INSTYTUT KOŚCIUSZKI

# Projekt ustawy o krajowym systemie cyberbezpieczeństwa

Stanowisko

Instytutu Kościuszki

Listopad 2017

Kraków

THINK TANK KREUJĄCY NOWE IDEE DLA POLSKI I EUROPY
(+48) 12 632 97 24 ul. Feldmana 4/9-10, 31-130 Kraków
www.ik.org.pl ik@ik.org.pl
NIP 6751 302 992 REGON 356 683 760 KRS 0000145838
Alior Bank PL55 2490 0005 0000 4600 4487 1442

*Ustawa o krajowym systemie cyberbezpieczeństwa* stanowi kolejny kluczowy element w budowie ram prawnych i instytucjonalnych, które mają zapewnić efektywność funkcjonowania państwa polskiego w obszarze ochrony cyberprzestrzeni. Po przygotowaniu dokumentu strategicznego – *Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-22* oraz planistycznego - *Planu Działań na rzecz wdrażania Krajowych Ram Cyberbezpieczeństwa RP na lata 2017-2022*, Ministerstwo Cyfryzacji, jako organ właściwy ds. bezpieczeństwa cyberprzestrzeni, przedstawił projekt aktu normatywnego, który ma stanowić kompleksową regulację zharmonizowanego i skonsolidowanego krajowego systemu cyberbezpieczeństwa oraz transponować do prawa polskiego postanowienia unijnej Dyrektywy NIS (Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii). Poniżej prezentujemy stanowisko Instytutu Kościuszki przedstawione w ramach konsultacji publicznych projektu ustawy. Doceniając wysiłek Ministerstwa Cyfryzacji, jako podmiotu aktywnie działającego na rzecz wzmacniania bezpieczeństwa cyberprzestrzeni oraz rozwoju ram instytucjonalnych zapewniających realizację polityki cyberbezpieczeństwa, Instytut Kościuszki zachęca do udoskonalenia przedłożonego projektu ustawy. Poniższe uwagi przedstawiono w dwu kategoriach. Na początku prezentujemy uwagi ogólne i postulaty, dla których głównym punktem odniesienia są *Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-22* oraz inne przedmiotowe dokumenty programowe. Część druga zawiera uwagi Instytutu Kościuszki dotyczące poszczególnych rozwiązań legislacyjnych zaproponowanych w projekcie ustawie.

## Uwagi ogólne i postulaty

*Ustawa o krajowym systemie cyberbezpieczeństwa* zgodnie z postulatami przedstawionymi w *Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-22*, *Planie Działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017 - 2022* oraz pozostałych dokumentach programowych Ministerstwa Cyfryzacji w przedmiotowym obszarze, powinna stanowić kompleksową regulację zapewniającą skuteczność systemu cyberbezpieczeństwa poprzez konsolidację i harmonizację działań wszystkich interesariuszy. Zgodnie z diagnozą, że efektywność dotychczasowych aktywności państwa w obszarze cyberbezpieczeństwa jest obniżona wskutek jej rozproszonego charakteru, ustawa o *krajowym systemie cyberbezpieczeństwa* powinna w sposób całościowy obejmować podstawy ustroju i wzajemnych relacji zaangażowanych podmiotów. Przedstawiony do konsultacji projekt pozostaje w tym zakresie niekompletny, ograniczając się do uporządkowania przedmiotowych obszarów w znacznym stopniu tylko w kontekście implementacji postanowień Dyrektywy NIS.

W tym kontekście projekt ustawy ignoruje m.in.: postulat utworzenia Naukowego Klastra Cyberbezpieczeństwa[1] (szkolnictwo wyższe jest elementem systemu wyłącznie w kontekście realizacji zgłoszeń incydentów, art. 28 ust. 6 lit. l w zw. z art. 4 pkt 13 – takie zawężenie jest też wątpliwe w świetle motywu 5 dyrektywy NIS[2]) lub budowy systemu wsparcia przedsięwzięć badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa[3], rozwoju *hubów* innowacyjności oraz uruchomienia programu *Cyberpark Enigma*[4]. Jakkolwiek do niektórych z tych kwestii odniesiono się częściowo w Ocenie Skutków Regulacji, należy podkreślić, iż brak literalnego określenia ich pozycji i zadań w ramach krajowego systemu cyberbezpieczeństwa stanowi niedociągnięcie, którego nie niwelują wskazane w art. 41 pkt. 2-3 kompetencje ministra właściwego ds. informatyzacji w zakresie realizacji Strategii Cyberbezpieczeństwa RP. W projekcie ustawy nie unormowano również roli Forum ds. Cyberbezpieczeństwa przy Ministerstwie Cyfryzacji, jak i Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP w ramach KRMC.

