kluczowego lub ważnego (podmiotu krajowego systemu cyberbezpieczeństwa). Dodatkowo, w art. 22 ust. 3 Dyrektywy NIS2 wspomina się jedynie o krytycznych usługach ICT, systemach ICT lub produktach ICT. Tymczasem decyzja o uznaniu dostawcy za dostawcę wysokiego ryzyka w odniesieniu do podmiotów krajowego systemu cyberbezpieczeństwa może dotyczyć niemal dowolnego sprzętu lub oprogramowania. W

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

odniesieniu do przedsiębiorców telekomunikacyjnych może objąć sprzęt i oprogramowanie określone „w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług" w załączniku nr 3 do ustawy. Wykaz ten obejmuje jednak m.in. „5G Radio Base Station Baseband Unit oraz inne funkcje", które zgodnie z 5G Toolbox nie są funkcjami krytycznymi („critical"). Co prawda, dyrektywa NIS2 uprawnia państwa członkowskie do przyjęcia lub utrzymania przepisów zapewniających wyższy poziom cyberbezpieczeństwa, ale tylko pod warunkiem, że takie przepisy będą spójne z obowiązkami państw członkowskich ustanowionymi w prawie Unii.

Poniżej przedstawiono podstawowe zastrzeżenia do proponowanej Procedury DWR, która nie tylko jest w zasadzie powtórzeniem poprzednio forsowanego rozwiązania, ale również rozszerza zakres jej oddziaływania z sektora telekomunikacyjnego na 18 sektorów objętych NIS2:

a) **Dyskryminacyjne kryteria Procedury DWR -** przesłanki oceny dostawcy usług, produktów i procesów ICT za dostawcę wysokiego ryzyka mają charakter wysoce ocenny, a kluczowe znaczenie przypisane zostało kryteriom politycznym i organizacyjnym (bliżej niezdefiniowane związki dostawcy z państwem trzecim, praktyka stosowania prawa w państwie trzecim itd.). Z kolei kryteria techniczne oceny zostały uwzględnione jedynie w ograniczonym zakresie. Projekt w obecnym kształcie może zostać uznany za dyskryminujący, co może być uznane za naruszające TFUE (zasada niedyskryminacji – art. 18 TFUE, zasady swobodnego przepływu towarów i usług – art. 34 i 35 TFUE, zakaz nadużywania pozycji dominującej art. 102 TFUE), Karty Praw podstawowych (art. 20 i 21 ust. 2 Karty praw podstawowych), a także innych zobowiązań międzynarodowych Rzeczpospolitej Polskiej.

b) **Ograniczenie prawa stron w Procedurze DWR oraz zasady jawności -** projekt wprowadza Procedurę DWR, zgodnie z którą podmioty wykorzystujące sprzęt lub oprogramowanie lub procesy takiego dostawcy, muszą wymienić sprzęt lub oprogramowanie w ciągu 7 lat lub w przypadku przedsiębiorców telekomunikacyjnych 4 lat, a także natychmiast zaprzestać wykorzystania nowych urządzeń lub oprogramowania. Jednocześnie projekt ustawy ogranicza w sposób bezprecedensowy możliwość udziału na prawach strony podmiotów objętych skutkami decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka („**Decyzja DWR**"), art. 28 k.p.a.), wyklucza możliwość dopuszczenia do udziału w postępowaniu zainteresowanych organizacji społecznych (art. 31 k.p.a.), czy wreszcie ogranicza uprawnienia strony w zakresie przeprowadzenia czynności dowodowych (art. 79 k.p.a.). Projektodawca zachował rozwiązaniu zgodnie z którym tylko przedsiębiorcy telekomunikacyjni z przychodami rocznymi wynoszącymi co najmniej ok. 160 mln zł mogą wziąć udział w postępowaniu. Ograniczenie prawa do udziału w postępowaniu dla przedsiębiorców, pomimo że będą objęci skutkami Decyzji DWR, może stanowić

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej.

c) Brak jawności postępowania - dostawcy objęci Procedurą DWR, nie otrzymują treści całego wyroku w sprawie odwołania od Decyzji DWR, co więcej także elementy uzasadnienia Decyzji DWR mogą być niejawne (nawet jeśli byłyby reprezentowane przez osoby, posiadające dostęp do informacji objętych klauzulami tajności). Kwestię te podniosła także Rada Legislacyjna w opinii do poprzedniego przedłożenia projektu z dnia 23 lutego 2021 r., która zwróciła uwagę na brak dostatecznej precyzji w przepisach o doręczaniu odpisów wyroków sądu administracyjnego w sprawach skarg na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Rada Legislacyjna podnosiła także wątpliwość o charakterze konstytucyjnym, a mianowicie, czy w ogóle jest zgodne z Konstytucją RP odstępowanie od doręczania stronie pełnego uzasadnienia wyroku sądu administracyjnego (według Rady, nie ulega wątpliwości, że w świetle konstytucyjnego prawa do sądu (art. 45 Konstytucji RP) zasadą musi być dostarczanie stronie pełnego uzasadnienia faktycznego decyzji administracyjnej, tak aby strona (będąca adresatem decyzji) mogła w sposób skuteczny, zaskarżyć tę decyzję do sądu administracyjnego. Ograniczenie prawa do obrony dla dostawcy, a także dla podmiotów objętych skutkami Decyzji DWR, może stanowić podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej.

d) **Natychmiastowa wykonalność Decyzji DWR i brak dwuinstancyjności -** Decyzja DWR jest natychmiast wykonalna, pomimo istotnych skutków gospodarczych (konieczność natychmiastowego zaprzestania nabywania nowego sprzętu lub oprogramowania i rozpoczęcie procedury wycofania). Dodatkowo projekt ustawy nie przewiduje możliwości złożenia wniosku o ponowne rozpatrzenie sprawy przez ministra właściwego do spraw informatyzacji ograniczając zasadę dwuinstancyjności. Oznacza to, że dopiero w postępowaniu odwoławczym, dostawca lub inna strona ma prawo wstrzymać natychmiastową wykonalność (przy czym może otrzymać niepełną treść Decyzji DWR, co naturalnie ogranicza prawo do zaskarżenia takiej decyzji). Ograniczenie prawa do obrony dla dostawcy, a także dla podmiotów objętych skutkami Decyzji DWR, może stanowić podstawę do stwierdzenia niezgodności przepisów z art. 45 Konstytucji RP oraz art. 47 Karty praw podstawowych Unii Europejskiej.

e) Nieprecyzyjny zakres decyzji ministra o uznaniu dostawcy za dostawcę wysokiego ryzyka – w pkt 3 załącznika nr 3 związanego z zarządzaniem łącznością z urządzeniami użytkowników mowa o „innych funkcjach" oprócz 5G Radio Base Station Baseband Unit, co powoduje, że w pkt 3 mieszczą się wszystkie urządzenia zarządzające łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych, a nie tylko związane z RAN. Taka redakcja prowadzi do niepewności co do ostatecznego zakresu decyzji, a także umożliwia szerokie i nieproporcjonalne wykluczenie urządzeń danego dostawcy, nawet

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

jeśli urządzenia te nijak odpowiadają za krytyczne funkcje w komunikacji. Ponadto istnieją poważne konstytucyjne wątpliwości co do możliwości wprowadzenia normy technicznej (standardu) jako obowiązującego aktu prawa, tj. choć załącznik nr 3 stanowi niewątpliwie część ustawy, to odwołanie się do funkcji 3GPP powoduje, że normy lub standardy tej organizacji stają się źródłem obowiązującego prawa w Polsce. Innymi słowy, 3GPP poprzez zmianę (np. aktualizację) standardu wpływać będzie na prawa i obowiązku adresatów załącznika nr 3 w Polsce, a tym samym moc prawna zostanie zrównana z ustawą. Szeroki zakres załącznika nr 3 do ustawy, wraz z odwołaniem się do zmieniających się norm 3GPP może stanowić podstawę do uchylenia tych przepisów przez Trybunał Konstytucyjny ze względu na naruszenie zasady praworządności (art. 2 Konstytucji RP) oraz powszechnie obowiązujących źródeł prawa (art. 87 Konstytucji RP).

f) **Negatywny wpływ na rynek i wzrost cen w efekcie zastosowania Procedury DWR -** uchwalenie projektu ustawy w jego obecnej treści może mieć liczne negatywne skutki dla konkurencji i konsumentów, w szczególności dlatego, że realizacja jego założeń może w wielu branżach doprowadzić do powstania duopolu lub oligopolu z nieuniknionym negatywnym skutkiem w postaci wzrostu cen dla konsumentów i przedsiębiorców. Z uwagi na strukturę rynku, wyeliminowanie dostawców spoza UE i NATO czyli w praktyce tych z chińskim kapitałem – doprowadzi do faktycznego zakłócenia konkurencji. Jeśli chińscy dostawcy utracą możliwość prowadzenia działalności, ich udział zostanie przejęty przez konkurencję. Wskutek wysokich barier wejścia związanych z kosztem badań i rozwoju i prawami własności intelektualnej, wejście na rynek innych, poważnych konkurentów nie wydaje się być możliwe. W dobie rosnącej inflacji już taki przypadek wystąpił w Wielkiej Brytanii, gdzie brytyjski operator – British Telecom – wprost odwołał się do konieczności podwyżki cen dla konsumentów m.in. z uwagi na konieczność kompensacji kosztów związanych z wymogiem usunięcia z sieci sprzętu wysokiego ryzyka[7]. Zastosowanie Procedury DWR spowoduje wzrost cen usług dla konsumentów. Nie można wykluczyć również obniżenia jakości, szczególnie w okresie zastępowania urządzeń.

g) **Ograniczenie swobody przepływu towarów i zgodności z przepisami UE -** projekt ustawy wprowadza Procedurę DWR, w ramach którego przewiduje się mechanizm powiadamiania o wszczęciu postępowania na stronie BIP oraz dopuszczeniem do postępowania jedynie największych przedsiębiorców telekomunikacyjnych. Jak zwrócił uwagę w poprzednim przedłożeniu tego projektu Minister ds. Unii Europejskiej – w opinii nr DPUE.920.1030.2021.AR(27) - komunikowanie (publiczne z art. 66a ust. 8), jak i ograniczone (do największych nabywców produktów ICT z art. 66a ust. 5), może stanowić środek o skutku równoważnym do ograniczeń ilościowych w przywozie i wywozie, o których mowa w art. 34 i 35 TFUE. Zgodnie z orzecznictwem Trybunału Sprawiedliwości UE środkami o skutku równoważnym do ograniczeń ilościowych są bowiem wszelkie

[7] BT misses deadline for removing Huawei from network core • The Register

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

przepisy państw członkowskich dotyczące obrotu handlowego mogące bezpośrednio lub pośrednio, rzeczywiście lub potencjalnie utrudnić wewnątrzunijną wymianę handlową (zob. wyrok Trybunału Sprawiedliwości Dassonville, 8/74, pkt 5). Nierówne traktowanie podmiotów może skutkować naruszeniem art. 21 Karty praw podstawowych Unii Europejskiej, art. 32 Konstytucji RP oraz I:1 i III.4 Układu Ogólnego w Sprawie Taryf Celnych i Handlu Światowej Organizacji Handlu („GATT") o art. 3 ust. 1 -2 umowy między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji z dnia 10 marca 1989 r. Ograniczenia związane z ograniczeniem stron i ograniczonym powiadamianiem **może wpływać na handel wewnątrz Unii Europejskiej, w tym na swobodny przepływ produktów legalnie wprowadzonych już do obrotu w Polsce**, jak i w innych państwach członkowskich.

h) **Narażenie Skarbu Państwa na odpowiedzialność odszkodowawczą w wyniku wdrożenia Procedury DWR** - projekt ustawy zawiera rozwiązania jawnie dyskryminujące inwestorów z krajów trzecich, w stosunku do inwestorów krajowych – co przede wszystkim dotyczy kryteriów wydania opinii Kolegium, na której opierać się będzie decyzja ministra o wykluczeniu. Kryteria te opierają się na przesłankach narodowościowych, uznaniowych i politycznych. Ponadto, w projekcie istotnie ograniczono podstawowe gwarancje ustawowe jak prawo do rzetelnego procesu, z możliwością udziału czynnika społecznego. Działania takie są wprost sprzeczne z art. I:1 i III.4 GATT, które wykluczają dyskryminację produktów importowanych względem produktów lokalnych, a także produktów importowanych z jednego członków tej organizacji względem tych z innego państwa. Członek Światowej Organizacji Handlu („WTO") nie może traktować towarów innego członka WTO w sposób mniej uprzywilejowany niż traktuje towary pochodzące z własnego terytorium lub z terytorium innego członka WTO. Co więcej, Procedura DWR zakłada wymianę produktów, usług lub procesów w terminie 4 lat lub 7 lat. W przypadku wymiany sprzętu telekomunikacyjnego azjatyckich producentów, koszt takiej decyzji wyniósłby kilkanaście miliardów złotych. W efekcie Skarb Państwa będzie musiał się zmierzyć z groźbą postępowań odszkodowawczych, w tym powództw wnoszonych do międzynarodowych trybunałów arbitrażowych przez podmioty poszkodowane przez rozwiązania zawarte w projekcie KSC, co może skutkować ekspozycją finansową budżetu państwa. Jak wskazano w raporcie pn. „Prawne i ekonomiczne skutki ograniczenia konkurencji wśród dostawców sprzętu sieciowego 5G w Polsce"[8] w wyniku wejścia w życie Projektu **szkody polskiej gospodarki wyniosłyby łącznie niemal -44 mld zł** (w tym 21,5 mld zł obniżenia PKB, 1,2 mld zł utraconej korzyści konsumentów, 0,6 mld zł bezpośredniej straty dla Skarbu Państwa oraz 14,1 mld zł bezpośredniej straty dla operatorów telekomunikacyjnych), co przełoży się bezpośrednio na ryzyko sporu ze Skarbem Państwa. Jednocześnie kryteria oceny jedynie w szczątkowym stopniu odnoszą się do kryteriów technicznych – dających się jednoznacznie i obiektywnie ustalić oraz powiązanych z podatnością danych systemów lub urządzeń. Zamiast tego ocena opiera się przede

