Stanowisko Polskiej Izby Informatyki i Telekomunikacji w sprawie projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw

Polska Izba Informatyki i Telekomunikacji (PIIT), platforma działająca na rzecz cyfrowej transformacji gospodarki i modernizacji państwa, od ponad 30 lat współtworząca fundamenty cyfrowego rozwoju, reprezentująca ok. 130 kluczowych firm przemysłu teleinformatycznego (w tym: operatorów stacjonarnych i mobilnych i firmy telekomunikacyjne, producentów sprzętu, producentów i integratorów oprogramowania, dystrybutorów treści audiowizualnych, platformy cyfrowe oraz wiele firm z sektora MŚP, będących silnymi graczami na polskim rynku), przedstawia opinię w sprawie projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa (dalej „ksc", „uksc").

PIIT z zadowoleniem przyjmuje zamiar polskiego rządu implementacji Dyrektywy NIS2 i unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G do końca tego roku. Podejście rządowe zapewni harmonizację przepisów i stabilność prawną. W kontekście drugiego sprawozdania [1]z postępu prac 5G Toolbox: „państwa członkowskie powinny niezwłocznie wdrożyć wskazany zestaw narzędzi". Przyjęcie ustawy nie powinno być dalej opóźniane. Jakiekolwiek dalsze opóźnienia mogą zagrozić zgodności z harmonogramami UE, zagrażać harmonizacji i ryzykować stabilność prawną dla sektora. Przedstawione stanowisko PIIT nie jest jednomyślne. Firmy Ericsson, Nokia i Samsung zgłosiły zdanie odrębne w punktach dotyczących dostawców wysokiego ryzyka.

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. 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 konsultacyjne**. Niestety bowiem wielokrotnie byliśmy zaskakiwani wprowadzaniem do projektu całych nowych rozdziałów, które nie były przedmiotem

[1] https://ec.europa.eu/commission/presscorner/detail/pl/ip_23_3309

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)?

Co więcej projekt ustawy wdrażającej DORA, która w części zmienia również ustawę o ksc w chwili obecnej ze względu na brak koordynacji w wielu miejscach koliduje z projektem nowelizacji ksc, a nawet wzajemnie się wykluczają.

Ponadto celem uzyskania pełnego obrazu wdrożenia wzajemnie przenikających się przepisów zasadne byłoby znać zależności pomiędzy konsultowaną nowelizacją ustawy a zapowiadaną ustawą implementującą Dyrektywę CER, która ma nakładać obowiązki na podmioty krytyczne.

Wreszcie należy wskazać, że zgodnie z definicją podmiotów kluczowych i ważnych (art. 5 ust. 1 i 2 ksc), zakresem regulacji będą objęte nie tylko co najmniej średnie przedsiębiorstwa, ale także mikro i małe przedsiębiorstwa. Przedsiębiorstwa te będą obciążone dużymi kosztami wdrożenia ksc. Koszty te nie zostały ocenione w Ocenie Skutków Regulacji („OSR"), w szczególności pod kątem zasady proporcjonalności. Oceny skutków finansowych regulacji dla mikro, małych i średnich przedsiębiorców wymaga także art. 66 ust 1 pkt 2 oraz ust. 2 Prawa przedsiębiorców.

Uwagi szczegółowe:

1. <u>Art. art. 1 ust. 8</u>

   Nowelizacja w art. 1 ust. 8 projektu (art. 5 uksc) znacząco rozszerza zakres podmiotowy dotychczasowej regulacji, nakładając nowe obowiązki na wiele podmiotów, które dotychczas jej nie podlegały np. podmioty z sektorów infrastruktury cyfrowej, zarządzania usługami ICT, a także usług cyfrowych. Wskazania te nie przewidują żadnych wyłączeń dla przypadków świadczenia tych usług przez jedną ze spółek z grupy kapitałowej wyłącznie na rzecz innych spółek z tej samej grupy. Jednocześnie taki sposób organizacji działalności IT w polskich grupach kapitałowych jest powszechny i sprzyja ich profesjonalizacji oraz jakości - pozwala to na utrzymanie wysokiego poziomu kwalifikacji specjalistów zatrudnianych przez jeden podmiot z grupy, specjalizujących się w zarządzaniu poszczególnymi systemami ICT, w tym cyberbezpieczeństwem.

   Objęcie podmiotów świadczących usługi ICT i cyberbezpieczeństwa wyłącznie na rzecz swoich grup kapitałowych jest sprzeczne z celem regulacji i może spowodować znaczące pogorszenie poziomu cyberbezpieczeństwa polskich przedsiębiorstw. Wysokie koszty dostosowania do wymogów

regulacyjnych, będą zachęcały przedsiębiorców do likwidacji wewnętrznych usług ICT poprzez likwidację centrów kompetencyjnych i przenoszenie zadań związanych z zarządzaniem systemami ICT i cyberbezpieczeństwa do każdego z podmiotów w grupie kapitałowej. Spowoduje, to że zamiast wysoko kompetentnych fachowców specjalizujących się w poszczególnych obszarach cyberbezpieczeństwa i ICT, będą zatrudniani niewyspecjalizowani pracownicy, których zakres zadań będzie nadmiernie szeroki, a zagadnienia dot. cyberbezpieczeństwa będą tylko jednym z wielu ich obowiązków.

W związku z tym, w naszej opinii, wszystkie definicje dodawane w projektowanym art. 2, dotyczące dostawców usług (od pkt 4b do pkt 4i) powinny zostać zmodyfikowane w taki sposób, żeby odnosiły się tylko do podmiotów, które świadczą wskazane usługi w sposób publicznie dostępny. Ewentualnie powinno zostać dodane 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.

Podobny problem dotyczy wskazania jako podmiotów kluczowych przedsiębiorców telekomunikacyjnych oraz podmiot świadczących usługi komunikacji interpersonalnej niewykorzystujące numerów. Przy zaproponowanych szerokich definicjach przedsiębiorcy komunikacji elektronicznej oraz przedsiębiorcy telekomunikacyjnego polska ustawa implementująca wychodzi 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. Tutaj również współpraca w ramach Grupy powoduje, że zgodnie z definicją europejską, nawet jeżeli jedno z przedsiębiorstw osiąga status średniego przedsiębiorcy, wpływa on na pozostałe podmioty. Tym samym nawet jeżeli działalność telekomunikacyjna niektórych podmiotów grupie jest marginalna – muszą one wdrożyć stosowne obowiązki. Aby zapewnić zgodność z wprowadzaną dyrektywą należy w szczególności zmodyfikować zaproponowaną definicję przedsiębiorcy telekomunikacyjnego w ten sposób, że powinna ona oznaczać jedynie przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, który świadczy publicznie dostępne usługi telekomunikacyjne. Dodatkowo, postulujemy, aby wielkość przedsiębiorstwa określać na podstawie jego przychodów bezpośrednio z działalności telekomunikacyjnej a nie całości przez nie generowanych.