Podobnie projekt ustawy pomija zagadnienie budowy klastra bezpieczeństwa dla administracji centralnej oraz roli jaką powinien on pełnić w ramach systemu na poziomie technicznym. Priorytetowe, zgodnie z *Krajowymi Ramami*, wyzwanie utworzenia bezpiecznych sieci typu intranet, oferujących połączenia wewnątrz sieci, usługi bezpieczeństwa oraz bezpieczny dostęp do sieci Internet[5], nie zostało uwzględnione w projekcie ustawy.

Projekt ustawy nie odnosi się także wprost do potrzeby budowania sektorowych zespołów CSIRT, która była postulowana w *Krajowych Ramach*[6]. Z uwagi na specyfikę sektorów, dogodnym rozwiązaniem byłoby, aby każdy organ właściwy w rozumieniu projektu ustawy posiadał zespół CSIRT będący z jednej strony jego zapleczem eksperckim, a z drugiej – elementem pośredniczącym pomiędzy operatorami usług kluczowych a właściwym CSIRT (NASK, GOV, MON). Warto w tym kontekście wykorzystać doświadczenie oddolnych inicjatyw sektorowych (np. w sektorze energetycznym)[7].

Zaznaczone wyraźnie w projekcie ustawy podejście sankcyjne nie zostało w dostatecznie wyraźnym stopniu uzupełnione w obszarze konkretnych zachęt oraz wsparcia administracji publicznej w

[1] *Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-22*, s. 20.
[2] (…) Z kolei brak wspólnych wymogów dotyczących operatorów usług kluczowych i dostawców usług cyfrowych uniemożliwia ustanowienie całościowego i skutecznego mechanizmu współpracy na poziomie Unii. Uczelnie i ośrodki badań naukowych mają do odegrania zasadniczą rolę w pobudzaniu badań, rozwoju i innowacyjności w tych obszarach.
[3] *Krajowe Ramy…*, s. 21.
[4] *Ibidem*, s. 20.
[5] *Ibidem*, s. 13.
[6] *Ibidem*, s. 11.
[7] Sordyl J., *Budowa CERT-u PSE oraz podejmowane działania na rzecz budowy CERT-u sektorowego – wymagania dla zapewnienia cyberbezpieczeństwa* [w:] Skokowski D., Jóźwik Z., *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny,* Instytut Kościuszki, Kraków 2017, s. 82-84.

przedmiocie realizacji nowych obowiązków nałożonych na podmioty objęte zakresem normowania. Zgodnie z *Krajowymi Ramami*, rząd powinien podejmować działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych[8]. Poza nieprecyzyjnymi postanowieniami art. 41 pkt 3-4, 6-7, projekt ustawy nie zawiera odpowiednich mechanizmów w tej kwestii. Dobrym rozwiązaniem byłoby opracowanie sektorowych standardów przy wsparciu CSIRT, organów właściwych, operatorów usług kluczowych, dostawców usług cyfrowych oraz z wykorzystaniem potencjału intelektualnego ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych[9], które w oparciu o normy międzynarodowe (np. NIST) i najlepsze praktyki a także wytyczne Agencji ENISA, umożliwiłyby efektywne wzmocnienie krajowego systemu cyberbezpieczeństwa. Podobnie ustawa o krajowym systemie cyberbezpieczeństwa powinna nakładać na operatorów usług kluczowych, podmioty publiczne, organy właściwe obowiązek systematycznych szkoleń i ćwiczeń (obecnie tylko w odniesieniu do organów właściwych) podnoszących ogólny poziom świadomości i kompetencji w obszarze cyberbezpieczeństwa. Postulat, zaznaczony w *Krajowych Ramach*[10], nie znalazł swego odzwierciedlenia w projekcie ustawy.