[8] Wykluczenie Huawei z 5G to 44 mld zł strat dla Polski do 2030 - Forsal.pl

wszystkim na niezwykle pojemnej przesłane prawdopodobieństwie pozostawania dostawcy pod wpływem obcego państwa spoza Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego. Takie ukształtowanie przesłanek stoi w sprzeczności z podstawowymi zasadami postępowania administracyjnego. W ramach postępowania administracyjnego organ wydający decyzję administracyjną obowiązany jest ustalić stan faktyczny na podstawie którego dokona subsumcji stanu prawnego, w wyniku którego wyda decyzję administracyjną. Ocena w ramach prowadzonego postępowania nie uwzględnia w żaden sposób takich okoliczności jak:

- sposób wykorzystania produktów ICT, usług ICT lub procesów ICT przez podmioty ważne i kluczowe, w tym możliwość objęcie zakresem decyzji nie tylko sieci 5G, ale także jakichkolwiek innych technologii lub zastosowań (brak ograniczenia zakresu regulacji do krytycznych aktywów, o których mowa w SM03 Toolbox 5G),
- możliwość dodatkowej konfiguracji urządzeń, pozbawiającej produktów ICT, usług ICT lub procesów ICT cech związanych z wysokim ryzykiem,
- możliwość stopniowania skutków decyzji administracyjnej (brak jakiejkolwiek proporcjonalności),
- brak wdrożenia jakiegokolwiek postępowania naprawczego.

i) **Procedura DWR obniży poziom inwestycji, w tym w sektorze innowacyjnym, wpływając bezpośrednie na obniżenie wpływów do budżetu państwa.** Wprowadzony model wykluczenia dostawcy wysokiego ryzyka, polegający na jego całkowitym wykluczeniu także w odniesieniu do 18 sektorów spowoduje, że w wyniku jednej, arbitralnej decyzji ministra właściwego do spraw informatyzacji, wydanej na podstawie opinii Kolegium ds. Cyberbezpieczeństwa taki dostawca, w sposób natychmiastowy, nie będzie mógł prowadzić działalności gospodarczej w Polsce, bez względu na jego związki ekonomiczne z Polską i dokonane inwestycje, w tym w produkty, procesy i usługi cechujące się wysokim poziomem innowacji. Stanie się tak bez poszanowania podstawowych gwarancji procesowych wynikających z Kodeksu postępowania administracyjnego i norm prawa międzynarodowego, co może wywołać efekt odstraszający dla innych zagranicznych podmiotów.

j) **Poważne wady związane z przyjętym modelem postępowania administracyjnego.** Do tych negatywnych elementów projektowanego postępowania należą:

i) **brak gwarancji bezstronności** - brak ustawowego wyłączenia właściwego ministra z procedury wydania opinii poprzedzającej wszczęcie postępowania administracyjnego, powoduje naruszenie zasady niezależności i bezstronności. Jest to szczególnie istotne w przypadku opinii poprzedzającej wszczęcie postępowania administracyjnego z uwagi na brak zastosowania ogólnych reguł włączeń osób i organów na gruncie przepisów kodeksu postępowania

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

administracyjnego (art. 24 i nast. ustawy z dnia 14 czerwca 1960 Kodeks postępowania administracyjnego („**KPA**")).

ii) **brak doręczania informacji o wszczęciu Procedury DWR wobec dostawców spoza UE/EFTA/Konfederacji Szwajcarskiej** - W ramach Procedury DWR przewiduje się brak indywidualnego informowania dostawcy, którego dotyczy postępowanie, o jego wszczęciu, jeśli jego siedziba znajduje się poza Unią Europejską/EFTA/Konfederacją Szwajcarską (w to miejsce przewidziano informację na stronie podmiotowej BIP właściwego organu), co skutkuje dyskryminacją podmiotów spoza tego obszaru – wobec takich podmiotów postępowanie jest jawne, w sytuacji gdy sam fakt wszczęcia postępowania może skutkować znacznym ograniczeniem zamówień przez podmioty objęte regulacją, ze względu na przyszłe ryzyko wykluczenia takiego dostawcy. Różne traktowanie przedsiębiorców ze względu na kraj pochodzenia może skutkować naruszeniem art. 21 Karty praw podstawowych Unii Europejskiej, art. 32 Konstytucji RP oraz I:1 i III.4 GATT, art. 3 ust. 1 -2 umowy między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Chińskiej Republiki Ludowej w sprawie wzajemnego popierania i ochrony inwestycji z dnia 10 marca 1989 r.

iii) **brak gwarancji czynnego udziału strony w postępowaniu** - identyfikujemy duże ryzyko wyłączenia uprawnień strony ww. zakresie w postaci możliwości wyłączenia dostępu do akt administracyjnych na podstawie art. 74 § 4 KPA (brak dostępu do akt sprawy zawierających informacje niejawne o klauzuli tajności „tajne" lub „ściśle tajne", a także do innych akt, które organ administracji publicznej wyłączy ze względu na ważny interes państwowy). Istnieje uzasadnione ryzyko, iż na etapie postępowania akta będą wyłączane na postawie klauzuli "ściśle tajne" lub "tajne" albo na podstawie przesłanki "ważnego interesu państwowego'. Takie ograniczenie dostępu do akt w połączeniu z powołanym wyżej możliwym brakiem sporządzenia uzasadnienia faktycznego może de facto uniemożliwić stronie postępowania realizacje jej uprawnień procesowych i przedstawienie swoich argumentów i dowodów tak na etapie postępowania administracyjnego jak i sądowo-administracyjnego.

iv) **brak transparentności postępowania sądowego** - nie ma również podstaw do wyłączenia podstawowego trybu działania sądów administracyjnych ww. sprawie jakim jest rozprawa sądowoadministracyjna i wskazanie ww. zakresie na obowiązek rozpatrzenia jej na posiedzeniu niejawnym. Posiedzenie niejawne stanowi istotne ograniczenie, gdyż ogranicza w poważnym stopniu kontrolę społeczną nad postępowaniem sądowym. Tymczasem charakter decyzji wydanej wskazuje, iż jest to decyzja o ogromnych skutkach społeczno-gospodarczych i przebieg postępowania sądowo administracyjnego ww. zakresie winien mieć charakter jawny.

v) **brak przesłanek do wydania decyzji administracyjnej** - proponowane przepisy nie zawierają żadnych przesłanek dotyczących podstaw prawnych do wydania

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

decyzji administracyjnej przez ministra właściwego do spraw informatyzacji. Jedyną przesłanką jest uznanie, że z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla bezpieczeństwa narodowego. W konsekwencji, minister właściwy do spraw informatyzacji, jest związany opinią Przewodniczącego Kolegium, nie mając żadnej możliwości zmiany decyzji administracyjnej wynikającej z tej opinii. W efekcie instancyjność postępowania ma charakter iluzoryczny, albowiem właściwy minister jedynie „broni" niejawnej opinii Kolegium.

vi) **brak określenia charakteru prawnego opinii Kolegium** - choć projektodawca wskazuje, że opinia Kolegium ma charakter opinii uzgadnianej podczas posiedzeń Kolegium, to w istocie, jak wskazano wyżej, opinia ta ma charakter wiążący a minister właściwy do spraw informatyzacji potwierdza ją jedynie w drodze decyzji administracyjnej. To opinia Kolegium ma charakter przesądzający o wykluczeniu danego dostawcy, a nie decyzja administracyjna ministra właściwego ds. informatyzacji. Oznacza to zatem, że nie ma podmiotu, któremu można przypisać odpowiedzialność za opinię, ponieważ od opinii Kolegium nie przysługuje żadne odwołanie, a właściwy minister wydając decyzję odwołuję się do niezaskarżalnej opinii, o niejasnym charakterze prawnym.

vii) **dyskryminacyjne kryteria Procedury DWR:** Przesłanki oceny dostawcy usług, produktów i procesów ICT za dostawcę wysokiego ryzyka mają charakter wysoce ocenny, a kluczowe znaczenie przypisane zostało kryteriom politycznym i organizacyjnym (bliżej niezdefiniowane związki dostawcy z państwem trzecim, praktyka stosowania prawa w państwie trzecim itd.). Z kolei kryteria techniczne oceny zostały uwzględnione jedynie w ograniczonym zakresie. Takie podejście jest sprzeczne z wytycznymi określonymi w dokumencie Komisji Europejskiej 5G Toolbox, który podkreśla konieczność odniesienia oceny do kluczowych aktywów (key assets), a zatem skoncentrowanie się na aspektach przedmiotowych, nie zaś podmiotowych. W obecnym kształcie przepisy projektu ustawy w tym zakresie mogą naruszać zasadę równego traktowania (niedyskryminacji) ze względu na przynależność państwową, która została określona nie tylko w art. 18 TFUE, ale także w art. 20 i art. 21 ust. 2 Karty praw podstawowych. Zasada niedyskryminacji może zostać naruszona nie tylko jawną dyskryminacją ze względu na przynależność państwową, ale także wszelką ukrytą dyskryminacją, która poprzez zastosowanie innych kryteriów zróżnicowania prowadzi w rzeczywistości do tego samego rezultatu. Przepisy regulujące Procedurę DWR mogą naruszać również art. 34 i art. 35 TFUE, które chronią swobodny przepływ towarów. Zauważyć należy, że dany dostawca może wytwarzać produkty i usługi w jednym kraju członkowskim i dostarczać do innych krajów, co jest powszechną praktyką w UE. Przepis art. 34 TFUE zakazuje natomiast państwom członkowskim przyjmowania „ograniczeń ilościowych w przywozie" i „wszelkich środków o skutku równoważnym". Wprawdzie zgodnie z art. 36 TFUE, postanowienia artykułów 34

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

i 35 nie stanowią przeszkody w stosowaniu wskazanych zakazów lub ograniczeń, gdy jest to uzasadnione m.in. względami bezpieczeństwa publicznego. Ochrona bezpieczeństwa publicznego zakłada jednak „istnienie rzeczywistego i dostatecznie poważnego zagrożenia, które narusza jeden z podstawowych interesów społeczeństwa, a w kontekście wspólnotowym należy je interpretować w sposób ścisły". Zwrócić należy także uwagę, że ciężar dowodu spoczywa na państwie członkowskim, które powinno „wykazać w każdym przypadku, że ich przepisy są niezbędne do zapewnienia skutecznej ochrony interesów, o których mowa w art. 36 TFUE". Zastosowanie odstępstwa przewidzianego w art. 36 TFUE wymaga zastosowania tzw. testu proporcjonalności, czyli sprawdzenia czy przewidziane rozwiązania są proporcjonalne do zamierzonych celów, w więc w tym przypadku, do ochrony bezpieczeństwa publicznego. TSUE w swoim orzecznictwie także wskazywał, że przepis krajowy zakazujący przywozu produktu jest nieproporcjonalny, jeżeli istnieją mniej restrykcyjne środki, które pozwalają na osiągnięcie zamierzonego celu. Ograniczenie swobodnego przepływu towarów oraz swobody przedsiębiorczości można uzasadnić na podstawie art. 36 TFUE, tylko wtedy, gdy środek jest konieczny, a więc w szczególności, gdy nie istnieją inne mniej restrykcyjne środki, które mogłyby osiągnąć ten sam cel. Zauważyć wreszcie należy, że wykluczenie z polskiego rynku określonych dostawców oznacza automatyczne polepszenie sytuacji innych dostawców działających na polskim rynku. Stanowić to może z kolei naruszenie art. 106 ust. 1 TFUE, który zakazuje państwom członkowskim przyjmowania lub utrzymywania w mocy, w odniesieniu do przedsiębiorstw, którym przyznano prawa wyłączne lub specjalne, wszelkich środków, które prowadziłyby do naruszenia innej zasady w traktatach UE. Przepisy te obejmują w szczególności art. 18 TFUE (zasada niedyskryminacji), art. 34 TFUE (swobodny przepływ towarów) i art. 102 TFUE (zakaz nadużywania pozycji dominującej). Projekt w obecnym kształcie może zostać uznany za dyskryminujący, co może być uznane za naruszające TFUE (zasada niedyskryminacji – art. 18 TFUE, zasady swobodnego przepływu towarów i usług – art. 34 i 35 TFUE, zakaz nadużywania pozycji dominującej art. 102 TFUE), Karty Praw podstawowych (art. 20 i 21 ust. 2 Karty praw podstawowych), a także potencjalnie naruszeniami innych zobowiązań międzynarodowych Rzeczpospolitej Polskiej.