2. Art. 2 – definicje

W celu zwiększenia komunikatywności ustawy postulujemy sformułowanie definicji użytych w niej pojęć, w taki sposób, by nie ograniczały się one do odsyłania czytelnika do konkretnych jednostek redakcyjnych w aktach unijnych, w których zawarte są inne definicje. O ile jest możliwe dokonanie tego w sposób nieprowadzący do zniekształcenia znaczenia poszczególnych pojęć, proponujemy powtórzenie definicji unijnych w ustawie. Za niepożądane należy uznać zmuszanie adresatów norm ustawowych do odtwarzania ich treści poprzez odwoływanie się do innych aktów prawnych. Jednocześnie proponujemy przemyślenie zastąpienia terminu „ICT" bardziej poprawnym terminem „teleinformatyka" (i konsekwentnie „procesu ICT" - „procesem teleinformatycznym", „produktu ICT" - „produktem teleinformatycznym" itd.).

3. 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,* ***przy danym poziomie zaufania****, 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.

4. Art. 2 punkt 8a - organ zarządzający

Dyrektywa NIS2 nie definiuje terminu „organu zarządzającego", a jedynie wykorzystuje go w ramach trzech odniesień, które dotyczą wymagań w zakresie zarządzania. Tymczasem w projekcie przedstawionym przez Ministerstwo Cyfryzacji (art. 2 pkt 8a) określenie „organ zarządzający" zostało zastąpione terminem „kierownik jednostki" z bezpośrednim odwołaniem interpretacyjnym do art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598), co sprawia, że przepisy interpretacji mają swoje zastosowanie nie tylko wobec członków zarządu danego podmiotu, ale także osób odpowiedzialnych (w danym momencie) za zarządzanie tym podmiotem. Wydaje się, że nie było to intencją twórców Dyrektywy.

5. Art. 2 pkt 11e - potencjalne zdarzenie dla cyberbezpieczeństwa

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*;".

6. Art. 2 pkt 12 - definicja ryzyka

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;

7. Art. 2 pkt 14 – system informacyjny

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.

8. Art. 3a – uprawnienia podmiotu krajowego systemu cyberbezpieczeństwa.

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

Poza powyższym, zauważamy, że wraz z uchyleniem rozdz. VIIA ustawy Prawo telekomunikacyjne 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.

9. Art. 5 – zakres stosowania określany wg GBER

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.

10. Art. 5 ust. 1 pkt 3 lit. b – dostawca usług zarządzanych w zakresie cyberbezpieczeństwa

    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.

11. Art. 7 – wykaz podmiotów kluczowych i ważnych

    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).

12. Art. 7 ust. 6 – wpis do wykazu w przypadku przedsiębiorców telekomunikacyjnych, dostawców zaufania

    Doprecyzowania lub wyjaśnienia wymaga forma oraz zakres danych, który ma być złożony we wniosku o wpis do wykazu przez przedsiębiorcę telekomunikacyjnego oraz inne podmioty wskazane w zmienianym art. 7 ust. 6. Zgodnie z brzmieniem projektowanego art. 7 ust. 6 zgodnie, z którym dane wskazane w art. 7 ust. 1 uzupełniane są przez ministra ds. informatyzacji na podstawie danych zawartych w rejestrach publicznych, lub przekazanych przez właściwe organy nadzorcze, jednocześnie zgodnie z art. 7 ust. 7 podmioty te uzupełniają dane w wykazie składając wniosek o zmianę wpisu w wykazie, pojawia się zatem wątpliwość, jakie dane powinny być wskazane przez przedsiębiorców telekomunikacyjnych we wniosku o wpis lub ewentualnie w wniosku o zmianę wpisu oraz jaki jest termin na dokonanie zmiany danych wpisanych przez ministra do spraw informatyzacji przez m.in. przedsiębiorców telekomunikacyjnych.

13. Art. 7 ust. 16 – wpis z urzędu

    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 projektowanego art. 7a, który również mówi o wpisie do wykazu przez organ właściwy podmiotu. Wątpliwości i niejasności budzi treść tego postanowienia w świetle postanowień ust. 6.

14. Art. 8.1 i mapowanie na Art 21.2.a-j Dyrektywy NIS2

    Zwracamy uwagę, że aktualny projekt wprowadza niepotrzebną komplikację mapowania 10 środków zarządzania ryzykiem pogrupowaną w Art. 21.2.a-j Dyrektywy NIS2. Proponowana wersja spowoduje komplikację w mapowaniu dla przedsiębiorstw wielonarodowych, gdzie zachodzi konieczność porównania statusu w poszczególnych domenach. Np. w niemieckim projekcie ustawy NIS2

transpozycje Art 21.2. Dyrektywy zachowano w relacji 1 do 1 (por. paragraf 30 niemieckiego projektu transpozycji dyrektywy[2]).

Proponujemy ujednolicenie zgodnie z Art. 21.2. Dyrektywy NIS2 poniższych praktyk, gdyż umożliwiają one zmapowanie na dobre praktyki i normy ISO. Aktualnie poprzestawiane są fragmenty Art 8.1.2 z porządkiem w Dyrektywie NIS2 oraz znajdują się w tych środkach wymagania nadmiarowe (np. „polityki tematyczne") lub występują pominięcia (albo odrębne potraktowanie bezpieczeństwa zasobów ludzkich).

Trudność i niejednoznaczność mapowania przedstawia poniższa tabela. Elementy pogrubione w lewej kolumnie tabeli nie występują w projekcie uksc.

Środki zarządzania ryzykiem (Art. 21.2 a-j Dyrektywy NIS2	**Środki zaproponowane w opiniowanym projekcie uksc**
a) polityka analizy ryzyka i bezpieczeństwa systemów informatycznych	Art. 8.1.2)a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne, Polityki tematyczne są nadmiarowe (por uwaga nr 15 dot. Polityk tematycznych)
b) obsługa incydentu	Art. 8.1.4) zarządzanie incydentami;
c) ciągłość działania, np. **zarządzanie kopiami zapasowymi** i przywracanie normalnego działania po wystąpieniu **sytuacji nadzwyczajnej, i zarządzanie kryzysowe**	Art. 8.1.2) b) utrzymanie i bezpieczną eksploatację systemu informacyjnego, punkt ten pasuje i do ciągłości działania i do punktu 21.2e) z kolumny obok. Brakuje jasnego wskazania na zarządzanie kopiami zapasowymi co w kontekście zagrożeń ransoware jest kluczowe (back-up/kopia bezpieczeństwa off-line nie zainfekowana). Ponadto zidentyfikowano pominięcie wymagań dot. Zarządzania kryzysowego na poziomie podmiotów kluczowych i ważnych. Nieuzasadnione wydaje się zawężenie wdrożenia praktyk zarządzania kryzysowego do podmiotów z branży energetycznej (por. Art. 8b. Podmioty kluczowe z podsektora energii elektrycznej). Jako obowiązująca norma w tym zakresie może być zastosowana ISO/IEC 22361. Art. 8.1.2) e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie, Proponujemy ujednolicenie zgodnie z Dyrektywą NIS2 oraz doprecyzowanie „sytuacji nadzwyczajnej" wg Dyrektywy NIS2) lub katastrofy (wg niniejszego projektu uksc).