Projekt ustawy nie wykorzystuje potencjału organizacji pozarządowych (fundacji, stowarzyszeń) w budowaniu świadomości społecznej w obszarze cyberbezpieczeństwa. Szczególnie w zakresie kompetencji nadanych ministrowi właściwemu ds. informatyzacji (art. 41 pkt 7) polegających na prowadzeniu działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i podnoszenia świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników, powinna zostać podkreślona rola i możliwe modele współpracy z trzecim sektorem. Pomijając już możliwą większą efektywność tego rodzaju zadań związanych z możliwości wykorzystania nieformalnych struktur sieciowych, w ramach których funkcjonują organizacje pozarządowe, możliwość delegacji przedmiotowych zadań podmiotom z trzeciego sektora byłaby zgodna z *Programem współpracy Ministra Cyfryzacji z organizacjami pozarządowymi oraz podmiotami wymienionymi w art. 3 ust. 3 ustawy o działalności pożytku publicznego I o wolontariacie* z 2016 roku.

[8] *Krajowe Ramy*…, s. 12-13.
[9] *Ibidem*, s. 13-14.
[10] Ibidem, s. 22.

# Uwagi dotyczące rozwiązań regulacyjnych

## Definicja cyberbezpieczeństwa (art. 2 pkt 5)

Należy rozważyć czy zaproponowana w projekcie ustawy definicja cyberbezpieczeństwa (art. 2 pkt 5 w związku z art. 2 pkt 18-19 projektu ustawy oraz art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne) odpowiada zakresowi pojęciu bezpieczeństwa sieci i systemów informatycznych zgodnie z art. 4 pkt 2 Dyrektywy NIS. Na podstawie wykładni literalnej przedmiotowego przepisu można postawić wniosek, iż projekt ustawy zawężą zakres normowania wyłącznie do bezpieczeństwa systemów informatycznych w rozumieniu dyrektywy NIS. Nawet jeżeli przyjąć przychylną projektodawcy wykładnię, iż postulat Dyrektywy NIS jest realizowany poprzez zawarte w art. 2 pkt 19 odesłanie do definicji systemu teleinformatycznego z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, należy stwierdzić niekonsekwencję terminologiczną, ponieważ w innych przepisach, projektodawca odnosi się literalnie do sieci teleinformatycznej (np. art. 28 ust. 5 pkt 2, art. 28 ust. 6 pkt 1 lit. a, art. 28 ust. 7 pkt 12 projektu ustawy). W związku z powyższym, w celu uniknięcia niejasności w odniesieniu do prawidłowej implementacji Dyrektywy NIS, należy dokonać jednoznacznego określenia definicji cyberbezpieczeństwa w kontekście pojęcia bezpieczeństwa sieci i systemów informatycznych.

## Wyłącznie ustawy o dostępie do informacji publicznej (art. 3 ust. 3)

Zgodnie z art. 3 ust. 3 projektu ustawy, do procedury udostępniania informacji o podatnościach na incydenty, incydentach, zagrożeniach cyberbezpieczeństwa, poziomie ryzyka wystąpienia incydentów, nie ma zastosowania ustawa o dostępie do informacji publicznej. Biorąc pod uwagę rygorystyczne kryteria wskazane w projekcie ustawy, uregulowania ustawy o ochronie informacji niejawnych, jak i proponowane rozwiązania w tym zakresie w projekcie ustawy o jawności życia publicznego (np. art. 2 ust. 1 pkt 2, art. 7 pkt 2 lit. b-d, art. 7 pkt 3 lit. a-b, art. 7 pkt 4) oraz wymogi art. 31 ust. 3 Konstytucji RP, należy stwierdzić, że takie ograniczenie stanowi nieproporcjonalną ingerencję w prawo informacji o działalności organów władzy publicznej (art. 61 Konstytucji RP). Z uwagi na okoliczność, iż nie każda informacja z zakresu określonego w art. 3 ust. 2, która mogłaby być potencjalnie przedmiotem wniosku o udostępnienie informacji publicznej, stanowi informację istotną z punktu widzenia bezpieczeństwa lub porządku publicznego państwa, sankcjonowanie wyłączenia na zasadzie klauzuli generalnej jest rozwiązaniem zbytnio naruszającym istotę prawa do informacji publicznej. Należy też zaznaczyć, że organ, wobec którego obywatel wystąpi z wnioskiem o udostępnienie informacji publicznej w przedmiotowym zakresie i tak dysponuje (w związku z przytoczonymi powyżej regulacjami, jak i warunkami z art. 3 ust. 2 projektu ustawy) istotnym zakresem uznania administracyjnego.