viii) **Arbitralność Procedury DWR:** projekt ustawy KSC przewiduje silnie dyskrecjonalną i arbitralną, a przede wszystkim jednoosobową, procedurę oceny ryzyka dostawcy sprzętu lub oprogramowania z punktu widzenia cyberbezpieczeństwa, i w szerszym ujęciu, bezpieczeństwa państwa. W ramach postępowania oddziałującego arbitralnie i szeroko na przedsiębiorców decyzja nie powinna być podejmowana wyłącznie jednoosobowo przez ministra właściwego do spraw informatyzacji. Zakres oceny bezpieczeństwa oraz wykluczenia produktów przedsiębiorcy z rynku ma skomplikowany charakter

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

wymagający wiedzy eksperckiej, która w ramach administracji państwowej skumulowana jest w różnych ministerstwach czy urzędach, jak np. Urzędzie Ochrony Konkurencji i Konsumentów, czy Urzędzie Komunikacji Elektronicznej. Z tego względu ważne byłoby uczestnictwo w podejmowaniu decyzji przez ministrów odpowiedzialnych za obszary istotne z perspektywy chronionych wartości (obronność, bezpieczeństwo i porządek publiczny) lub za obszary właściwe merytorycznie z perspektywy sektora, którego dotyczy decyzja (rozwój i technologia) – uczestnictwo w procesie decyzyjnym mogłoby sprowadzać się do możliwości wyrażenia sprzeciwu w zakresie wydania decyzji. Za błędne rozwiązanie uznać należy również brak zapewnienia udziału czynnika eksperckiego w procesie wydania opinii przez Kolegium, co stanowi przecież istotny element całego postępowania w sprawie uznania za dostawcę wysokiego ryzyka, poprzedzającego decyzję ministra. Przedmiotowa opinia z założenia powinna brać pod uwagę wyniki analizy szeregu uwarunkowań – politycznych, ekonomicznych, technologicznych i organizacyjnych oraz stanowić kluczowy element merytorycznego uzasadnienia podejmowanej decyzji. Tym samym właściwy dobór osób biorących udział w jej wydaniu wydaje się być kluczowy dla zapewnienia jej kompletności i rzetelności, a w konsekwencji prawidłowości całego postępowania. Z tego względu nie ulega wątpliwości, że do prac nad jej treścią powinni zostać włączeni np. przedstawiciele izb zrzeszających podmioty z sektora ICT czy przedsiębiorców korzystających z rozwiązań ICT. Powyższa uwaga ma tym większe znaczenie, że Kolegium jest z definicji organem politycznym, złożonym przede wszystkim z ministrów (art. 66 ustawy o krajowym systemie cyberbezpieczeństwa), a zaangażowanie CSIRT'ów nie spełnia wystarczającej gwarancji udziału czynniku eksperckiego, czy też następczo izb gospodarczych.

71. Nadmierne rozszerzenie zakresu wykluczenia dostawcy na wszystkie podmioty ważne i kluczowe

Jednostka redakcyjna: art. 67b – 67f projektu KSC
Jednostka redakcyjna NIS2: 20 ust.1; art. 21 ust 1 w zw. z ust.2 w zw. z ust. 3

Uwaga: W odróżnieniu od wcześniejszych propozycji, obecna wersja projektu ustawy zakłada rozszerzenie Procedury DWR na cały sektor cyberbezpieczeństwa (18 sektorów). Taki krok może prowadzić do znacznego rozszerzenia zakresu regulacji, potencjalnie obejmując szeroki wachlarz produktów i usług ICT. Wprowadzenie tej procedury objęłoby około 38 532 podmioty (dane OSR), co jest istotnym rozszerzeniem w stosunku do wcześniejszych propozycji legislacyjnych. Wśród tych produktów znajdą się na przykład panele fotowoltaiczne, falowniki, chipsety czy procesory przemysłowe, które są powszechnie stosowane we wszystkich sektorach. Może to zagrażać ciągłości funkcjonowania sektorów i generować znaczne koszty, co jest skutkiem trudnym do przewidzenia na etapie wprowadzania regulacji. Warto podkreślić, że:

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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. zgodnie z NIS2 środki zarządzania ryzykiem w cyberbezpieczeństwie powinny być adekwatne do rzeczywistego poziomu ryzyka, na które są narażone sieci i systemy informatyczne poszczególnych podmiotów kluczowych i ważnych. Stosowane środki powinny być oparte na najnowszej wiedzy oraz, gdzie to możliwe, na europejskich i międzynarodowych normach. Powinny również uwzględniać koszty ich wdrożenia, aby unikać nakładania na podmioty nieproporcjonalnie dużych obciążeń finansowych i administracyjnych. Istotne jest również dostosowanie tych środków do specyfiki każdego podmiotu, biorąc pod uwagę takie czynniki jak krytyczność działalności, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów oraz potencjalne skutki społeczne i gospodarcze związane z takimi incydentami (por. motyw. 81 i 82, art. 21 ust. 1 NIS2).
2. wdrożone przez NIS2 skoordynowane oszacowania ryzyka dla bezpieczeństwa krytycznych łańcuchów dostaw koncentrują się na konkretnych sektorach, mając na uwadze konieczność dostosowania oszacowania do jego specyfiki (por. motyw 91, art. 22 NIS2). Te oszacowania prowadzone są przez Grupę Współpracy we współpracy z Komisją Europejską i ENISA, a nie przez ministra właściwego do spraw informatyzacji.
3. 5G Toolbox, nakazuje analizę i weryfikację łańcucha dostaw w sieciach mobilnych (telekomunikacji), a nie w każdym sektorze, w którym wykorzystywane są systemy informatyczne, a w szczególności zaleca:

i. oceniać profil ryzyka dostawców w odniesieniu do kluczowych zasobów uznanych za krytyczne i wrażliwe w unijnej skoordynowanej ocenie ryzyka;
ii. utrzymywania zróżnicowanego i zrównoważonego łańcucha dostaw 5G w celu uniknięcia długotrwałej zależności;
iii. koordynację między państwami członkowskimi.

Wprowadzenie w projekcie ustawy KSC procedury wykluczenia dostawcy obejmującej wszystkie podmioty kluczowe i ważne. Proponowany zakres wprowadza rygorystyczne regulacje osiemnastu sektorów, co jest rozwiązaniem niespotykanym w Unii Europejskiej i mogącym prowadzić do poważnych konsekwencji operacyjnych i finansowych dla szerokiego spektrum przedsiębiorstw.

Sektory takie jak administracja publiczna, zdrowie, bankowość, energetyka, a także nauka i produkcja (w tym żywności i chemikaliów), znajdują się wśród tych, które będą musiały zastosować się do Procedury DWR, co oznacza całkowite wyeliminowanie i zastąpienie urządzeń oraz oprogramowania wykluczonego dostawcy w ciągu zaledwie 7 lat. To nie tylko stwarza ryzyko znaczących przerw w działalności, ale także narzuca ogromne koszty związane z wymianą sprzętu i oprogramowania, bez przewidzianego odszkodowania dla dotkniętych tym podmiotów.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Tak szerokie zastosowanie Procedury DWR bez proporcjonalnej oceny ryzyka i specyfiki każdego sektora jest nieadekwatne i może prowadzić do nadmiernego obciążenia podmiotów, które niekoniecznie są wrażliwe na zagrożenia związane z wykorzystaniem technologii od określonych dostawców. Co więcej, brak rekompensaty za wymianę sprzętu może spowodować poważne obciążenia finansowe dla wielu przedsiębiorstw, co z kolei może wpłynąć negatywnie na całą gospodarkę.

W obliczu potencjalnych niezgodności z NIS2 oraz nieproporcjonalnego charakteru proponowanych środków zarządzania cyberbezpieczeństwem, postulujemy:

- ujednolicenie terminu na usuwanie sprzętu dla wszystkich sektorów do 7 lat;
- w kontekście brzmienia 5G toolbox, który przewiduje ewentualne ograniczenia w zakresie korzystania ze sprzętu lub usług do funkcji krytycznych, postulujemy by ewentualne wykluczenia dotyczyły infrastruktury krytycznej;szczegółowe wytyczne w zakresie infrastruktury krytycznej były formułowane dla każdego sektora w akcie prawnym niższego rzędu, tj. w rozporządzeniu wydawanym przez organu ds. cyberbezpieczeństwa właściwy dla danego sektora. Takie podejście umożliwi dynamiczne reagowanie na zmiany na rynku i w technologii, umożliwiając dostosowanie zakresu do faktycznych potrzeb i konkretnej specyfiki danego sektora. Wprowadzenie przepisów na poziomie aktów niższego rzędu pozwoli na bardziej elastyczne i precyzyjne zarządzanie infrastrukturą krytyczną, co jest niezbędne w obliczu szybko zmieniających się technologii i rosnących zagrożeń w obszarze cyberbezpieczeństwa. Pozwoli to na lepsze zrozumienie specyficznych potrzeb poszczególnych sektorów i na zastosowanie środków adekwatnych do rzeczywistych zagrożeń, bez konieczności stałych zmian ustawowych. Takie rozwiązanie sprzyja również transparentności i przejrzystości procesu legislacyjnego, umożliwiając konsultacje i współpracę z zainteresowanymi stronami, co jest kluczowe dla skutecznego wdrożenia regulacji i zapewnienia wysokiego poziomu ochrony infrastruktury krytycznej;
- przywrócenie konstytucyjnych gwarancji procesowych w postępowaniu dotyczącym wykluczenia dostawcy

72. Polecenia zabezpieczające naruszające standardy demokratycznego państwa prawa

Jednostka redakcyjna: art. 67g projektu KSC
Jednostka redakcyjna NIS2: art. 9 ust. 1

Uwaga: Przepis art. 67g projektu ustawy w nowym brzmieniu daje szerokie kompetencje ministrowi właściwemu do spraw informatyzacji w zakresie wydawania poleceń zabezpieczających w przypadku wystąpienia incydentu krytycznego. Zasadniczym celem tej regulacji jest ochrona cyberbezpieczeństwa. Niemniej jednak, wiele argumentów prawnych

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

można przytoczyć przeciwko aktualnemu kształtowi tego przepisu, bazując zarówno na analizie samego przepisu.

Art. 67g ust. 14 stanowi, że polecenie zabezpieczające podlega natychmiastowej wykonalności. Taka regulacja znacząco ogranicza możliwość obrony podmiotów, na które nałożono takie polecenia. Co więcej, przepisy KPA przewidują w tym zakresie odpowiednie narzędzia umożliwiające ochronę interesów stron postępowania administracyjnego. Rygor natychmiastowej wykonalności może prowadzić do sytuacji, w której podmiot, w tym zarówno jednostka samorządu terytorialnego, jak i inne podmioty kluczowe i ważne, nie będzie miał możliwości wypełnienia swoich zadań ustawowych ze względu na brak środków finansowych na realizację polecenia zabezpieczającego.

Przepis nie przewiduje żadnego okresu na wycofanie sprzętu lub oprogramowania, co może prowadzić do natychmiastowego paraliżu działalności jednostek, które muszą stosować się do polecenia zabezpieczającego. Sytuacja ta jest szczególnie trudna dla jednostek samorządu terytorialnego, które muszą przestrzegać przepisów o zamówieniach publicznych, co de facto uniemożliwia im szybkie przeprowadzenie zamówienia na nowy sprzęt lub oprogramowanie. Jednakże, dotyczy to również innych podmiotów objętych poleceniem, które mogą mieć ograniczone możliwości finansowe i organizacyjne do szybkiej adaptacji do nowych wymogów.

Art. 67g ust. 17 stanowi, że od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy. To istotne ograniczenie prawa do sądu i środka odwoławczego, co jest sprzeczne z podstawowymi zasadami państwa prawa. Zgodnie z art. 78 Konstytucji RP, każda decyzja administracyjna powinna być poddana kontroli sądu administracyjnego, co w przypadku poleceń zabezpieczających jest znacząco ograniczone. Ograniczenie możliwości odwołania się od decyzji stawia podmioty, na które nakładane są polecenia, w sytuacji bezsilności wobec decyzji administracyjnych, które mogą mieć istotny wpływ na ich funkcjonowanie.

Proces wydawania polecenia zabezpieczającego jest arbitralny i może prowadzić do nadmiernej uznaniowości organów administracyjnych. Wydawanie takich poleceń bez szczegółowego uzasadnienia oraz brak możliwości skutecznego odwołania się od decyzji podważają zaufanie do administracji publicznej oraz mogą prowadzić do nieprzewidywalności w funkcjonowaniu podmiotów kluczowych i ważnych. Taka arbitralność może prowadzić do sytuacji, w której decyzje są podejmowane bez pełnego zrozumienia kontekstu i skutków dla poszczególnych podmiotów.