[2] https://ag.kritis.info/wp-content/uploads/2024/03/CI1_17002_41_22-86-32-NIS2UmsuCG-2.-RefE-22-12-2023-09-58h.docx

d) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami	Art. 8.1.2) d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
e) bezpieczeństwo w procesie nabywania, rozwoju i utrzymania sieci i systemów informatycznych, w tym postępowanie w przypadku podatności i ich ujawnianie	Art. 8.1.2) b) utrzymanie i bezpieczną eksploatację systemu informacyjnego – punkt ten pasuje również do ciągłości działania – por. Pkt c z kolumny obok. Art. 8.1.2) f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym, Art. 8.1.3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi; Art. 8.1.5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym, b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji, c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń;
f) polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie	Art. 8.1.2) g) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
g) podstawowe praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa	Art. 8.1.2) h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny,
h) polityki i procedury stosowania kryptografii i, w stosownych przypadkach, szyfrowania	Art. 8.1.2) i) polityki i procedury stosowania kryptografii, w tym szyfrowania;
i) **bezpieczeństwo zasobów ludzkich**, polityka kontroli dostępu **i zarządzanie aktywami**	Art. 8.1.2) c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, Brakuje w projekcie bezpieczeństwa zasobów ludzkich (jest to częściowo zaadresowane w artkule 8f1 i2, ale nie wyczerpuje tematu (Background checks to również sprawdzenie osób w kontekście powiazań kapitałowych, prania brudnych pieniędzy, list terrorystycznych, oraz przeszłości zatrudnienia, itp.). Ponadto brakuje

	kluczowego dla bezpieczeństwa obszaru zarządzania aktywami – dlatego jeszcze raz wnioskujemy o proponujemy ujednolicenie punktów Art 8.1. UKSC z Art. 21.2. a-j) Dyrektywy.
j) stosowanie uwierzytelniania wieloskładnikowego lub ciągłego, zabezpieczonych połączeń głosowych, tekstowych i wideo oraz zabezpieczonych systemów łączności wewnątrz podmiotu w sytuacjach nadzwyczajnych	Art. 8.1.6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, Art. 8.1.6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe.

Brakuje ponadto wskazania norm ISO/IEC 30111:2019 oraz ISO/IEC 29147:2018 w zakresie zarządzania podatnościami i ujawniania podatności, które zostały wskazane w Dyrektywie NIS2 motyw (58). Normy te jasno pokazują sposób realizacji zarzadzania podatnościami, co jest kluczowe dla ujednolicenia dobrych praktyk w tym zakresie i zagwarantowania jasności zakresu wymagań w tym zakresie.

Podobnie brakuje wskazania odniesień do normy ISO/IEC 17788:2014 wskazanej w Motywie (33) Dyrektywy NIS2 (obecnie jest wspomniana norma zastąpiona przez normę ISO/IEC 22123-1/2:2023) w zakresie stosowanych pojęć z obszaru Chmury Obliczeniowej (przy okazji prac nad uksc należy uspójnić Komunikat Chmurowy UKNF, również w kontekście rozporządzenia DORA i uspójnić zalecenia z Ministerstwem Finansów koordynującym wdrożenie DORA).

15. Art. 8 pkt 2 lit a – polityki tematyczne

    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.

16. Art. 8 pkt 2 lit. d – łańcuch dostaw

    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*

17. Art. 8 pkt 2 lit e – katastrofa

    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 lub wskazanie odpowiedniego odwołania do istniejących definicji, co może być jednak problematyczne. Możliwe jest też jego zastąpienie zwrotem *„po przerwaniu ciągłości jego działania*” lub powiązania konieczności odtworzenia systemy informacyjnego po wystąpieniu incydentu poważnego, krytycznego lub cyberzagrożenia na dużą skalę.

Z uwagi na potencjalne kary pieniężne konieczne jest zachowanie maksymalnej precyzji pojęć używanych do opisu wymagań.

18. Art. 8 ust. 2

Wnioskujemy o uwzględnienie w tym przepisie wymagań wskazanych w normie ISO/IEC 27001 oraz ISO/IEC 22301. Niektóre podmioty mogą posiadać certyfikaty na zgodność z angielskojęzyczną wersją przywołanych norm - wskazanie wersji polskojęzycznej w przepisie nie powinno dyskwalifikować tych certyfikatów, ponieważ ich treść, a tym samym wymogi pozostają niezmienne w obu wersjach językowych.

19. Art. 8 ust. 3 – mapowanie PN

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 oraz że zadanie to powinno być obowiązkiem ministra ds. informatyzacji a nie możliwością.

20. Art. 8 ust. 4 – dostawca

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 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 zostaną wydane.***

Wydanie skoordynowanych ocen jest fakultatywne.

Ponadto definicja dostawcy sprzętu lub oprogramowania obejmuje także importera lub dystrybutora – co obejmuje w konsekwencji bardzo szeroki zakres analiz w przedsiębiorstwie co do podmiotów współpracujących, pod kątem spełniania przez nich wymogów bezpieczeństwa informacji, a w przypadku uznania za HRV także dystrybutora - może to zablokować lub znacząco utrudnić działalność podmiotu kluczowego.

21. Art. 8a – uszczegółowienie wymagań

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 to możliwość rozpoczęcia przygotowań zorientowanych na osiągnięcie oczekiwanych regulacyjnie efektów.

22. Art. 8b – spółki obrotu

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 rozdz. 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.

23. Art. 8d pkt 4 – zakres szkoleń personelu

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

24. Art. 8f ust. 1 – brak karalności

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 dotyczące potwierdzenia niekaralności powinny zostać ograniczone do zakresu kluczowego personelu definiowanego przez pracodawcę.

25. Art. 8h – wymiana informacji

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 (…)*".

W obecnym brzmieniu projektu zmian w ksc wymiana informacji de facto jest obowiązkiem, podczas gdy zgodnie z art. 29 NIS2 wymiana ta ma się odbywać na zasadzie dobrowolności, tym bardziej, że jest to obowiązek penalizowany. Obowiązkiem powinna być objęta tylko wymiana informacji z CSIRT, jak w NIS 2.

26. Art. 9 ust. 1 pkt 1) – osoby kontaktowe

Projekt ustawy przewiduje zmianę w art. 9 ust. 1 pkt 1) ustawy o krajowym systemie cyberbezpieczeństwa, tak, aby obowiązkiem podmiotów kluczowych i ważnych było wyznaczanie dwóch osób odpowiedzialnych za utrzymywanie kontaktów z innymi podmiotami kluczowymi

i ważnymi. W naszej ocenie wymóg wskazywania konkretnych dwóch osób nie jest optymalnym rozwiązaniem i powinien zostać zastąpiony wymogiem określenia i wskazania sposobu i kanału kontaktu, który może być wykorzystywany do kontaktowania się z podmiotem w sprawach związanych z wykonywaniem ustawy i cyberbezpieczeństwem. Czyli zamiast wymogu wyznaczania dwóch osób wymóg wyznaczenia adresu e-mail i numeru telefonu, które będą służyły do kontaktu.