## Elementy krajowego systemu cyberbezpieczeństwa (art. 4)

Zgodnie z *Krajowymi Ramami*, do krajowego systemu cyberbezpieczeństwa, poza podmiotami wskazanymi bezpośrednio w Dyrektywie NIS, zaliczają się także operatorzy infrastruktury krytycznej[11]. W związku z powyższym, katalog wskazany w art. 4 nie jest wyczerpujący w świetle art. 3 pkt 2 ustawy o zarządzaniu kryzysowym, ponieważ nie odnosi się on literalnie do wszystkich systemów infrastruktury krytycznej wskazanej w niniejszej ustawie. Oznacza to, że proponowany w ustawie krajowy system cyberbezpieczeństwa może być niekompletny (np. w zakresie zaopatrzenia w żywność, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych). Zalecanym rozwiązaniem byłoby zatem odpowiednie poszerzenie katalogu z art. 4 lub odwołanie do przedmiotowych przepisów ustawy o zarządzaniu kryzysowym.

W tym kontekście warto również rozważyć na ile zasadne jest włączanie do katalogu z art. 4 projektu ustawy uczelni publicznych (art. 4 pkt 13 projektu ustawy, co wiąże się wszak z nakładaniem na nie rozbudowanych obowiązków w zakresie zawiadamiania o incydentach, itp.) lub alternatywnie wyłączenie z tego katalogu uczelni prywatnych (co z kolei byłoby niezrozumiałe z uwagi na podobieństwo podmiotów lub możliwy wpływ regulacji na rynek usług szkolnictwa wyższego).

## Upoważnienia ustawowe a terminy transpozycji Dyrektywy NIS (art. 6, art. 11. ust. 3, art. 12 ust. 4, art. 15 ust. 4)

Zgodnie z art. 25 ust. 1 Dyrektywy NIS, w celu transpozycji, państwa członkowskie przyjmują i publikują w terminie do dnia 9 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne oraz stosują je od dnia 10 maja 2018 roku. W związku z zawartymi w projekcie ustawy delegacjami ustawowymi do wydawania przez właściwe organy rozporządzeń (art. 6, art. 11. ust. 3, art. 12 ust. 4, art. 15 ust. 4 projektu), istnieje ryzyko, iż proces implementacji prawa unijnego będzie zaburzony. W celu efektywnej transpozycji oraz przede wszystkim sprawnej konsolidacji krajowego systemu cyberbezpieczeństwa, konieczne jest aby omawianych przepisać wskazać odpowiednie terminy do realizacji delegowanej kompetencji (np. 6 miesięcy od wejścia w życie ustawy).

## Obowiązki informacyjne przedsiębiorcy w obszarze cyberbezpieczeństwa (art. 15 ust. 1 pkt 2)

Zgodnie z art. 15 ust. 1 pkt 2 projektu ustawy operatorzy usług kluczowych zobowiązani są do zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi

[11] *Krajowe Ramy…*, s. 6.

zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Powyższy przepis został sformułowany w sposób nieprecyzyjny oraz jest pozbawiony sankcji (art. 57 projektu), co może istotnie przyczynić się do braku realizacji dyspozycji ustanowionej nim normy. Operatorzy usług kluczowych, jako podmioty realizujące zadania o fundamentalnym znaczeniu dla współczesnego społeczeństwa i gospodarki, powinni być zobowiązani do uczestnictwa w budowaniu świadomości użytkowników w obszarze cyberbezpieczeństwa. Warto w tym kontekście rozważyć nałożenie obowiązku przesyłania okresowej informacji (nie tylko „zapewniania dostępu do wiedzy" ale konkretnych obowiązków informacyjnych) dotyczącej aktualnych zagrożeń cybernetycznych mogących wiązać się z korzystaniem z danej usługi kluczowej (np. na zasadzie aktualizacji polityki prywatności udostępnianych użytkownikom przez platformy cyfrowe lub prowadzenie działań edukacyjnych, kampanii uświadamiajacych). Będzie to też miało korzystny wpływ na cyberbezpieczeństwo operatorów usług kluczowych, którzy mogą dzięki temu uzyskiwać bieżącą informację od użytkowników na temat wykrytych podatności i incydentów (zidentyfikowanych dzięki ostrzeżeniom operatorów).

Warto również rozważyć, aby obowiązek ten dotyczył także innych podmiotów krajowego systemu cyberbezpieczeństwa, np. przedsiębiorstw telekomunikacyjnych (art. 4 pkt 5), organów administracji publicznej (art. 4 pkt 6), jednostek samorządu terytorialnego (art. 4 pkt 12).