Nałożenie polecenia zabezpieczającego na podmioty prywatne może prowadzić do znacznych kosztów finansowych, które nie są rekompensowane przez Skarb Państwa. W kontekście przedsiębiorstw, które zainwestowały znaczne środki w swoją infrastrukturę, wymóg natychmiastowego zaprzestania używania określonych produktów lub oprogramowania może prowadzić do ich bankructwa. Brak odpowiedzialności odszkodowawczej po stronie Państwa za szkody wynikłe z wykonania polecenia zabezpieczającego stawia podmioty prywatne w bardzo trudnej sytuacji ekonomicznej. Przepisy dotyczące poleceń zabezpieczających nie uwzględniają zasady proporcjonalności,

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

która jest kluczowa w prawie administracyjnym. Nakładane środki powinny być adekwatne do zagrożenia oraz powinny być stosowane tylko w ostateczności, po wyczerpaniu innych mniej drastycznych środków. Brak proporcjonalności może prowadzić do nieuzasadnionych ograniczeń działalności gospodarczej i nadmiernych kosztów po stronie podmiotów, które są objęte poleceniem.

Przepis art. 67g projektu KSC nie przewiduje obowiązku konsultacji z podmiotami, na które ma być nałożone polecenie zabezpieczające, co narusza zasadę partycypacji społecznej w procesie stanowienia prawa. Brak konsultacji może prowadzić do wydania decyzji bez pełnego zrozumienia skutków jej wykonania, co w konsekwencji może skutkować niewłaściwym zastosowaniem środków zabezpieczających i dodatkowymi problemami dla podmiotów, na które te środki są nakładane.

Możliwość nakazania zablokowania dostępu do określonych serwerów, stron internetowych czy usług stwarza ryzyko nadużyć i wprowadzenia cenzury, co jest sprzeczne z art. 54 Konstytucji RP, gwarantującym wolność słowa i prawo do informacji. Takie środki mogą być wykorzystywane w sposób nieproporcjonalny, co zagraża wolnościom obywatelskim i transparentności działania administracji publicznej.

Brak bezpośredniego doręczenia polecenia zabezpieczającego, które jest uznawane za doręczone z chwilą ogłoszenia w dzienniku urzędowym, narusza podstawowe zasady postępowania administracyjnego dotyczące komunikacji z zainteresowanymi stronami. Podmioty objęte takim poleceniem mogą nie być świadome nałożonych na nie obowiązków w odpowiednim czasie, co ogranicza ich możliwość reakcji i przygotowania się do wykonania polecenia. Bezpośrednie doręczenie decyzji jest kluczowe dla zapewnienia, że wszystkie strony są w pełni poinformowane i mogą odpowiednio dostosować swoje działania. Jest to o tyle istotne, że przy podobnej konstrukcji prawnej (wyłączenia doręczenia) Trybunał Konstytucyjny w orzeczeniu z 26.11.2019 r. sygn. akt P 9/18 z orzekł, że art. 49 ustawy zmieniającej w zakresie, w jakim w sprawach dotyczących wpisów, o których mowa w art. 55 pkt 4 i 5 KRSU, wyłącza obowiązek doręczenia przez sąd uczestnikowi postępowania rejestrowego postanowienia o wpisie do rejestru dłużników niewypłacalnych wraz z uzasadnieniem, a także pozbawia uczestnika tego postępowania prawa do wniesienia skargi na postanowienie refe-rendarza sądowego zarządzające wpis do takiego rejestru, jest niezgodny z art. 45 ust. 1 w związku z art. 31 ust. 3 Konstytucji. z perspektywy wymogów wynikających z art. 45 ust. 1 Konstytucji osoba wpisana do rejestru dłużników na mocy postanowienia refe-rendarza sądowego powinna mieć zapewnione nie tylko prawo do otrzymania informacji o wydaniu takiego postanowienia i jego treści, ale także prawo do przedstawienia sprawy or-ganowi będącemu sądem w konstytucyjnym rozumieniu (por. także wyrok z 23.05.2018 r. sygn. SK 8/14).

Polecenie zabezpieczające w obecnym kształcie przepisu art. 67g projektu KSC budzi zatem poważne wątpliwości prawne i konstytucyjne. W celu ochrony interesów podmiotów objętych takim poleceniem oraz zapewnienia zgodności z zasadami państwa prawa, zaleca się zniesienie rygoru natychmiastowej wykonalności lub wprowadzenie możliwości zawieszenia wykonania polecenia do czasu rozpatrzenia odwołania, wprowadzenie okresu

„*vacatio legis*" na wycofanie sprzętu lub oprogramowania, zapewnienie możliwości odwołania się od polecenia zabezpieczającego, ograniczenie uznaniowości poprzez precyzyjne określenie przesłanek wydania polecenia zabezpieczającego, zapewnienie rekompensat finansowych dla podmiotów, na które nakładane są polecenia zabezpieczające, obowiązkowe konsultacje z podmiotami objętymi poleceniem przed jego wydaniem, wprowadzenie zasady proporcjonalności w stosowaniu poleceń zabezpieczających oraz ograniczenie możliwości blokowania stron internetowych i usług tylko do wyjątkowych sytuacji, z pełnym uzasadnieniem. Powyższe zmiany są niezbędne, aby przepisy dotyczące poleceń zabezpieczających były zgodne z zasadami demokratycznego państwa prawa oraz chroniły zarówno interesy publiczne, jak i prywatne. W demokratycznym państwie prawnym konieczne jest zapewnienie realnej kontroli instancyjnej decyzji dotyczących zgromadzenia przed jego terminem[9].

Warto także zwrócić uwagę na wyłączenie stosowania art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I KPA w procedurze wydawania polecenia zabezpieczającego ma poważne konsekwencje dla stron postępowania, a także dla praworządności. Poniżej znajduje się analiza poszczególnych przepisów KPA, których wyłączenie wpływa na przebieg postępowania:

a) art. 10 KPA - Zasada czynnego udziału stron w postępowaniu: Wyłączenie tego przepisu oznacza, że strony nie mają zapewnionego prawa do czynnego udziału w postępowaniu, co ogranicza ich możliwość przedstawienia swojego stanowiska, dowodów i argumentów. To może prowadzić do wydania decyzji bez uwzględnienia wszystkich istotnych okoliczności, co wpływa na rzetelność i sprawiedliwość postępowania.
b) art. 34 KPA - Udział organizacji społecznych: Wyłączenie tego artykułu pozbawia organizacje społeczne możliwości uczestniczenia w postępowaniu, co ogranicza społeczną kontrolę nad działaniami administracji i może prowadzić do pominięcia interesu publicznego i zbiorowych interesów społecznych.
c) art. 79 KPA - Prawo do zapoznania się z aktami sprawy i wypowiedzenia się co do zebranych dowodów: Bez tego przepisu, strony nie mają możliwości zapoznania się z aktami sprawy, co uniemożliwia im pełną obronę swoich praw. Brak dostępu do dowodów i informacji zebranych w sprawie prowadzi do nierówności stron i ogranicza transparentność postępowania.
d) art. 81 KPA - Obowiązek informowania stron o zebranych dowodach: Wyłączenie tego przepisu powoduje, że strony nie są informowane o zebranych dowodach, co może prowadzić do sytuacji, w której nie są świadome podstaw decyzji administracyjnej, a tym samym nie mogą skutecznie bronić swoich interesów.

[9] Jak stwierdził Trybunał Konstytucyjny w orzeczeniu z 18.09.2014 sygn. K 4412 procedura odwołania od decyzji o zakazie zgromadzenia publicznego nie spełnia - w obecnym kształcie - wymogu skuteczności środka odwoławczego. Biorąc pod uwagę sposób ujęcia terminów doręczenia decyzji zakazującej zgromadzenia, wniesienie odwołania od tej decyzji oraz rozpatrzenia tego odwołania, uzyskanie rozstrzygnięcia konkretnej sprawy przed planowanym terminem zgromadzenia staje się w praktyce niewykonalne. Świadczy to o nieefektywności obowiązującej procedury odwoławczej.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

e) art. 81a KPA - Prawo do uzupełnienia dowodów i materiałów w sprawie: Brak stosowania tego przepisu uniemożliwia stronom przedstawienie dodatkowych dowodów i wyjaśnień, co może skutkować wydaniem decyzji na podstawie niepełnych lub jednostronnych informacji.
f) art. 107 § 1 pkt 3 KPA - Obowiązek uzasadnienia decyzji: Wyłączenie tego obowiązku oznacza, że decyzje administracyjne mogą być wydawane bez szczegółowego uzasadnienia, co utrudnia stronom zrozumienie podstaw decyzji oraz ogranicza możliwość skutecznego zaskarżenia decyzji w sądzie.
g) art. 145 § 1 pkt 4 KPA - Wznowienie postępowania: Bez możliwości wznowienia postępowania na podstawie nowych okoliczności lub dowodów, strony są pozbawione ważnej drogi prawnej do korekty decyzji administracyjnej w przypadku pojawienia się nowych faktów, które mogłyby wpłynąć na wynik sprawy.
h) art. 156 § 1 pkt 4 KPA - Stwierdzenie nieważności decyzji: Wyłączenie tego przepisu uniemożliwia stwierdzenie nieważności decyzji administracyjnej z powodu rażącego naruszenia prawa. To pozbawia strony ważnej ochrony prawnej przed decyzjami, które są obarczone poważnymi wadami prawnymi.
i) Rozdział 8 działu I KPA - Przepisy dotyczące doręczeń: Wyłączenie tych przepisów oznacza, że procedura doręczenia decyzji administracyjnej nie musi być zgodna z KPA, co może prowadzić do sytuacji, w której strony nie są właściwie informowane o wydanych decyzjach i nie mają możliwości podjęcia odpowiednich działań prawnych w odpowiednim czasie.
j) Wyłączenie powyższych przepisów KPA w procedurze wydawania poleceń zabezpieczających znacząco ogranicza prawa stron i narusza zasady praworządności. Brak udziału stron w postępowaniu, brak dostępu do akt sprawy, brak możliwości wznowienia postępowania czy stwierdzenia nieważności decyzji oraz brak należytego doręczenia decyzji osłabiają kontrolę nad działaniami administracji i mogą prowadzić do decyzji, które są nieprzejrzyste, niesprawiedliwe i trudne do zaskarżenia. Taka regulacja podważa fundamenty sprawiedliwego postępowania administracyjnego i zaufanie obywateli do państwa prawa.

73. Polecenia zabezpieczające – brak notyfikacji technicznej TRIS podważa skuteczność nowego rozwiązania

Jednostka redakcyjna: art. 67g projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Projektodawca zdecydował się na wprowadzenie dodatkowych poleceń zabezpieczających, które nie zostały przewidziane w dyrektywie NIS2. Projektodawca w uzasadnieniu do projektu ustawy jednocześnie twierdzi, że nie ma konieczności notyfikacji technicznej TRIS tych przepisów, mimo, że polecenia zabezpieczające nie stanowią implementacji prawa UE. W poprzedniej wersji projektu ustawy z 2023 r. zrezygnowano z poleceń zabezpieczających, co było spowodowane właśnie wymogiem notyfikacji

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

technicznej, jak wynika z pisma Ministra Cyfryzacji z dnia 23 czerwca 2023 r. (DRC.WL.0610.4.2021). Natomiast w obecna wersja na powrót wprowadza to rozwiązanie a projektodawca twierdzi, że taka notyfikacja techniczna nie jest wymagana. Konsekwencje zaniechania notyfikacji technicznej TRIS są następujące:

- Podważenie skuteczności przepisów: Brak notyfikacji technicznej TRIS może skutkować podważeniem skuteczności nowych rozwiązań prawnych. Notyfikacja jest istotnym elementem zapewniającym, że nowe przepisy są zgodne z prawem unijnym i nie stwarzają barier w jednolitym rynku.
- Ryzyko procedur naruszeniowych: Komisja Europejska może wszcząć procedurę naruszeniową przeciwko Polsce za niewłaściwą implementację prawa unijnego. To może prowadzić do nałożenia kar finansowych oraz konieczności modyfikacji wprowadzonych przepisów.
- Niepewność prawna dla przedsiębiorców: Brak notyfikacji technicznej TRIS może powodować niepewność prawną dla przedsiębiorców działających w sektorach objętych nowymi przepisami. Przedsiębiorcy mogą być zmuszeni do stosowania się do przepisów, które mogą być później zmienione lub uchylone, co generuje dodatkowe koszty i ryzyko biznesowe.
- Ograniczenia dla polskich przedsiębiorców: Nowe, nienotyfikowane przepisy mogą stanowić barierę dla działalności gospodarczej polskich firm na rynku unijnym. Przedsiębiorcy mogą napotkać trudności w uzyskaniu certyfikacji lub zgodności z unijnymi standardami, co ogranicza ich konkurencyjność.
- Zahamowanie inwestycji: Inwestorzy mogą być niechętni do angażowania się w projekty w Polsce, obawiając się niestabilności prawnej i potencjalnych konfliktów z prawem unijnym. To może negatywnie wpłynąć na rozwój gospodarczy i innowacyjność kraju.

Wobec powyższego, wprowadzenie dodatkowych poleceń zabezpieczających bez notyfikacji technicznej TRIS jest decyzją ryzykowną, która może przynieść więcej szkód niż korzyści. Zaleca się ponowne rozważenie konieczności notyfikacji tych przepisów, aby zapewnić zgodność z prawem unijnym i uniknąć potencjalnych negatywnych konsekwencji.