Biorąc pod uwagę, że podmiotów kluczowych i ważnych w nowym systemie cyberbezpieczeństwa będą tysiące nie ma najmniejszych szans na ustanowienie relacji personalnych pomiędzy tymi podmiotami, relacji, które uzasadniałyby konieczność określenia konkretnych osób jako kontaktowych. A jednocześnie wskazywanie punktów kontaktowych z imienia i nazwiska, wobec dużej rotacji na rynku pracy, będzie skutkowało zarówno po stronie administracji jak i po stronie podmiotów kluczowych i ważnych wymogiem ciągłej aktualizacji danych osób kontaktowych.

Lepszym rozwiązaniem byłaby możliwość wskazania adresu e-mail i numeru telefonu do kontaktu (albo innych powszechnie wykorzystywanych kanałów komunikacji), przy zapewnieniu, że adres ten i numer telefonu będą obsługiwane przez osobę albo zespół osób, których zadaniem w danym czasie jest obsługiwanie spraw związanych z cyberbezpieczeństwem.

27. Art. 9 – termin rozpoczęcia korzystania z S46

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.

28. Art. 10 – dokumentacja

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

Dodatkowe zastrzeżenia budzą:

- Art. 10 ust. 3 pkt 5 - co gdy zostaną wydane rekomendacje z art. 8a? Co ma zrobić podmiot kluczowy z posiadaną dokumentacją?
- Art. 10 ust. 5 pkt 2 - integralność to właśnie ochrona przed jakąkolwiek modyfikacją

Ponadto za nieuzasadniony i uciążliwy, a zatem zbędny, należy uznać wymóg protokolarnego niszczenia dokumentacji bezpieczeństwa systemu informacyjnego. Projektowany art. 10 ust. 7 ustawy stanowi, że zniszczenie wycofanej z użytkowania dokumentacji potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji mają być przechowywane w sposób trwały.

W przypadku dużych organizacji, korzystających z licznych systemów informacyjnych, spełnienie tego wymogu – nawet przy spełnieniu wszystkich innych wymogów związanych z nadzorem nad tymi dokumentami – będzie zadaniem uciążliwym, czasochłonnym, a zatem kosztownym. Dokumentacja taka może być bowiem przechowywana w kilku różnych egzemplarzach, w różnych zasobach, co oznacza, że wymóg protokolarnego niszczenia dokumentów pośrednio oznacza wymóg ciągłego inwentaryzowania wszystkich egzemplarzy i kopii tych dokumentów. Z drugiej strony, jeśli dokumentacja jest odpowiednio chroniona, to nie jest konieczne jej niszczenie, a tym bardziej nieszczelnie protokolarne. I nie sposób pominąć wymogu bezterminowego (czyli po wsze czasy) przechowywania protokołów. Prosimy o usunięcie w całości ust. 7 z art. 10 ustawy.

Zwracamy również uwagę na potrzebę weryfikacji prawidłowości zapisów w ust. 6 w art. 10 ustawy (w brzmieniu nadawanym projektowaną ustawą), który to przepis wyznacza termin (i określa sposób liczenia tego terminu) przechowywania dokumentacji systemu informacyjnego wykorzystywanego do świadczenia usługi, która została wycofana. Przepis ten stanowi, że momentem początkowym, od którego należy liczyć dwuletni termin jest 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Nie wiadomo jak rozumieć ten przepis, bo literalnie rzecz ujmując przepis wymaga, aby początek terminu przechowywania dokumentacji liczyć od momentu wygaśnięcia okresu przechowywania.

29. Art. 11

Słowo „użytkownicy" może wprowadzać w błąd. Dlatego też, aby poprawić przejrzystość i zharmonizowane podejście w całej UE, sugerujemy użycie sformułowań określonych w dyrektywie NIS 2 (UE) 2022/2555 https://eur-lex.europa.eu/eli/dir/2022/2555

Dyrektywa NIS2, Artykuł 23 - Obowiązki w zakresie zgłaszania incydentów"

„W stosownych przypadkach dane podmioty bez zbędnej zwłoki powiadamiają odbiorców swoich usług o poważnych incydentach, które mogą mieć niekorzystny wpływ na świadczenie tych usług."

Jeśli chodzi o zgłaszanie incydentów, jeżeli znaczący incydent obejmuje całą UE, prawo powinno zapewniać, że taki znaczący incydent powinien być zgłaszany do jednego zespołu CSIRT: zespołu CSIRT państwa członkowskiego, w którym znajduje się siedziba ważnego podmiotu, lub unijnego zespołu CSIRT.

30. Art. 11 ust. 1a – zbyt krótki termin zgłoszeń incydentów dla przedsiębiorców telekomunikacyjnych

Wnioskujemy o wykreślenie art. 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.

31. Art. 11 ust. 4 – progi incydentu poważnego

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.*

W przypadku wydania w tym samym zakresie przepisów krajowych może wystąpić kolizja norm.

32. Art. 12 ust. 1 pkt 5 – wczesne ostrzeżenie

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.

33. Art. 12 ust. 3 pkt 1 lit. f w zw. z ust. 2

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*

34. Art. 15 ust. 1b

W zakresie decyzji dot. nakazu przeprowadzenia audytu należy doprecyzować w jakim trybie będzie wydawana decyzja. Koniecznym jest uzupełnienie przepisu o minimalny okres od dnia wydania decyzji na uruchomienie audytu, żeby organ nie wydał decyzji w poniedziałek z obowiązkiem przedstawienia sprawozdania w piątek.

35. Art. 16

Z uwagi na objęcie przepisami bardzo szerokiego katalogu podmiotów, także niebędących dotychczas podmiotami krajowego systemu cyberbezpieczeństwa postulujemy wydłużenie terminów na implementację do 18 miesięcy na wdrożenie obowiązków oraz 24 miesiące na przeprowadzenie pierwszego audytu.

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. Należy zaznaczyć, że obecne brzmienie projektowanego przepisu może spowodować, że okres audytu będzie dotyczyć okresu w którym podmiot nie miał obowiązku realizacji obowiązków w zakresie cyberbezpieczeństwa jako podmiot kluczowy lub ważny.

36. Art. 16a - abonent nazwy domeny

Projekt ustawy przewiduje dodanie do ustawy o krajowym systemie cyberbezpieczeństwa szeregu przepisów z nowymi wymogami dla rejestrów nazw domen najwyższego poziomu (TLD) i podmiotów świadczących usługi rejestracji nazw domen (nowy art. 16a i następne). Nowo dodawane przepisy w kilku miejscach posługują się pojęciem „abonenta nazwy domeny", nie definiując tego pojęcia. Brak definicji wynika zapewne z tego, że Projektodawca uznał, że jest to pojęcie występujące w obrocie gospodarczym, zrozumiałe i z tego względu nie wymagające definiowania i takie podejście jest poniekąd zrozumiałe.