## Delegacja obowiązków podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa (art. 15 ust. 2)

Zgodnie z literalną wykładnią przepisów ustawy, jedynie operatorzy usług kluczowych mogą powierzać realizację poszczególnych zadań, podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa. Takiej możliwości nie przewidują regulacje dotyczące dostawców usług cyfrowych, jak i podmiotów publicznych. Takie ograniczenie zdaje się nieuzasadnione.

Przy okazji warto nadmienić, że podmioty świadczące usługi z zakresu cyberbezpieczeństwa (art. 4 pkt 15 projektu ustawy) powinny być poddane certyfikacji ABW lub SKW (procedura zbliżona do nadania certyfikatu bezpieczeństwa teleinformatycznego - zgodnie z art. 50 ust. 3 ustawy o ochronie informacji niejawnych). Z uwagi na zakres zadań, który może być przekazany podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa (art. 15 ust 2 w związku z art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1 oraz art. 14, art. 23), jak i zadania z zakresu współpracy z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi (art. 35 ust. 5) oraz dostęp do systemu teleinformatycznego, o którym mowa w art. 42 ust. 1 pkt 1), należy rozważyć, czy ustawa nie powinna w sposób literalny odnosić się do wymogu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. W tym aspekcie, nadzór ministra właściwego ds. informatyzacji przewidziany w art. 47 ust. 1 pkt. 1 projektu ustawy, należy uznać za model niewystarczający zarówno w kontekście ograniczonych kryteriów kontroli (zawężonych

do czynników wskazanych w art. 15 ust. 2), następczego charakteru realizacji przedmiotowej kompetencji, jak i ograniczonego zakresu czynności kontrolnych (zgodnie z procedurą kontroli działalności gospodarczej przedsiębiorcy opisaną w ustawie o swobodzie działalności gospodarczej - art. 48 ust. 1 w związku z art. 47 ust. 1 pkt 1 projektu ustawy).

Potrzeba literalnego odniesienia się do mechanizmu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, wynika zarówno z okoliczności faktycznych, dokumentów programowych Ministerstwa Cyfryzacji oraz generalnego postulatu jasności prawa (kompleksowości tekstu prawnego). Po pierwsze, z uwagi na podstawowe interesy bezpieczeństwa państwa, certyfikacja zminimalizuje ryzyko wykorzystywania w ramach ochrony teleinformatycznej operatorów usług kluczowych rozwiązań, które przyczyniałyby się do obniżenia poziomu cyberbezpieczeństwa poprzez m.in. użytkowanie oprogramowania zawierającego celowo umieszczone luki (m.in. *backdoor*). Postulat udziału ABW w procesie weryfikacji producentów i usługodawców rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej, podnoszony był również w *Założeniach strategii cyberbezpieczeństwa RP* z 2016 roku. Ustanowienie mechanizmu certyfikacji w ustawie, pomoże też zminimalizować ewentualną niejasność co do stosowania właściwych przepisów (np. ustawy o ochronie informacji niejawnych) w kontekście zlecania zadań przez operatorów usług kluczowych podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa. Co z kolei może się pozytywnie przyczynić do faktycznej realizacji przedmiotowych obowiązków – a zatem podnieć stopień odporności krajowego systemu cyberbezpieczeństwa.

## Audyt bezpieczeństwa teleinformatycznego operatorów usług kluczowych (art. 16 ust. 1)

Zgodnie z art. 16 ust. 1 projektu ustawy, na operatorów usług kluczowych nałożony został obowiązeksą realizacji audytu bezpieczeństwa teleinformatycznego co najmniej raz na dwa lata. Z uwagi na tempo rozwoju liczby i zaawansowania zagrożeń w cyberprzestrzeni oraz znaczenie operatorów usług kluczowych dla funkcjonowania współczesnego społeczeństwa i gospodarki, audyty bezpieczeństwa teleinformatycznego powinny być realizowane w okresach częstszych – np. co pół roku.

Tym samym ustawa powinna doprecyzować procedurę wyboru (prawdopodobnej certyfikacji jak w przypadku podmiotów świadczących usługi z zakresu cyberbezpieczeństwa) oraz organ dokonujący akredytacji (art. 16 ust. 2) podmiotów uprawnionych do realizacji audytów.