74. Polecenie zabezpieczające

Jednostka redakcyjna: Art. 67g

Zgodnie z projektowanym ust. 8 wprowadzono słuszne uprawnienie dyrektora RCB do dopraszania podmiotów kluczowych lub ważnych do prac zespołu prowadzącego analizę przed wydaniem polecenia zabezpieczającego. Udział w pracach podmiotu wydaje się wręcz

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

niezbędny, aby polecenie było proporcjonalne do zagrożenia oraz realne do wdrożenia bez tworzenia dodatkowych zagrożeń w ramach obsługi incydentu krytycznego.
Wnosimy o uzupełnienie przepisów o wprowadzenie zasady informowania podmiotu kluczowego lub ważnego o rozpoczęciu prac nad ewentualnym wydaniem polecenia zabezpieczającego.

75. Przesłanki do uwzględniania w toku analizy

Jednostka redakcyjna: Art. 67g ust. 5 w zw. z ust. 11

Wnosimy o uzupełnienie katalogu przesłanek analizowanych przed wydanie polecenia zabezpieczającego, o określenie spodziewanych skutków zastosowania się do polecenia w zakresie kosztów jego wdrożenia, czasu niezbędnego na realizację, a także ciągłość świadczenia usług przez podmiot kluczowy lub ważny oraz odtworzenie ich działania.
Rozumiejąc nadzwyczajną instytucję polecenia, zwracamy jednak uwagę na bardzo poważne skutki, które jego zastosowanie może wywołać, także w zakresie odpowiedzialności podmiotu kluczowego lub ważnego wobec podmiotów trzecich, w tym dostawców, usługodawców lub usługobiorców. Tym bardziej jego wydanie musi odbywać się w sposób szeroko uwzględniający skutki wydania decyzji.
Przewidziana w ust. 11 „adekwatność" wydaje się w tym zakresie istotnie niewystarczająca.

76. Czas obowiązywania polecenia zabezpieczającego

Jednostka redakcyjna: Art. 67g ust. 12

Przewidziany maksymalny czas (2 lata) stosowania polecenia zabezpieczającego wydaje się zdecydowanie zbyt długi. W naszej ocenie polecenie powinno być wydawane na okres obsługi incydentu, nie dłuższy niż 30 dni, z możliwością jego przedłużenia, jeśli incydent nie został zamknięty.

77. Brak odpowiedniej formy Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskie

Jednostka redakcyjna: art. 69 projektu KSC
Jednostka redakcyjna NIS2: art. 7
Uwaga: Implementacja przepisów nie powinna polegać na automatycznym przenoszeniu postanowień Dyrektywy NIS2 do krajowego porządku prawnego. Konieczna jest adaptacja i implementacja do realiów prawnych, co obejmuje obowiązujący w Polsce katalog źródeł prawa. Dyrektywa NIS2 nakłada określone obowiązki na państwa członkowskie UE w zakresie

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

cyberbezpieczeństwa, ale każda implementacja musi uwzględniać specyficzne warunki i wymagania prawne danego kraju.
Zasady określone w art. 69 ust. 1 pkt 3 projektu KSC dotyczące współpracy między sektorem publicznym i prywatnym powinny być sformalizowane jako ustawa, aby zapewnić ich przestrzeganie. Taka regulacja zapewniłaby, że obie strony będą zobowiązane do współpracy w określonych warunkach i na określonych zasadach, co zwiększy efektywność działań w zakresie cyberbezpieczeństwa.
Mechanizmy wymiany informacji między organami właściwymi w art. 69 ust. 1 pkt 5 i ust. 2 pkt 8 projektu KSC powinny stanowić materię ustawową. To zapewniłoby, że wszystkie istotne informacje dotyczące cyberzagrożeń, incydentów oraz ryzyka będą systematycznie i skutecznie wymieniane między odpowiednimi podmiotami, co przyczyni się do zwiększenia bezpieczeństwa narodowego w obszarze cybernetycznym.
Wymogi związane z cyberbezpieczeństwem w zamówieniach publicznych (art. 69 ust. 2 pkt 2 projektu KSC) powinny być również wprowadzone jako przepisy rangi ustawowej. Ustawowe wprowadzenie tych wymogów zapewni, że wszystkie zamówienia publiczne będą uwzględniać kwestie bezpieczeństwa cyfrowego, co jest kluczowe dla ochrony infrastruktury krytycznej.
Wątpliwości budzi relacja strategii, o której mowa w art. 69 projektu KSC, w stosunku do strategii, o których mowa w art. 9 ustawy o zasadach prowadzenia polityki rozwoju. Analiza treści uzasadnienia nie przynosi w tym zakresie rozstrzygnięcia. Wprowadzenie strategii cyberbezpieczeństwa powinno być spójne z innymi strategiami rozwojowymi, aby zapewnić jednolitość i koherencję działań na poziomie krajowym. W tym celu niezbędne jest dokładne zbadanie i wyjaśnienie, jak nowa strategia będzie współgrać z istniejącymi planami i strategiami rozwoju, w szczególności w kontekście wykorzystania środków europejskich na realizację celów w zakresie osiągania wysokiego poziomu cyberbezpieczeństwa.

78. Niedopuszczalne zmieszanie kompetencji wojskowych z cywilnymi oraz brak transparentności w formie komunikatu w tej sprawie

Jednostka redakcyjna: art. 67k projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy
Uwaga: Na podstawie art. 67k ust. 1 projektu KSC, Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26 ustawy. Jednakże, niniejsze przepisy budzą poważne zastrzeżenia z kilku kluczowych powodów:
Po pierwsze przepisy art. 67k projektu KSC pozwalają Ministrowi Obrony Narodowej przejąć koordynację działań związanych z obsługą incydentów cyberbezpieczeństwa, bez względu na stan wojny lub stan wojenny. Oznacza to, że w drodze arbitralnego komunikatu, MON może uzyskać kompetencje, o których mowa w art. 26 projektu KSC, rozciągające się na całą

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

cyberprzestrzeń w Polsce, nawet w czasie pokoju. Takie rozwiązanie jest niedopuszczalne, ponieważ prowadzi do zmieszania kompetencji wojskowych z cywilnymi. Wprowadzenie tego typu kompetencji dla MON w czasie pokoju narusza zasadę rozdziału władzy cywilnej i wojskowej, co jest fundamentalną zasadą demokratycznego państwa prawa.
Po drugie powierzenie realizacji zadań odbywa się na podstawie komunikatu ogłaszanego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". Komunikat ten nie ma charakteru decyzji administracyjnej, co uniemożliwia podmiotom dotkniętym tym komunikatem odwołanie się od niego i skutecznie kwestionowanie jego zasadności. Taka forma jest nieakceptowalna, gdyż łamie podstawowe zasady praworządności i transparentności, przewidziane w Konstytucji RP.
Po trzecie przepisy nie określają maksymalnego okresu, na jaki mogą zostać powierzone zadania Ministrowi Obrony Narodowej. Aby zapewnić tymczasowy charakter tego powierzenia, powinno być ono ograniczone do konkretnego okresu, np. nie dłużej niż 3 miesiące. Brak takiego ograniczenia stwarza ryzyko, że tymczasowe powierzenie zadań może de facto stać się permanentne, co dodatkowo narusza zasadę rozdziału kompetencji wojskowych i cywilnych
Wreszcie powierzenie Ministrowi Obrony Narodowej realizacji zadań w zakresie cyberbezpieczeństwa, nawet w czasie pokoju, może prowadzić do erozji cywilnej kontroli nad wojskiem. Jest to szczególnie niebezpieczne w kontekście utrzymania równowagi między siłami cywilnymi a wojskowymi, co jest kluczowym elementem stabilności i bezpieczeństwa demokratycznego państwa.

79. Nieprawidłowa forma prawna Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę (uchwała Rady Ministrów to akt prawa wewnętrznego, a nie źródło prawa).

Jednostka redakcyjna: art. 72a projektu KSC
Jednostka redakcyjna NIS2: art. 9
Uwaga: Zgodnie z art. 72a projektu KSC Rada Ministrów przyjmuje Krajowy plan reagowania na incydenty i sytuacja kryzysowe w cyberbezpieczeństwie na dużą skalę w drodze uchwały. Taki plan określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwa na dużą skalę, a w szczególności zawiera:

a) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie;
b) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
c) rodzaje krytycznej infrastruktury informatycznej;
d) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu incydentami i

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Ww. materia nie powinna jednak stanowić przedmiot regulacji uchwały Rady Ministrów. Zgodnie z art. 93 Konstytucji RP uchwały Rady Ministrów oraz zarządzenia Prezesa Rady Ministrów i ministrów mają charakter wewnętrzny i obowiązują tylko jednostki organizacyjnie podległe organowi wydającemu te akty. Oznacza to zatem, że uchwała Rady Ministrów w postaci Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie nie może obejmować materii dotyczących sektora prywatnego, sektora publicznego w zakresie jakim nie podlega Radzie Ministrów (np. jednostki samorządu terytorialnego). Proponowane zatem postanowienie wykracza poza kompetencje Rady Ministrów i wymagają one zmiany na formę odpowiedniego rozporządzenia lub ustawy.

80. Nieprecyzyjna zawartość Krajowego planu reagowania na incydenty i sytuacje kryzysowe w Cyberbezpieczeństwie na dużą skalę

Jednostka redakcyjna: art. 72b projektu KSC
Jednostka redakcyjna NIS2: art. 9

Uwaga: W art. 72b projektu KSC projektodawca posługuje się pojęciami, które nie są jednoznacznie zdefiniowane, co może negatywnie wpłynąć na wykonalność Krajowego planu. W szczególności:

a) W ust. 2 pkt 1) nie wiadomo, o jakiej gotowości mowa (*Krajowy Plan zawiera w szczególności: cele krajowych środków i działań służących w zakresie gotowości* (?)). Nie jest jasne, które podmioty zaliczają się do sektora publicznego, a które do prywatnego (czy np. spółki Skarbu Państwa należą do sektora prywatnego, czy publicznego – ust. 2 pkt 5).

b) Nie jest sprecyzowane, co rozumie się przez "krytyczną infrastrukturę informatyczną" (ust. 2 pkt 6), zwłaszcza w kontekście definicji infrastruktury krytycznej zawartej w ustawie o zarządzaniu kryzysowym, której wykazy stanowią załączniki do planów zarządzania kryzysowego (por. art. 5 ustawy o zarządzaniu kryzysowym).

c) Brak jest informacji na temat systemowej relacji ww. krajowego planu do planów zarządzania kryzysowego, a w szczególności niejasna jest relacja między Krajowym Planem Zarządzania Kryzysowego a Krajowym planem reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.

81. Przekazanie w całości Krajowego planu reagowania na incydenty i sytuacje kryzysowe w Cyberbezpieczeństwie na dużą skalę Komisji Europejskiej i

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa

Jednostka redakcyjna: art. 72f projektu KSC
Jednostka redakcyjna NIS2: art. 9 ust. 5

Uwaga: Zgodnie z art. 9 ust. 5 NIS2 Państwa członkowskie przedkładają Komisji i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa (EU-CyCLONe) ważne informacje związane z wymogami określonymi w ust. 4, dotyczące krajowych planów reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę w terminie trzech miesięcy od daty przyjęcia tych planów. Państwa członkowskie mogą wyłączyć niektóre informacje, jeżeli i w zakresie w jakim jest to kluczowe z punktu widzenia ich bezpieczeństwa narodowego. Natomiast projekt ustawy w ogóle nie korzysta z tego zastrzeżenia, co może rodzić wątpliwości co do zakresu przekazywanych informacji mających istotne znaczenie z punktu widzenia bezpieczeństwa narodowego. Proponowane przepisy w tym zakresie nie przewidują objęcia informacji znajdujących się w tym planie tajemnicą państwową, a ponadto, mimo że NIS2 wymaga przekazania jedynie elementów takiego planu, projektodawca zamierza przekazywać plan w całości, bez względu na analizę co do przydatności takich informacji dla Komisji Europejskiej i europejskiej sieci organizacji łącznikowych, a także zasadę minimalizacji i ochrony informacji o krytycznym dla Polski znaczeniu (ujawnienie informacji może bowiem nastąpić na poziomie innego Państwa Członkowskiego).

82. Wprowadzenie wysokich kar administracyjnych, w sytuacji gdy nie wynika to z NIS2

Jednostka redakcyjna: art. 73 ust.1 pkt 15), 19), 20), 21) i ust. 1a projektu KSC
Jednostka redakcyjna NIS2: art. 34 ust. 4 i 5

Uwaga: Zgodnie z art. 34 ust. 4 i 5 NIS2 państwa członkowskie zapewniają, by podmioty kluczowe i podmioty ważne dokonujące naruszeń art. 21 lub 23 NIS2 podlegały wysokim karom pieniężnym, których limit został określony w dyrektywie. Wysokość tych kar została wprowadzona w projekcie KSC, niemniej nie wszystkie naruszenia przepisów kwalifikujących się pod karę w wysokości określonej w projekcie ustawy to naruszenia art. 21 i 23 NIS2. Dodatkowo projektodawca nie wprowadził żadnego stopniowania kary – choć kary powinny być proporcjonalne (por. art. 36 NIS2). Innymi słowy polska implementacja zamiast dokonać stopniowania kar, tam gdzie to możliwe i zgodne z NIS2, to proponuje podejście zgodnie z którym wysokość kary została pozostawiona decyzji administracyjnej. W praktyce oznacza to, że podmiot ważny lub kluczowy może otrzymać kilkadziesiąt milionów EUR kary za czynności zakwalifikowane jako „utrudniania" wykonywania kontroli" (art. 73 ust. 1 pkt 15 projektu KSC), czy nie zapewnienia użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej (art. 73 ust. 1a projektu KSC). Ryzyko takie pewnie mogłoby być teoretyczne – jednak czy w kontekście zasady praworządności oraz zasady proporcjonalności kary, wynikającej z art. 36 NIS2, konieczne byłoby wprowadzenie stopniowania kar, tam gdzie to możliwe. W odróżnieniu od odpowiedzialności karnej, w przypadku administracyjnych kar pieniężnych często nie jest wymagane stwierdzenie winy. Istotne jest samo stwierdzenie faktu naruszenia przepisów.