Niemniej jednak zwracamy uwagę na potencjalny problem związany z tym, że projektowana ustawa zmienia ustawę o krajowym systemie cyberbezpieczeństwa m.in. w taki sposób, że elementem systemu stają się przedsiębiorcy telekomunikacyjni (przedsiębiorcy komunikacji elektronicznej), w tym dostawcy publicznie dostępnych usług telekomunikacyjnych, których klientami są „abonenci" w rozumieniu ustawy – Prawo telekomunikacyjne (a w przyszłości ustawy – Prawo komunikacji elektronicznej).

Brak w ustawie o krajowym systemie cyberbezpieczeństwa definicji „abonenta nazwy domeny" może skutkować nieuzasadnionymi próbami stosowania na potrzeby nowego rozdziału 3a UKSC definicji „abonenta" z Prawa telekomunikacyjnego (w przyszłości Prawa komunikacji elektronicznej). I choć ryzyko takich nieuzasadnionych interpretacji nie wydaje się wysokie, to aby je całkowicie wyeliminować warto rozważyć albo wprowadzenie do UKSC definicji „abonenta nazwy domeny", albo posłużenie się w przepisach rozdziału 3a uksc pojęciem innym, niż „abonent" nazwy domeny.

37. Art. 33 – badanie produktów, usług, procesów ICT

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.

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.

38. Art. 36b - ocena bezpieczeństwa systemu informacyjnego

Projektu ustawy zakłada dodanie do ustawy o krajowym systemie cyberbezpieczeństwa nowych przepisów (rozdział 6a, art. 36b i następne) dotyczących oceny bezpieczeństwa systemów informacyjnych. W ustawie ma się pojawić m.in. art. 36b ust. 1, który w projekcie ustawy ma następujące brzmienie (podkreślenie własne):

> *Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona:*
>
> > *1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności* ***lub***
> >
> > *2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.*

Zwracamy uwagę na konsekwencje posłużenia się spójnikiem „lub", który w języku prawniczym jest alternatywą. Użycie spójnika „lub" oznacza, że projektowany przepis dopuszcza możliwość przeprowadzanie oceny bezpieczeństwa systemu informacyjnego na zlecenie organu (punkt 2), bez konieczności uzyskania zgody podmiotu, który ma zostać poddany ocenie (punkt 1).

Jeśli obecna redakcja przepisu jest wynikiem błędu, to błąd ten powinien zostać poprawiony. Jeśli jednak obecna redakcja jest zabiegiem celowym, to jako Izba uznajemy za nieakceptowalne i szkodliwe rozwiązanie, które pozwala prowadzić ocenę bezpieczeństwa systemu informacyjnego danego podmiotu bez zgody i wiedzy tego podmiotu. Zgoda podmiotu, wobec którego ma zostać przeprowadzona ocena bezpieczeństwa systemu informacyjnego, musi być warunkiem *sine qua non* przeprowadzania takiej oceny, a podmiot kluczowy i podmiot ważny musi mieć możliwość niewyrażenia zgody na udział w ocenie, bez ponoszenia z tego tytułu negatywnych konsekwencji ze strony organów właściwych do spraw cyberbezpieczeństwa. Prowadzenie takiej oceny bez zgody albo co gorsza bez wiedzy podmiotu, który jest poddawany ocenie, oznaczałoby, że oceniany podmiot prowadzoną ocenę postrzegałby jako wrogi atak i reagowałby zgodnie z procedurami przewidzianymi na okoliczność ataku, włączając w to poinformowanie organów ścigania o podejrzeniu popełnienia albo usiłowania popełnienia przestępstwa. Oczywiście zrozumiałe jest, że nie wszyscy pracownicy podmiotu poddawanego ocenie muszą i powinni wiedzieć, że trwa ocena, niemniej jednak osoby decyzyjne w podmiocie kluczowym lub ważnym muszą mieć taką wiedzą i muszą mieć możliwość świadomego podjęcia decyzji, czy chcą, aby kierowana przez nich organizacja brała udział w takim badaniu.

Biorąc powyższe pod uwagę widzimy potrzebę przeredagowania analizowanego przepisu tak, aby jednoznacznie wynikało z niego, że w każdym przypadku zgoda podmiotu kluczowego albo podmiotu ważnego jest warunkiem przeprowadzania oceny bezpieczeństwa systemu informacyjnego takiego podmiotu. Można to osiągnąć albo przez zastąpienie spójnika „lub" spójnikiem „oraz" albo przez nadanie analizowanemu przepisowi następującego brzmienia:

> *Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona na zlecenie organu właściwego do spraw cyberbezpieczeństwa, za uprzednią zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności.*

39. Art. 41 – organy właściwe do spraw cyberbezpieczeństwa

Przyjęta na gruncie ustawy o krajowym systemie cyberbezpieczeństwa logika wyznaczania organów właściwych do spraw cyberbezpieczeństwa wydaje się nie uwzględniać w wystarczającym stopniu realiów rynkowych i faktu, że wiele przedsiębiorstwa prowadzi równolegle działalność w dwóch lub większej ilości sektorów. Logika przyjęta w ustawie powoduje, że wielosektorowe podmioty kluczowe i ważne będą jednocześnie podlegały kontroli i nadzorowi dwóch, trzech albo większej ilości organów właściwych, co jest rozwiązaniem dalekim od optymalnego.

Tytułem przykładu wyobraźmy sobie przedsiębiorcę telekomunikacyjnego, który nie tylko świadczy usługi telekomunikacyjne i dostarcza sieć telekomunikacyjną, ale jednocześnie świadczy usługi DNS i CDN (co jest stosunkowo powszechną praktyką na rynku telekomunikacyjnym), a na dodatek sprzedaje energię elektryczną. Od razu zaznaczmy również, że nie jest to przykład teoretyczny, bowiem istnieją podmioty, które prowadzą działalność w takim właśnie zakresie i nie są to przypadki odosobnione (spadająca rentowność działalności telekomunikacyjnej zmusza przedsiębiorców telekomunikacyjnych do szukania przychodów na innych rynkach). Podmiot taki, jako potencjalny podmiot kluczowy, zgodnie z przepisami ustawy będzie podlegał kontroli i nadzorowi co najmniej trzech organów właściwych:

- Prezesa Urzędu Komunikacji Elektronicznej – jako podmiot kluczowy z podsektora komunikacji elektronicznej;
- ministra właściwego ds. informatyzacji – jako podmiot kluczowy świadczący usługi takie jak DNS czy CDN;
- ministra właściwego ds. energii – jako podmiot kluczowy sprzedający energię elektryczną

W praktyce pojawią się podmioty kluczowe podlegające nawet większej licznie organów. Z powodów oczywistych sytuacja, w której ten sam podmiot ma podlegać dwóm, trzem albo większej ilości organów kontroli i nadzoru nie jest sytuacją optymalną, w szczególności, że każdy z tych organów będzie przecież mógł i chciał egzekwować swoje kompetencje w tym samym obszarze, czyli w obszarze wymogów związanych z cyberbezpieczeństwem. Konflikty, sprzeczności a co najmniej brak spójności są wręcz wpisane w taki model.

Szczególnie kłopotliwy może być fakt, że nawet w sektorze „infrastruktura cyfrowa" pojawią się dwa organy (Prezes UKE dla podsektora komunikacja elektroniczna i Minister Cyfryzacji dla pozostałej części infrastruktury cyfrowej), które będą miały kompetencje kontrolne i nadzorcze wobec bardzo zbliżonych usług i obszarów. Przykładowo usługa dostępu do Internetu to na gruncie UKSC będzie obszarem zainteresowania Prezesa UKE, ale już usługi DNS i CDN (które technicznie są powiązane z usługą dostępu do sieci Internet i transmisją danych) ma być przedmiotem kontroli i nadzoru ze strony Ministra Cyfryzacji. Żeby dopełnić obrazek trzeba też przypomnieć, że Prezes UKE jest organem nadzorowanym przez Ministra Cyfryzacji.

Prosimy Projektodawcę o ponowne przeanalizowanie tego rozwiązania i tam gdzie to możliwe uproszczenie systemu tak, aby wyeliminować albo ograniczyć do minimum przypadki, w których ten sam podmiot kluczowy albo podmiot ważny podlega w zakresie cyberbezpieczeństwa więcej niż jednemu organowi. W szczególności prosimy o uproszczenie systemu dla podmiotów działających w sektorze „infrastruktura cyfrowa", tak, aby dla całego tego sektora był tylko jeden organ właściwy. Organem tym powinien być Prezes UKE, biorąc pod uwagę doświadczenie Urzędu Komunikacji Elektronicznej w sprawowaniu nadzoru nad rynkiem telekomunikacyjnym.

40. Art. 46 ust. 1 pkt 7 – S46 i zgłaszanie naruszeń danych osobowych

Projekt ustawy przewiduje dodanie do art. 46 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa nowego punktu 7, który w połączeniu ze zdaniem wprowadzającym może być

odczytywany w ten sposób, że system S46 ma wspierać m.in. dokonywanie zgłoszeń naruszenia ochrony danych osobowych, o których mowa w art. 33 RODO. Niestety projektowany przepis jest dosyć ogólny i prowokuje szereg pytań, które będą musiały doczekać się odpowiedzi w toku dalszych prac legislacyjnych. Nieznana jest ani kierunkowa intencja Projektodawcy (jaki cel ten przepis ma realizować?) ani to, czy podmioty kluczowe i ważne będą prawnie zobowiązane do zgłaszania Prezesowi Urzędu Ochrony Danych Osobowych naruszeń bezpieczeństwa danych osobowych wyłącznie za pośrednictwem S46 (zastępując tym samym istniejące i działające mechanizmy zgłaszania naruszeń) czy też może S46 ma być narzędziem, z którego podmioty kluczowe i ważne mogą, ale nie muszą korzystać do zgłaszania naruszeń danych osobowych?

Jako Izba prosimy o dialog w tym zakresie, tak aby przyszłe przepisy w tym zakresie uwzględniały doświadczenia wypracowane przez Inspektorów Ochrony Danych Osobowych zdobyte przez lata stosowania przepisów o ochronie danych osobowych. Nie można również zapominać, że przedsiębiorcy telekomunikacyjni znajdują się w tym zakresie w szczególnej sytuacji, bo muszą stosować nie tylko horyzontalne przepisy RODO, ale związani są również przepisami sektorowymi, a konkretnie wciąż obowiązującą dyrektywą 2002/58/WE z dnia 12 lipca 2002 r. *dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej* (dyrektywa e-Privacy) i wydanym na jej podstawie rozporządzeniem Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. *w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej*. Konsekwencją tych przepisów jest art. 174a ustawy – Prawo telekomunikacyjne, który wprost stanowi, że dostawca publicznie dostępnych usług telekomunikacyjnych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu danych osobowych w terminie i na zasadach określonych w rozporządzeniu Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych.

41. Art. 46 ust. 4 – zakres korzystania z S46 przez podmioty kluczowe i ważne

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;*

42. Art. 46 ust. 6 – termin dostosowania do S46

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. Dlatego postulujemy dokonanie konsultacji wymagań przed ich publikacją.

Dodatkowo należy wskazać, że proponowane nowelizacją brzmienie art. 46 ust. 6 – „zapewnienie zgodności systemów informacyjnych" wskazuje na postanowienia znacząco ograniczające swobodę działalności gospodarczej, w ocenie Izby podmioty zobowiązane do podłączenia się do s46 powinny zapewnić kompatybilność swojego systemu z s46. Obecne brzmienie art. 46 ust. 6 oznacza, że to minister ds. informatyzacji będzie decydował o kształcie systemów informatycznych służących do komunikacji w zakresie zadań wynikających z ksc bez możliwości uwzględnienia jakichkolwiek zmian przez podmioty zobowiązane związanych ze specyfiką działalności danego podmiotu.

Z tego względu wnioskujemy o wydłużenie terminu na dostosowanie wskazanego w ustawie do 6 miesięcy, z możliwością ewentualnego wcześniejszego zgłoszenia gotowości. Jednocześnie należy rozważyć wprowadzenie możliwości wskazania przez Ministra dłuższego terminu, w samych wymaganiach.

43. art. 53c

Zgodnie z art. 32 ust. 3 dyrektywy NIS2 właściwe organy wykonując swoje uprawnienia wskazane w art. 32 ust. 2 lit. e), f) g), tj. uprawnienia do wnioskowania o udzielenie informacji, udzielenie dostępu oraz przedstawienie dowodów realizacji polityki cyberbezpieczeństwa, podają cel wniosku i określają informacje, o które wnoszą. Tym samym wymogi określone w art. 53c powinny mieć zastosowanie zarówno do wniosków o udzielenie informacji, wniosków o udzielenie dostępów jak również wniosków o przedstawienie dowodów realizacji polityki bezpieczeństwa. Tym samym wnioskujemy o wskazanie w art. 53c ust. 1, że wymogi tam określone dotyczą również obok żądania przekazania danych, informacji i dokumentów: *żądania uzyskiwania dostępu do danych, dokumentów i informacji koniecznych do wykonania nadzoru* oraz *dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.*

44. Art. 53c ust. 2 pkt 5 – termin przekazania danych, informacji i dokumentów

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.

45. Art. 53d ust. 1 – uprawnienia urzędnika monitorującego

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.

W zakresie uprawnienia do swobodnego wstępu bez obowiązku uzyskania przepustki dostrzegamy sprzeczność z normą ISO 27001. Kontrola dostępu jest jednym z wymogów ISO27001, na które

powołuje się niniejszy akt prawny. Zgodnie z tym standardem i najlepszymi praktykami z zakresu cyberbezpieczeństwa i socjotechniki na wstęp i poruszanie się po siedzibie spółki niezbędne jest uzyskanie przepustki. W związku z powyższym dostrzegamy konieczność zmiany poprzez wykreślenie punktu lub zmianę na: 1) wstępu i poruszania się po terenie podmiotu kluczowego za uzyskaniem przepustki.