83. Fakultatywność kary pieniężnej (opcja alternatywna w stosunku do propozycji powyżej)

Jednostka redakcyjna: Art. 73 ust. 1

Propozycja zmiany:

„ust. 1 otrzymuje brzmienie:

*„1. Karze pieniężnej **może** podlegać podmiot kluczowy lub podmiot ważny, który:*

(…)

***– jeżeli przemawia za tym czas, zakres lub charakter naruszenia**.*

W obecnym brzmieniu art. 73 ust. 1 każde naruszenie ww. obowiązków obliguje do nałożenia kary pieniężnej. W ocenie KL nieznaczne i nieintencjonalne naruszenie nie może skutkować automatyczną sankcją. Organ właściwy do spraw cyberbezpieczeństwa powinien za każdym razem uwzględniać czas, zakres oraz charakter naruszenia, podobnie jak w przypadku oceny naruszeń kierownika podmiotu kluczowego lub podmiotu ważnego (art. 73a). Powyższa zmiana ujednoliciłaby brzmienie art. 73 w zakresie ust. 1a projektu ustawy, przecinając wątpliwości interpretacyjne co do obligatoryjności administracyjnej kary pieniężnej, zwłaszcza w świetle możliwości odstąpienia od nałożenia kary przewidzianym w art. 76a ust.

84. Powrót do limitowania wysokości kary pieniężnej w zależności od rodzaju naruszenia ustawy (rozwinięcie propozycji przedstawionej w pkt 74)

Jednostka redakcyjna: Art. 73 ust. 2

„ust. 2 otrzymuje brzmienie:

„2. Wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1, wynosi do _____

2) ust. 1 pkt 2, wynosi do 150 000 zł;

3) ust. 1 pkt 3, wynosi do _____

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

4) ust. 1 pkt 4, wynosi do 100 000 zł;

5) ust. 1 pkt 5, wynosi do 50 000 zł;

6) ust. 1 pkt 6, wynosi do _____

7) ust. 1 pkt 7, wynosi do 20 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu;

8) ust. 1 pkt 8, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego

9) ust. 1 pkt 9, wynosi do _____

10) ust. 1 pkt 10, wynosi do _____

11) ust. 1 pkt 11, wynosi do _____

12) ust. 1 pkt 12 i 13, wynosi do 20 000 zł;

13) ust. 1 pkt 14 i 17, wynosi do 200 000 zł;

14) ust. 1 pkt 15, wynosi do 50 000 zł

15) ust. 1 pkt 16, wynosi do _____

16) ust. 1 pkt 18, wynosi do _____

17) ust. 1 pkt 19, wynosi do _____

18) ust. 1 pkt 20, wynosi do _____

19) ust. 1 pkt 21, wynosi do _____

20) ust. 1a pkt 2, wynosi do 20 000 zł;

Postulujemy przywrócenie limitowania kar pieniężnych co do niektórych obowiązków, zwłaszcza tych, których naruszenie nie może prowadzić do wyrządzenie znacznej szkody. Nakładanie kary z uwzględnieniem sytuacji majątkowej podmiotu istniejącego w chwili wydania decyzji o nałożeniu kary nie może prowadzić do sytuacji, gdzie podmiot (np. wskutek niewyznaczenia osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi) może podlegać karze, której górna granica wynosi odpowiednio 7 milionów euro dla podmiotów ważnych, a 10 milionów euro w przypadku podmiotów kluczowych. Uwzględnienie specyfiki każdego z obowiązków oraz stopnia potencjalnego ich naruszenie pozwoli na ukształtowanie odpowiednich „limitów" kar pieniężnych, co ochroni podmioty kluczowe lub podmioty ważne przed nałożeniem nieproporcjonalnie wysokiej kary w stosunku do wagi naruszenia.

85. Nieproporcjonalna wysokość kar dla podmiotów ważnych

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Jednostka redakcyjna: art. 73 ust. 4 projektu KSC
Jednostka redakcyjna NIS2: art. 34 ust. 5

Uwaga: Projektodawca proponuje określenie tej samej podstawy wymiaru kary dla podmiotów ważnych i kluczowych w sytuacji, gdy okres działalności takich podmiotów jest krótszy niż rok. Podstawą wymiaru kary jest kwota 500 000 EUR i kwota ta dotyczy zarówno podmiotu ważnego i kluczowego, podczas gdy w art. 34 ust. 5 NIS2 dokonano obniżenia wysokości kary dla podmiotu ważnego. Zasada ta powinna zostać również odpowiednio odzwierciedlona w wymiarze kary dla podmiotu ważnego prowadzącego działalność gospodarczą krócej niż 12 miesięcy.

86. Kara do 100 mln zł. Nieproporcjonalne kary za bezpośrednie i poważne zagrożenie cyberbezpieczeństwa lub zagrożenie wywołania poważnej szkody lub utrudnień w świadczeniu usług

Jednostka redakcyjna: Art. 73 ust. 5
Jednostka redakcyjna NIS2: art. 34 ust. 4 i 5

W pierwszej kolejności zauważamy, że określenie dodatkowych pułapów kar wykracza poza zakres wynikający wprost z NIS2. W naszej ocenie wystarczające są przewidziane już, bardzo wysokie kary za naruszenie poszczególnych przepisów ustawy, które mogą wynosić nawet do 10 mln EUR i będą wielokrotnie przekraczać dotychczasowy pułap maksymalny za naruszenia, który według art. 73 ust. 5 wynosi 10 mln zł.
W drugiej kolejności zauważamy, że redakcja przepisu powoduje, że będzie istniała nadmiarowa dowolność w zakresie interpretacji danego naruszenia jako stanowiącego poważne zagrożenie, czy skutkującego powstaniem poważnych szkód majątkowych lub poważnych utrudnień w świadczeniu usług. W praktyce, zasadniczo niemal każde naruszenie będzie obarczone ryzykiem nałożenia kary w wysokości do 100 mln zł. Ponadto zauważamy usunięcie z przepisu istotnego słowa, które znajdowało się w jego dotychczasowym brzmieniu, tj. wskazania na „uporczywość" danego naruszenia. Miało ono kluczowe znaczenie dla nadania stosowaniu aktualnego przepisu większej proporcjonalności i ograniczenia do naruszeń, których w szczególności podmiot miał świadomość, a nie podejmował w ich zakresie działań naprawczych.
Poza tym, w projektowanym stanie prawnym nie będzie jest jasne jaka jest relacja do uprawnienia nałożenia kary z ust. 1 do kary z ust. 5. W naszej ocenie istnieje ryzyko nakładania kar podwójnego karania za te same naruszenia.
Z tego względu przepis ten powinien zostać usunięty z projektu. Kary maksymalne w wysokości do 10/7 mln EUR są zdecydowanie wystarczające i spełniają funkcję prewencyjną, represyjną i będzie adekwatnie dolegliwie odstraszać od naruszeń.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Jest to kara o bardzo wysokiej dolegliwości – choć przepis wymienia tylko jej maksymalną wysokość, to jak wynika z orzecznictwa, istnieje zasada, że **maksymalny pułap kary administracyjnej** powinien być brany pod uwagę przy wymierzaniu sankcji. Oznacza to, że bez względu na skalę działalności podmiotu punktem referencyjnym do wymierzenia kary będzie kara w wysokości 100 000 000 zł. Tak wysoki limit kary jest również nieproporcjonalny mając na uwadze przepisy art. 7 ustawy o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary. Zgodnie z nim wobec podmiotu zbiorowego sąd orzeka karę pieniężną w wysokości od 1000 do 5 000 000 złotych, nie wyższą jednak niż 3% przychodu osiągniętego w roku obrotowym, w którym popełniono czyn zabroniony będący podstawą odpowiedzialności podmiotu zbiorowego. A zatem tak wysoki pułap kary nie jest proporcjonalny do innych kar, już funkcjonujących w polskim systemie prawnym, za czyny o znacznie wyższym zabarwieniu negatywnym.

87. Przesłanki nadania rygoru natychmiastowej wykonalności dla decyzji w sprawie wymierzenia kary

Jednostka redakcyjna: art. 74 ust. 2 projektu KSC
Jednostka redakcyjna NIS2: art. 34 ust. 1

Uwaga: Projektodawca wprowadził możliwość nałożenia na decyzję w sprawie kary rygoru natychmiastowej wykonalności w całości lub w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego. Okoliczności te jednak są bez znaczenia dla określenia rygoru natychmiastowej wykonalności. Rygor ten bowiem co do zasady nie jest nakładany na decyzje administracyjne w sprawie kar ze względu na uzasadnione ryzyko naruszenia podstawowych praw podmiotu, uniemożliwiając mu odwołanie się od sankcji – nałożona kara pieniężna (szczególnie gdy może osiągnąć 100 mln zł) może bowiem spowodować zaprzestanie działalności bez możliwości odwołania się. Ogólna zasada nadawania rygoru natychmiastowej wykonalności określona w art. 108 kpa odwołuje się do takich kwestii jak ochrona zdrowia lub życia ludzkiego albo dla zabezpieczenia gospodarstwa narodowego przed ciężkimi stratami bądź też ze względu na inny interes społeczny lub wyjątkowo ważny interes strony. Niemniej w przypadku administracyjnej kary pieniężnej mamy do czynienia z relacją państwo – podmiot ukarany, stąd ewentualny rygor natychmiastowej wykonalności mógłby być uzasadniony np. uzasadnionym podejrzeniem podejmowania działań, mających na celu bezprawne uniknięcie zapłaty wymierzonej kary (np. wyprowadzanie środków pieniężnych). Odwołanie się natomiast do ogólnych klauzul ochrona bezpieczeństwa lub porządku publicznego wypacza sens nadania rygoru natychmiastowej wykonalności, ponieważ w istocie oznacza możliwość arbitralnego nadawania takiego rygoru. Podczas gdy nadawanie rygoru natychmiastowej wykonalności dla decyzji administracyjnych wymierzających kary powinno być wyjątkiem. Analogicznej konstrukcji, do projektowanego art. 74 ust. 2 projektu KSC próżno szukać w ustawie – Prawo

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

telekomunikacyjne, czy w ustawie o ochronie danych osobowych. Przykładowo w ustawie – Prawo telekomunikacyjne, zgodnie z art. 206 ust. 2aa, decyzje regulacyjne podlegają natychmiastowemu wykonaniu, ale z wyjątkiem decyzji w sprawie nałożenia kar, właśnie z uwagi na ich nieodwracalne skutki.

88. Mechanizm finansowania pracowników organów ds. cyberbezpieczeństwa z nakładanych kar

Jednostka redakcyjna: art. 74 ust. 3 projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: W art. 74 ust.3 projektu KSC proponuje się utrzymanie zasady, zgodnie z którą wpływy z kar nakładanych na podstawie ustawy o krajowym systemie cyberbezpieczeństwa stanowią przychody Funduszu Cyberbezpieczeństwa. Taki mechanizm budzi kontrowersje z kilku istotnych powodów. Przede wszystkim, powiązanie wpływów z kar z wynagrodzeniami osób odpowiedzialnych za ich nakładanie rodzi poważne wątpliwości co do bezstronności i obiektywizmu procesu nakładania tych kar. Mechanizm ten może prowadzić do sytuacji, w której osoby mające kompetencje do nakładania kar będą bardziej skłonne do ich stosowania, nawet w przypadkach, gdzie mogłyby one być nieadekwatne lub zbyt surowe. Zwiększenie wpływów Funduszu Cyberbezpieczeństwa poprzez nakładanie większej liczby kar bezpośrednio wpływa na wynagrodzenia osób odpowiedzialnych za te decyzje, co może stanowić bodziec do nadużyć. Takie rozwiązanie może być postrzegane jako konflikt interesów, podważając zaufanie do całego systemu cyberbezpieczeństwa. Działanie organów państwa musi być transparentne i wolne od konfliktu interesów. Przepisy prawa powinny być konstruowane w taki sposób, aby zapobiegać sytuacjom, w których decyzje administracyjne mogą być podejmowane z pobudek osobistych lub finansowych. W świetle tego proponowane brzmienie (choć utrzymujące dotychczasową konstrukcję art. 74 ustawy KSC może być uznane za sprzeczne z zasadą bezstronności działania organów państwowych. Choć idea Funduszu Cyberbezpieczeństwa jako źródła finansowania wynagrodzeń osób realizujących zadania z zakresu cyberbezpieczeństwa jest uzasadniona, to powiązanie wpływów z kar z tym funduszem rodzi poważne wątpliwości natury etycznej i prawnej. Dla zapewnienia bezstronności oraz zaufania do systemu cyberbezpieczeństwa, konieczne jest przemyślenie i zmodyfikowanie tego mechanizmu, tak aby unikać potencjalnych nadużyć oraz konfliktu interesów.