Ponieważ urzędnik monitorujący byłby sui generis „kuratorem" podmiotu kluczowego należy rozważyć czy nie powinno się doprecyzować, że pracownik taki powinien mieć poświadczenie bezpieczeństwa co najmniej o klauzuli "tajne", a decyzja o której mowa w przepisie powinna wskazywać ściśle określone zadania jakie ma wykonywać taki „kurator" zgodnie z art. 32 ust. 4 lit g NIS2 albo przynajmniej wprowadzenie możliwości odpowiedzialności za ujawnienie tajemnicy przedsiębiorstwa

46. Art. 56 ust. 3 – tłumaczenia na język polski

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.

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.

47. Art. 62 ust. 3 – zakupy na rzecz podmiotów publicznych

Izba wnioskuje o usunięcie albo ograniczenie możliwości dokonywania zakupów produktów ICT, usług ICT lub procesów ICT przez Pełnomocnika na rzecz podmiotów publicznych. Uprawnienie to może spowodować, że uszczuplone zostaną możliwości konkurowania o zlecenia podmiotów publicznych, a Pełnomocnik zostanie pośrednikiem w zakupach mającym charakter Operatora Sieci obejmującej podmioty publiczne. Podobne pomysły były przedmiotem ostrej krytyki poprzednich projektów ustawy i w znacznym stopniu przyczyniły się do ich pogrzebania.

48. Art. 67a – rekomendacje Pełnomocnika

Projekt ustawy przewiduje dodanie do ustawy o krajowym systemie cyberbezpieczeństwa nowego art. 67a, który daje Pełnomocnikowi kompetencję do wydawania rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Nowo dodawany przepis określa również podstawowe aspekty związane z wydaniem, udostępnieniem i wykonywaniem rekomendacji.

W związku z powyższym zwracamy uwagę, że w ustawie o krajowym systemie cyberbezpieczeństwa już dzisiaj funkcjonują przepisy art. 33 ust. 4 – 9, które upoważniają Pełnomocnika do wydawania, zmieniania i odwoływania rekomendacji dotyczących stosowania produktów ICT, usług ICT lub procesów ICT, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Przepisy te określają również tryb wydawania rekomendacji, sposób ich udostępniania i dostępne środki odwoławcze. Podkreślić trzeba, że projekt ustawy przewiduje wprowadzenie szeregu zmian do art. 33 ust. 4 – 9 ustawy o krajowym systemie cyberbezpieczeństwa, jednocześnie zakładając utrzymanie w mocy tych przepisów.

W efekcie dodanie do ustawy o krajowym systemie cyberbezpieczeństwa art. 67a, z jednoczesnym utrzymaniem w mocy art. 33 ust. 4 - 9 ustawy, spowoduje, że ta sama instytucja i narzędzie, czyli rekomendacje Pełnomocnika, będą regulowane zestawem dwóch różnych przepisów tej samej

ustawy. A podkreślić trzeba, że dodawany art. 67a i zmieniany art. 33 ust. 4 nieco odmiennie opisują procedurę wydawania, udostępniania i wykonywania rekomendacji Pełnomocnika i cel, któremu te rekomendacje mają służyć. Jeśli jest to błąd to błąd ten należy poprawić. Jeśli natomiast intencją Projektodawcy było stworzenie dwóch różnych narzędzi prawnych, z których każdy nazywa się „rekomendacjami Pełnomocnika" to taki zabieg należy ocenić krytycznie, gdyż taka konstrukcja będzie powodowała liczne wątpliwości i spory praktyczne. Jeśli zamierzeniem było oddanie w ręce Pełnomocnika dwóch różnych narzędzi to musi to znaleźć odzwierciedlenie w przepisach ustawy, która powinna wyraźnie rozgraniczać (również na poziomie nazewnictwa) oba instrumenty.

49. Art. 67b ust. 1 – podmioty, do których może być kierowana decyzja HRV

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.

50. Art. 67b – przegląd decyzji HRV

Postulujemy, aby wprowadzić zasadę cyklicznego przeglądu wydanych decyzji dot. dostawcy wysokiego ryzyka. Przegląd wydanej decyzji powinien się odbywać po okresie nie krótszym niż czas wynikający z decyzji (w tym przypadku 4 lata).

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.

51. Art. 67b – notyfikacja techniczna

Wyjaśnienia wymaga wyrażone w uzasadnieniu utrzymanie założenia dot. braku uzasadnienia dla dokonania notyfikacji technicznej w zakresie przepisów. 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.

52. Art. 67c ust. 2 – termin na wycofanie produktów ICT, rodzajów usług ICT, konkretnych procesów ICT wskazanych w decyzji HRV

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-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 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.

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[3]. W Stanach Zjednoczonych, istotnych opóźnień doznaje także program wymiany zasobów „lokalnych operatorów", w którym zabrakło publicznych środków finansujących zmiany w sieciach[4]. Może to – wg FCC – grozić upadkiem niektórych firm 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:

- W pierwszej kolejności o wprowadzenie dla wszystkich podmiotów jednolitego terminu wycofania wynoszącego 7 lat.
- W drugiej kolejności o przywrócenie brzmienia poprzednich wersji projektu, tj. wprowadzenie terminu 5-letniego dla zasobów z załącznika nr 3.
- W obu powyższych wypadkach o wprowadzenie wyraźnej procedury umożliwiającej podmiotowi obowiązanemu do wymiany złożenie wniosku o wyrażenie przez Ministra zgody na przedłużenie terminu określonego w decyzji.

53. Art. 67c ust. 3 – użytkowanie w czasie na wycofanie

3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT (…)

W art. 67c ust. 3 zawarto błędne odwołanie do art. 67b ust. 1 pkt 2, który wskazuje: „2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat". Może to sugerować, że jedynie zasoby podlegające wymianie w 7 lat mogą być użytkowane w okresie na wycofanie. Uzasadnienie projektu nie wskazuje na takie rozróżnienie, które byłoby jednocześnie skrajnie nieadekwatne i mogłoby skutkować koniecznością natychmiastowego przerwania działania usług.

[3] https://www.ft.com/content/54d46cf2-5e24-49d4-9939-63a564c27ca6
[4] https://www.washingtonpost.com/technology/2024/05/02/huawei-rip-remove-order-threatens-service/

Dlatego niezbędne jest wprowadzenie poprawki w projekcie, która będzie zawierała odwołanie do wszystkich typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT niezależnie od okresu na ich wymianę. W przypadku utrzymania konstrukcji zawierającej odwołanie, powinno ono odnosić się zarówno do ust. 1 pkt 2, jak i do ust. 2.

54. Art. 67g – polecenie zabezpieczające

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 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.

55. Art. 67g ust. 5 w zw. z ust. 11 – przesłanki do uwzględniania w toku analizy

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.

56. Art. 67g ust. 12 – czas obowiązywania polecenia zabezpieczającego

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.

57. Art. 73 ust. 5 – kara do 100 mln zł

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 jasne jaka jest relacja do uprawnienia nałożenia kary z ust. 1 do kary z ust. 5. W naszej ocenie istnieje ryzyko 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 będą adekwatnie dolegliwie odstraszać od naruszeń.