89. Niekonstytucyjny mechanizm wymuszenia realizacji ostrzeżeń

Jednostka redakcyjna: art. 74 ust. 3 i art. 53 ust. 4 projektu KSC
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Na podstawie art. 53 ust. 4 ustawy KSC, w przypadku uzasadnionego podejrzenia naruszenia przepisów ustawy przez podmiot kluczowy, organ właściwy do spraw

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, wskazując czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania naruszania przepisów ustawy. Następnie, zgodnie z art. 76b ust. 1 tejże ustawy, organ może nałożyć na podmiot kluczowy okresową karę pieniężną w wysokości od 500 zł do 100 000 zł za każdy dzień opóźnienia w wykonaniu czynności określonych w ostrzeżeniu. Jednakże, należy podkreślić, że ostrzeżenie, o którym mowa w art. 53 ust. 4 projektu KSC, nie stanowi decyzji administracyjnej ani postanowienia. Forma prawna tego dokumentu nie jest jasno określona w przepisach. Brak precyzyjnego zdefiniowania formy prawnej ostrzeżenia rodzi poważne wątpliwości co do jego charakteru i skutków prawnych. Podmiot, który otrzymał takie ostrzeżenie, może zostać obciążony wysoką karą dzienną aż do 100 000 zł, co stanowi poważne obciążenie finansowe. Nakładanie takiej kary na podstawie dokumentu, który nie ma jednoznacznie określonej formy prawnej, łamie podstawowe zasady praworządności i demokratycznego państwa prawa, przewidziane w Konstytucji RP. W demokratycznym państwie prawa każda ingerencja organu administracji publicznej w prawa i obowiązki obywateli musi być jasna, precyzyjna i oparta na jednoznacznych przepisach prawnych. Zgodnie z art. 2 Konstytucji RP, Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej. W demokratycznym państwie prawa każda ingerencja organu administracji publicznej w prawa i obowiązki obywateli musi być jasna, precyzyjna i oparta na jednoznacznych przepisach prawnych. Ponadto, zgodnie z art. 7 Konstytucji RP, organy władzy publicznej działają na podstawie i w granicach prawa. Nakładanie kary na podstawie ostrzeżenia, którego forma prawna nie jest jasno określona, stoi w sprzeczności z tymi fundamentalnymi zasadami.

90. Dzienna kara pieniężna

Jednostka redakcyjna: Art. 76b ust. 1

Kolejną formą kary pieniężnej nieprzewidzianą wprost w dyrektywie NIS2 jest możliwość nakładania kar dziennych *„w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego obowiązków”.* Jak wskazaliśmy wyżej, w naszej ocenie wysokość zwiększana wielokrotnie wysokości maksymalnych kar pieniężnych stanowi pełne i wystarczające narzędzie odstraszające. Jednocześnie, maksymalny pułap możliwe kary dziennej tj. 100 tys. zł został określony na zbyt wysokim poziomie. W przypadku utrzymania tego przepisu na kolejnych etapach prac maksymalną karę dzienną należy obniżyć do poziomu wynoszącego maksymalnie 5 tys. zł.

91. Przekazywanie danych operacji finansowych przez Szefa Krajowej Administracji Skarbowej organom właściwym do spraw cyberbezpieczeństwa oraz CRIST NASK

Jednostka redakcyjna: art. 299i ustawy Ordynacja podatkowa
Jednostka redakcyjna NIS2: art. 3 ust. 4

Uwaga: Zgodnie z projektowanym art. 299i ustawy – Ordynacja podatkowa, Szef Krajowej Administracji Skarbowej udostępnia organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego (CRIST) działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, dane nieodpłatnie, w drodze teletransmisji, bez konieczności składania każdorazowo pisemnych wniosków o udostępnienie. Dane te obejmują roczne zatrudnienie, roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych, w zakresie niezbędnym do dokonania przez te podmioty weryfikacji wielkości przedsiębiorstwa zgodnie z art. 5 ust. 1 i ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Chociaż dane dotyczące rocznego obrotu netto ze sprzedaży towarów, wyrobów i usług mogą być uzasadnione, warto zaznaczyć, że nie są one tożsame z pojęciem przychodu. Zupełnie niezrozumiałe jest, dlaczego miałyby być przekazywane dane z operacji finansowych, które są objęte tajemnicą skarbową, na rzecz organów do spraw cyberbezpieczeństwa. Taki zakres przekazywania danych jest nadmiarowy i nieproporcjonalny. Narusza on podstawowe zasady prawa, w tym zasadę praworządności (por. art. 7 Konstytucji RP). Z art. 51 ust. 5 Konstytucji RP wynika, że zasady i tryb gromadzenia oraz udostępniania informacji o jednostce określa ustawa. Oznacza to, że organy władzy publicznej nie mogą dowolnie dysponować informacjami o jednostce, lecz wyłącznie na zasadach i w trybie ściśle określonym w ustawie. Trybunał Konstytucyjny wielokrotnie podkreślał, że w ustawie powinny być uregulowane takie zagadnienia, jak zobowiązanie do ujawnienia informacji o swojej osobie, określenie podmiotów zobowiązanych, okoliczności powstania obowiązku ujawnienia informacji oraz zakres tych informacji, a także zasady ich przechowywania, poprawiania, udostępniania i usuwania (wyrok z dnia 6 czerwca 2018 r., sygn. akt K 53/16, OTK-A z 2018 r., poz. 38; wyrok Trybunału Konstytucyjnego z dnia 19 lutego 2002 r., sygn. akt U 3/01, OTK z 2002 r., Nr 1/A, poz. 3). Wreszcie ustawa musi określać tryb gromadzenia i udostępniania informacji, a więc procedurę postępowania podmiotu, który tymi informacjami dysponuje (wyroki Trybunału Konstytucyjnego z dnia 19 lutego 2002 r., sygn. akt U 3/01; z dnia 16 lipca 2015 r., sygn. akt K 2/13; z dnia 6 czerwca 2018 r., sygn. akt K 53/16). Materia ustawowa powinna obejmować zasady gromadzenia i udostępniania informacji, w tym ich przetwarzanie. Ustawa musi także określać tryb gromadzenia i udostępniania informacji, a więc procedurę postępowania podmiotu, który tymi informacjami dysponuje.

Warto również zauważyć, że w art. 43 ust. 2 projektu KSC proponuje się wprowadzenie kompetencji dla organów właściwych do spraw cyberbezpieczeństwa w zakresie przekazywania informacji z rejestrów publicznych, z zachowaniem przepisów o tajemnicach prawnie chronionych. Oznacza to, że dostęp do informacji został już zapewniony, co budzi

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

głębokie wątpliwości co do potrzeby przyznawania dodatkowych uprawnień dotyczących danych podatkowych.

92. Brak definicji rocznej liczby pracowników lub rocznej liczby ubezpieczonych w ustawie o systemie ubezpieczeń społecznych i w ustawie Ordynacja podatkowa

Jednostka redakcyjna: art. 50 ust. 28 ustawy o systemie ubezpieczeń społecznych; art. 299i § 2 ustawy – Ordynacja podatkowa
Jednostka redakcyjna NIS2: nie dotyczy
Uwaga: W art. 50 ustawy o systemie ubezpieczeń społecznych proponuje się dodanie przepisu, zgodnie z którym Zakład Ubezpieczeń Społecznych miałby udostępniać organom właściwym do spraw cyberbezpieczeństwa i Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, drogą elektroniczną, dane zgromadzone na koncie płatnika składek, o których mowa w art. 45 tej ustawy. Dane te obejmowałyby roczną liczbę pracowników lub roczną liczbę ubezpieczonych, w zakresie niezbędnym do realizacji ich ustawowych zadań. Podobny przepis został zaproponowany w ustawie – Ordynacja podatkowa (art. 299i). Niemniej ani ustawa o systemie ubezpieczeń społecznych, ani ustawa – Ordynacja podatkowa nie posługują się pojęciem rocznej liczby pracowników czy ubezpieczonych. Brak definicji tych pojęć rodzi praktyczne i wymierne konsekwencje, ponieważ nie jest jasne, jak należy liczyć taką roczną liczbę pracowników – czy ma to być liczba na koniec roku (31 grudnia), średnioroczna, czy wystarczy przekroczenie 250 pracowników przez jeden dzień w roku. Kwestie te mają istotne znaczenie prawne z uwagi na konsekwencje dla podmiotu co do kwalifikacji jako podmiot ważny lub kluczowy. Bez precyzyjnej definicji, podmioty mogą mieć trudności w interpretacji przepisów i spełnieniu wymogów ustawy, co może prowadzić do niepewności i niezgodności z prawem.

93. Niepotrzebne wyłączenie stosowania art. 54 i 55 tzw. Konstytucji dla Biznesu (ustawy – Prawo przedsiębiorców)

Jednostka redakcyjna: art. 61 pkt 3 ustawy – Prawo przedsiębiorców
Jednostka redakcyjna NIS2: nie dotyczy
Uwaga: Artykuł 61 pkt 3 ustawy – Prawo przedsiębiorców określa wyłączenia stosowania przepisów Prawa przedsiębiorców, które dotyczą zakazu równoczesnych kontroli oraz ograniczonego czasu trwania kontroli. Projektodawca proponuje wyłączenie kolejnej kategorii kontroli dotyczących przedsiębiorców, tj. kontroli obowiązków związanych z cyberbezpieczeństwem. Taki wymóg nie wynika z treści NIS2 i wygląda na to, że zamiast dążyć do ograniczania obciążeń i równoczesnych kontroli, projektodawca nakłada kolejne ograniczenia na przedsiębiorców bez należytego uzasadnienia. Gdyby brzmienie przepisu

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

było ograniczone do nagłych przypadków lub zarządzania incydentami, miałoby to bardziej logiczne uzasadnienie. Natomiast projektodawca świadomie szeroko definiuje podmiotowe wyłączenie, co w praktyce iluzoryczną czyni ochronę praw przedsiębiorców. Dodatkowo, kontrole mogą być prowadzone w sposób nieograniczony w czasie, co – jak pokazuje praktyka – zachęca do przedłużania czynności kontrolnych. Takie podejście jest sprzeczne z duchem Konstytucji dla Biznesu, która ma na celu ochronę przedsiębiorców przed nadmiernym obciążeniem administracyjnym i zapewnienie im stabilnych warunków do prowadzenia działalności gospodarczej.

94. Brak wystarczającego uzasadnienia dla wykluczeniu w zamówieniach publicznych dla produktów, usług lub procesów ICT po wystosowaniu (niewiążących) rekomendacji

Jednostka redakcyjna: art. 226 ust. 1 ustawy – Prawo zamówień publicznych
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Projektodawca zakłada, że oferty składane w zamówieniach publicznych obejmujące produkty ICT, usługi ICT lub procesy ICT wskazane w rekomendacjach, o których mowa w art. 33 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa lub w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, będą odrzucane. Należy jednak odwołać się do art. 13 lit. a) Dyrektywy 2009/81/WE, który przewiduje wyłączenia związane z zamówieniami, w przypadku których stosowanie przepisów tej dyrektywy zobowiązywałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje ono za sprzeczne z jego podstawowymi interesami bezpieczeństwa. Należy rozważyć, czy rzeczywiście wyłączenie stosowania prawa zamówień publicznych jest adekwatne i ściśle związane z podstawowymi interesami bezpieczeństwa, w sytuacji gdy niemal każdy urząd i podmioty im podległe lub nadzorowane będą objęte wyłączeniem. Wynika to z bardzo szerokiego katalogu zadań obejmujących m.in. ochronę zdrowia, bezpieczeństwo ekonomiczne, dostawy energii, sprawiedliwość, ochronę środowiska, weterynaryjną ochronę zdrowia publicznego, nadzór sanitarny oraz zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym zapewnienie ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa. Proponowane przepisy wydają się nadmiernie szerokie, co budzi wątpliwości co do ich proporcjonalności i adekwatności do każdego zamówienia publicznego udzielanego na podstawie przepisów ustawy o zamówieniach publicznych. Taki szeroki zakres wyłączeń może prowadzić do destabilizacji systemu udzielania zamówień publicznych, ponieważ może dochodzić do sytuacji, w których konieczne będzie odrzucenie danej oferty ze względu na poboczne wykorzystywanie produktów, usług lub procesów ICT objętych rekomendacją lub decyzją o uznaniu dostawcy za dostawcę wysokiego ryzyka[10]. Co więcej do

[10] W tym zakresie swoje wątpliwości podnosił także Minister ds. Unii Europejskiej do poprzedniej wersji tego projektu. Warto także w tym kontekście przywołać opinie: opinia nr DPUE.920.1030.2021.AR(43), opinia

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

wyłączeń z zamówień publicznych dojdzie w wyniku wydania rekomendacji, nie posiadających rangi źródła prawa.

95. Brak zwrotu niewydatkowanych lub nieprawidłowo wydatkowanych środków z Funduszu Cyberbezpieczeństwa do budżetu państwa

Jednostka redakcyjna: art. 2 ust. 4 ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Projektodawca proponuje wprowadzenie przepisu, zgodnie z którym jakiekolwiek dotacje z budżetu państwa udzielane Funduszowi Cyberbezpieczeństwa nie podlegają zwrotowi. Przepis ten oznacza wyłom od naczelnej zasady finansów publicznych, tj. obowiązku zwrotu dotacji w przypadku ich niezgodnego z przeznaczeniem wykorzystania, pobrania nienależnie lub w nadmiernej wysokości, zgodnie z ustawą z dnia 27 sierpnia 2009 r. o finansach publicznych. Proponowana konstrukcja powoduje, że dotacje z budżetu państwa nie będą podlegać zwrotowi, nawet w przypadku niewykorzystania środków lub ich nieprawidłowego wydatkowania, co może prowadzić do szkód dla finansów publicznych. Taki przepis jest sprzeczny z zasadą odpowiedzialności za publiczne środki finansowe i może skutkować brakiem odpowiedniego nadzoru nad wydatkowaniem środków z Funduszu Cyberbezpieczeństwa. Przykładem bardziej zasadnego podejścia jest art. 43 § 15 kodeksu karnego wykonawczego, który tworzy Fundusz Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej, gdzie przewidziane są mechanizmy kontroli i zwrotu niewykorzystanych lub niewłaściwie wykorzystanych środków. Wprowadzenie podobnych zasad dla Funduszu Cyberbezpieczeństwa byłoby zgodne z zasadami finansów publicznych i zapewniłoby lepszą ochronę środków publicznych.[11] .

96. Art. 14 ustawy nowelizującej – termin realizacji obowiązków i wpis do rejestru

Wyjaśnienia wymaga relacja projektowanego art. 14 ust. 1 ustawy nowelizującej, który wskazuje termin półroczny na realizację wszystkich obowiązków z rozdziału 3 wobec projektowanego art. 16 ustawy uksc, który również wskazuje termin 6 miesięczny od dnia spełnienia przesłanek uznania za podmiot kluczowy lub ważny, ale od wejścia w życie ustawy.

nr DPUE.920.1030.2021.AR(27), opinia nr KPDPUE.920.1030.2020.AR(2)), opinia nr DPUE.920.1030.2021.KWM(47), opinia nr DPUE.920.1030.2021.KWM(52), DPUE.920.1030.2021.KWM(57).

[11] Zgodnie z tym przepisem: W przypadku wykorzystania dotacji niezgodnie z przeznaczeniem lub pobranych nienależnie lub w nadmiernej wysokości stosuje się odpowiednio przepisy ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych dotyczące dotacji udzielonych z budżetu państwa.

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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 szczególności, w przypadku art. 14 mowa o wszystkich wymaganiach, w tym audycie, który wg art. 16 ma być wykonany w ciągu 12 miesięcy po raz pierwszy.
Podobnie niejasna jest relacja art. 14 ust. 2 dot. „zarejestrowania się" w wykazie zgodnie z „komunikatem o harmonogramie" wobec art. 7 ust. 3, który termin na „złożenie wniosku o wpis" w wykazie składa się w terminie 2 miesięcy od dnia spełnienia wymogów.
Kwestie te wymagają ponownej weryfikacji i szczegółowego opisania w uzasadnieniu projektu.

97. Uwagi redakcyjne

- Projektowany art. 2 pkt 8a – odesłanie do ustawy o rachunkowości powinno dotyczyć art. 3 ust. 1 pkt 6, a nie art. 3 pkt 6, ponieważ ta jednostka redakcyjna jest podzielona na ustępy.
- W dotychczasowym art. 15 ust. 6 pozostało sformułowanie „operator usługi kluczowej".

98. Nieuzasadnione zakwalifikowanie uczelni wyższych, instytucji kultury oraz zakładów opieki zdrowotnej jako podmiotów kluczowych

Jednostka redakcyjna: załącznik nr 1
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa nieprawidłowo klasyfikuje wszystkie uczelnie wyższe, państwowe i samorządowe instytucje kultury (np. muzea, teatry) oraz sektor zdrowia (w tym hospicja, zakłady rehabilitacyjne, zakłady pielęgnacyjno-opiekuńcze) jako podmioty kluczowe. Taka regulacja jest całkowicie nieproporcjonalna i nieadekwatna do rzeczywistych potrzeb oraz specyfiki działalności tych jednostek. Oznacza to, że jednostki, których główna działalność w żaden sposób nie wpływa na bezpieczeństwo krytycznej infrastruktury państwa, będą zobowiązane do spełnienia wymogów, które są zbędne, kosztowne i nie przyczyniają się do podniesienia poziomu cyberbezpieczeństwa kraju. Takie podejście może być przykładem nieefektywnego prawa, które zamiast zabezpieczać, generuje nadmierne obowiązki

99. Nierównomierność w rozdzielaniu wsparcia finansowego pomiędzy administracją centralną a jednostkami samorządu terytorialnego

Jednostka redakcyjna: OSR
Jednostka redakcyjna NIS2: nie dotyczy

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwaga: W kontekście przydzielania wsparcia finansowego dla administracji centralnej i rządowej oraz samorządów, analiza Oceny Skutków Regulacji (załącznik do ustawy KSC) ujawnia znaczącą dysproporcję. Planuje się udzielenie wsparcia w wysokości około 700,5 mln zł dla około 70 podmiotów administracji centralnej i rządowej, co przekłada się na średnio 10 mln zł na każdą z tych jednostek. Tymczasem dla 2500 samorządów przeznaczono 1,5 mld zł, co oznacza średnio jedynie około 600 tys. zł na jednostkę samorządową.

Tak duża dysproporcja w rozdzielaniu środków, gdzie samorządy otrzymują znacznie mniej środków na jednostkę, może prowadzić do nierówności w możliwościach wdrażania niezbędnych działań związanych z cyberbezpieczeństwem. Co więcej, środki przeznaczone dla samorządów pochodzą z Europejskiego Funduszu Rozwoju Regionalnego (FERC), co oznacza, że ich wykorzystanie wiąże się z dodatkowymi rygorami dofinansowania europejskiego, które są zwykle bardziej skomplikowane i czasochłonne w administracji niż bezpośrednie środki budżetowe dostępne dla administracji centralnej.

Taka różnica w finansowaniu nie tylko wprowadza nierówności, ale także może skutkować różnicami w poziomie zabezpieczeń cybernetycznych między różnymi poziomami administracji. W kontekście równości i sprawiedliwości w dostępie do publicznych zasobów, zasadne byłoby ponowne przemyślenie i potencjalne zrównoważenie wsparcia finansowego, tak aby wszystkie jednostki administracyjne miały równą szansę na wzmocnienie swojego cyberbezpieczeństwa.

100. Brak wdrożenia Rozporządzenia PE i Rady (UE) 2019/881

Jednostka redakcyjna: nie dotyczy
Jednostka redakcyjna NIS2: nie dotyczy

Uwaga: Ustawa KSC pomimo odniesień do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. dotyczącego ENISA (Europejskiej Agencji ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w obszarze technologii informacyjno-komunikacyjnych, nie zawiera konkretnych rozwiązań ani procedur wdrażających wspomniane przepisy. Brak jest jasnych wskazań dotyczących sposobu implementacji wymogów rozporządzenia, co stawia pod znakiem zapytania skuteczność przyszłych działań w zakresie zwiększenia cyberbezpieczeństwa na poziomie krajowym. Poprzednie konsultacje projektów ustawy podkreślały potrzebę wdrożenia rozporządzenia 2019/881, a nie dyrektywy NIS2, co czyni tę zaniechaną implementację szczególnie problematyczną.

101. Brak przeprowadzenia Oceny Skutków Regulacji (OSR)

Jednostka redakcyjna: OSR
Jednostka redakcyjna NIS2: nie dotyczy

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwaga: Nie dokonano analizy skutków nowych przepisów i zaniechano zapewnienia zasobów: Zgodnie z § 28 Regulaminu Prac Rady Ministrów odrębną część uzasadnienia projektu aktu normatywnego stanowi ocena skutków regulacji, która przedstawia wyniki oceny przewidywanych skutków społeczno-gospodarczych, a w szczególności przedstawienie wyników analizy wpływu projektowanego aktu normatywnego na podmioty, w tym na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego, rynek pracy, konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, a zwłaszcza mikroprzedsiębiorców, małych i średnich przedsiębiorców. W tym zakresie jednak projektodawca zaniechał przeprowadzenia głębszej analizy:

1. Brak estymacji kosztów przeprowadzenia obowiązkowych cyklicznych audytów bezpieczeństwa - OSR nie zawiera estymacji kosztów związanych z obowiązkiem przeprowadzania cyklicznych audytów bezpieczeństwa. Dokument nie oferuje analizy finansowej ani wpływu tych kosztów na mniejsze podmioty, które mogą być szczególnie obciążone tym wymogiem, a także na jednostki samorządu terytorialnego (str. 10-16 OSR).

2. Brak estymacji kosztów wdrożenia obowiązków przez podmioty kluczowe i ważne, w szczególności podmioty nieobjęte dotychczas ustawą o krajowym systemie cyberbezpieczeństwa, ani równoważnymi obowiązkami. OSR nie przedstawia szczegółowej analizy kosztów dla nowych podmiotów kluczowych i ważnych, które będą musiały dostosować swoje operacje do wymogów ustawy. Brak takiej analizy może prowadzić do nieprzewidzianych obciążeń finansowych dla tych podmiotów (str. 27-30 OSR).

3. Brak choćby próby estymacji wpływu wydania decyzji o uznaniu dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka. W OSR brakuje oszacowania wpływu decyzji o klasyfikacji dostawców jako dostawców wysokiego ryzyka na operacje podmiotów kluczowych i ważnych. Takie decyzje mogą prowadzić do konieczności wymiany infrastruktury IT, co generuje znaczące koszty, szczególnie dla mniejszych firm (str. 29 OSR).

4. Brak oceny, jak długo w praktyce przedsiębiorcy rzeczywiście wykorzystują sprzęt/oprogramowanie danego typu, przyjęcie za punkt odniesienia do obowiązku usuwania sprzętu jego „żywotności". OSR nie zawiera analizy dotyczącej realnego okresu użytkowania sprzętu i oprogramowania przez podmioty. Brak takiej analizy może skutkować ustanowieniem niewykonalnych wymagań dotyczących czasu na

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

wymianę sprzętu w sytuacji klasyfikacji dostawcy jako dostawcy wysokiego ryzyka (str. 29 OSR).

102. Wydłużenie vacatio legis

Dodaje się art. 27a w brzmieniu:

> *„Podmioty, które nie zostały wpisane do wykazu operatorów usług kluczowych, o którym mowa w art. 7 ustawy zmienianej, na podstawie decyzji o uznaniu za operatora usługi kluczowej, o której mowa w art. 5 ust. 2 ustawy zmienianej - realizują obowiązki, o których mowa w rozdziale 3 w brzmieniu nadanym niniejszą ustawą, w terminie 12 miesięcy od dnia dokonania wpisu do wykazu, o którym mowa w art. 7 ust. 1., w brzmieniu nadanym niniejszą ustawą"*

Proponowana nowelizacja Ustawy obejmie nowe podmioty wskazane w załączniku nr 1 i nr 2 (np. producentów leków), które będą zobowiązane realizować obowiązki wynikające zarówno z obecnie obowiązującej ustawy jak i z treści projektu. Mając na uwadze stopień ich skomplikowania oraz wysokie koszty wdrożenia – proponujemy wskazanie terminu 12 miesięcy dla podmiotów, które nie zostały wpisane do wykazu operatorów usług kluczowych w rozumieniu w art. 7 ustawy zmienianej.

103. Termin wejścia w życie nowelizowanej ustawy – doprecyzowanie terminu wejścia w życie ustawy

Mając na uwadze wątpliwości związane z kręgiem podmiotów zobowiązanych do stosowania przepisów nowelizowanej ustawy KSC, które wynikają zarówno z definicji proponowanych w treści nowelizowanej ustawy jak i z definicji przedsiębiorcy telekomunikacyjnego, znajdujących się procedowanej równolegle projekcie ustawy PKE, niezbędnym wydaje się prawidłowe określenie procesu legislacyjnego dla obu procesowanych aktualnie ustaw. Z uwagi na odwołania w treści nowelizowanej ustawy KSC do definicji zawartych w procesowanym PKE niezbędne wydaje się w pierwszej kolejności uchwalenie nowego PKE a dopiero w konsekwencji przepisów KSC, które w swojej treści odwołują się do definicji zawartych w PKE.

104. Brak udziału ministra ds. informatyzacji w ramach prac Rządowego Zespołu Zarządzania Kryzysowego

Jednostka redakcyjna: nie dotyczy
Jednostka redakcyjna NIS2: art. 9

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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

Uwaga: Umocowanie ministra właściwego do spraw informatyzacji (Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa) jako organu wiodącego w zakresie cyberbezpieczeństwa nie znajduje odzwierciedlenia we włączeniu tego organu do działalności Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ustawy o zarządzaniu kryzysowym. Minister do spraw informatyzacji może być jedynie doproszony do tego gremium na podstawie art. 8 ust. 3 ustawy o zarządzaniu kryzysowym. Z uwagi na znaczenie ministra właściwego do spraw informatyzacji, zasadne byłoby wprowadzenie odpowiedniej zmiany w tej jednostce redakcyjnej ustawy o zarządzaniu kryzysowym w celu zapewnienia spójności i koordynacji reagowania organów administracji publicznej w obliczu sytuacji kryzysowych.

KL/295/80/AM/2024

Konfederacja Lewiatan
ul. Zbyszka Cybulskiego 3
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