58. Art. 74 ust. 2 – możliwość nadania karze pieniężnej rygoru natychmiastowej wykonalności

Jako Izba stoimy na stanowisku, że kara pieniężna nigdy nie powinna być nakładana pod rygorem natychmiastowej wykonalności. Możliwość nadania rygoru natychmiastowej wykonalności decyzji nakładającej karę pieniężną przewiduje art. 74 ust. 2 ustawy (w brzmieniu nadawanym projektowaną ustawą) i choć jest to możliwość (a nie ustawy rygor natychmiastowej wykonalności) to uważamy, że nie powinno być takiej możliwości. Kary pieniężne, w szczególności tak wysokie jak te, które przewiduje ustawa w brzmieniu nadawanym projektowaną ustawa, są bardzo dotkliwe i nie powinny nigdy być natychmiast wykonywane, a więc wykonywane zanim jeszcze decyzja o nałożeniu kary stanie się prawomocna i zakończy się ewentualne postępowanie sądowe zainicjowane odwołaniem się od decyzji. Konieczność uiszczenia wysokiej kary pieniężnej może oznaczać koniec działalności podmiotu kluczowego albo ważnego, a skutki mogą nieodwracalne, nawet jeśli po latach sąd przyzna rację podmiotowi skarżącemu decyzję o karze. Natychmiastowa wykonalność kary pieniężnej budzi zastrzeżenia natury konstytucyjnej, bo może być odczytywana jako ograniczenie prawa do sądu, w szczególności biorąc pod uwagę przeciętny czas oczekiwania na wydanie orzeczenia przez sąd.

Właśnie z tych względów szereg przepisów obowiązującego prawa, traktujących o nakładaniu kar pieniężnych przez organy nadzorcze w różnych sektorach działalności regulowanej, wprost wyłączają możliwość nadania rygoru natychmiastowej wykonalności decyzji o nałożeniu kary pieniężnej. Dobrym przykładem jest tu obowiązująca ustawa – Prawo telekomunikacyjne, która w art. 210 ust. 1 zdanie drugie jednoznacznie i kategorycznie przesądza, że decyzjom o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.

Projektowane przepisy powinny być zmienione na wzór przytoczonego przepisu ustawy – Prawo telekomunikacyjne. Projektowany art. 74 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa powinien wprost i jednoznacznie przesądzać, że decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.

59. Art. 76 - inne przyczyny nałożenia kary

Za wątpliwe w kontekście zasady proporcjonalności jest nałożenie kar, pomimo zaprzestania naruszenia prawa lub naprawienia szkody - takie przyjęcie penalizacji w ksc narusza podstawowe zasady TFUE; ponadto jest to jednocześnie sprzeczne z art. 76a ust 6, gdzie wskazano na możliwość odstąpienia od wymierzenia kary i jedną z możliwości odstąpienia jest właśnie zaprzestanie naruszenia, za które jednocześnie jest penalizacja w art. 76 - zastosowano tutaj alternatywę rozłączną „albo".

60. Art. 76b ust. 1 – dzienna kara pieniężna

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 zwiększana wielokrotnie

wysokość 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.

Ponadto nieakceptowalny jest przepis, który pozwala na nakładanie okresowych (dziennych) kar pieniężnych za każdy dzień niewykonania przez podmiot kluczowy albo ważny ostrzeżenia wydanego przez organ, a taką właśnie możliwość przewiduje projektowany art. 76b ust. 1 pkt 1) ustawy. Przepis ten daje możliwość nakładania okresowej kary pieniężnej za każdy dzień opóźnienia w wykonaniu czynności określonych w ostrzeżeniu wydanym na podstawie art. 53 ust. 4. Nie może być kar pieniężnych (ani okresowych ani żadnych innych) za niezastosowanie się przez przedsiębiorcę do ostrzeżenia (o którym mowa w art. 53 ust. 4 ustawy – w brzmieniu nadawanym projektowaną ustawą), a więc niewiążącego dla przedsiębiorcy instrumentu prawnego. Nowo dodawany art. 53 ust. 4 ustawy przewiduje, że w przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobiegnięcia lub zaprzestania naruszania przepisów ustawy. Zatem ostrzeżenie zostało pomyślane jako narzędzie nie władcze (instrument „miękki"), dające podmiotowi kluczowemu albo ważnemu możliwość polubownego załatwienia sprawy bez wdawania się w postępowanie i spór z organem, z drugiej stromy nie wymagające od organu wydającego ostrzeżenie wykazania i udowodnienia, że doszło do naruszenia (wystarczy uzasadnione podejrzenie po stronie organu), niewymagające również wydania decyzji administracyjnej (przepis mówi o pisemnym wystąpieniu). Ostrzeżenie nie jest narzędziem władczym, podmiot kluczowy i ważny nie ma prawnego obowiązku zastosowania się do ostrzeżenia, i z tych powodów projektowane przepisy wydają się nie przewidywać możliwości zaskarżenia ostrzeżenia przez podmiot kluczowy lub ważny. A skoro tak to nie może być mowy o nakładaniu na podmiot kluczowy albo ważny jakichkolwiek kar za niezastosowanie się do ostrzeżenia, skoro nie ma obowiązku zastosowania się do ostrzeżenia. Jeśli podmiot kluczowy albo ważny nie zastosuje się do ostrzeżenia, a organ ma uzasadnione podejrzenie, że doszło do naruszenia ustawy, to może skorzystać z instrumentu władczego jakim są „nakazy", o których mowa w art. 53 ust. 5 i następne ustawy (w brzmieniu nadawanym projektowana ustawą).

Biorąc powyższe pod uwagę uważamy za konieczne usunięcie z projektowanego art. 76b ust. 1 punktu i fragmentu, który daje możliwość nakładania dziennych kar pieniężnych za niezastosowanie się do ostrzeżenia.

61. <u>Art. 14 ustawy nowelizującej – termin realizacji obowiązków i wpis do rejestru</u>

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. 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.

62. 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".

Zdanie odrębne firm Ericsson, Nokia oraz Samsung

Zdaniem firm Ericsson, Nokia i Samsung nie do przedsiębiorstw sektora prywatnego należy kwestionowanie środków podjętych przez rząd w celu ochrony bezpieczeństwa narodowego. Polska propozycja przepisów dotycząca dostawców uznanych za stwarzających wysokie ryzyko nie odbiega od tego, co zaproponowała większość krajów, które podjęły środki do tej pory, i odzwierciedlają one zrównoważone i rozsądne podejście oparte na ocenie ryzyka. Uwagi naszych firm (które stanowią głos większości producentów i dostawców rozwiązań telekomunikacyjnych) do stanowiska PIIT, dotyczące punktów związanych z dostawcami wysokiego ryzyka nie zostały uwzględnione, dlatego w tym zakresie nie popieramy tego stanowiska.

Niemniej jednak w stanowisku PIIT wspieramy komentarze związane z NIS2 oraz ze stanowiskiem dotyczącym niezwłocznego przyjęcia ustawy w celu harmonizacji przepisów oraz stabilności prawnej. Z zadowoleniem przyjmujemy zamiar polskiego rządu implementacji Dyrektywy NIS2 i unijnego zestawu narzędzi na potrzeby cyberbezpieczeństwa sieci 5G.