## Obowiązki podmiotów publicznych (art. 25)

Zakres obowiązków podmiotów publicznych zgodnie z projektem ustawy jest znacznie ograniczony w porównaniu do operatorów usług kluczowych. Z uwagi na wymogi konsolidacji krajowego systemu

cyberbezpieczeństwa, trudno zrozumieć *ratio legis* takiego zabiegu. Co najmniej organy centralnej administracji rządowej powinny być zobowiązane do realizacji obowiązków przewidzianych w art. 10, art. 11 ust. 1 i ust. 3, art. 12 ust. 1 pkt 6 zd. 2, art. 13 oraz art. 14 projektu ustawy. W tym też kontekście należy jasno określić relacje pomiędzy ustawą o krajowym systemie cyberbezpieczeństwa a obowiązkami wynikającymi z ustawy o ochronie danych osobowych (np. art. 3 ust. 1, art. 39a ), rozporządzeniem MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, jak i Krajowymi Ramami Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

## Przegląd wykazu zidentyfikowanych operatorów usług kluczowych. (art. 39 ust. 1 pkt 1)

Zgodnie z art. 39 ust. 1 pkt 1 organy właściwe są zobowiązane do bieżącej analizy podmiotów w danym sektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej (podobnie w art. 5 ust. 4). Należy rozważyć uzupełnienie przepisu zgodnie z brzmieniem art. 5 ust. 5 Dyrektywy NIS, który oprócz obowiązku regularnego przeglądu, wskazuje termin dwuletni dla przeprowadzenia okresowej analizy. Biorąc pod uwagę zapewnienie skuteczności realizacji przedmiotowej dyspozycji, wydaje się zasadne uzupełnienie przepisu, tak aby organ właściwy był zobowiązany do bieżącej analizy oraz przedkładania np. pojedynczemu punktowi kontaktowemu w terminie nie rzadziej niż co dwa lata, po dniu 9 maja 2018 r., informacji o przeprowadzeniu przeglądu zidentyfikowanych operatorów usług kluczowych.

## Zakres Strategii Cyberbezpieczeństwa RP (art. 56 ust. 2-3)

Zakres materii koniecznych do uwzględnienia w strategii cyberbezpieczeństwa wskazany w art. 56 ust. 3 pkt 1-7 projektu ustawy pomija wskazany w art. 7 ust. 1 lit. b Dyrektywy NIS a także podrozdziale 2.2. pkt II *Załącznika do Komunikatu Komisji do Parlamentu Europejskiego i Rady „Pełne Wykorzystanie Potencjału Bezpieczeństwa Sieci i Informacji – Zapewnienie Skutecznego Wdrożenia Dyrektywy NIS”*[12], wymóg ustalenia ram zarządzania służących realizacji celów i priorytetów krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, w tym ról i zakresów obowiązków organów rządowych i innych właściwych podmiotów. Projekt ustawy w przedmiotowej kwestii zdaje się odnosić wyłącznie do wymogu wskazania podmiotów zaangażowanych we wdrażanie strategii, co zgodnie z literalną wykładnią art. 7 ust.1 lit. g Dyrektywy NIS, stanowi odrębną materię. Zarówno z uwagi na konieczność prawidłowej implementacji prawa UE, a przede wszystkim podnoszone w m.in. *Krajowych*

[12] *Załącznik do Komunikatu Komisji do Parlamentu Europejskiego i Rady Pełne Wykorzystanie Potencjału Bezpieczeństwa Sieci i Informacji – Zapewnienie Skutecznego Wdrożenia Dyrektywy NIS,* COM(2017) 476 final, s. 6.

*Ramach*, *Założeniach Strategii Cyberbezpieczeństwa dla RP* opracowanych przez Zespół Zadaniowy Ministerstwa Cyfryzacji, Raporcie NIK dot. *Realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP* czy ekspertyzie NASK *System bezpieczeństwa cyberprzestrzeni RP*, postulaty konsolidacji krajowego systemu cyberbezpieczeństwa oraz określenia zadań i wzajemnych relacji podmiotów w nim uczestniczących, należy odpowiednio uzupełnić art. 56 ust. 3 ustawy.

Podobnie należy odnieść się do art. 56 ust. 2 projektu ustawy, zgodnie z którym, strategia obejmuje sektory wskazane w załączniku do ustawy (a więc sektory, podsektory i podmioty z zakresu usług kluczowych) oraz usługi kluczowe. W związku z powyższym oraz w świetle art. 7 ust. 1 zdanie 1 Dyrektyw NIS[13], pojawia się wątpliwość, na ile intencją projektodawcy było zawężenie zakresu strategii i wyłączenie z niej m.in. operatorów infrastruktury krytycznej czy administracji publicznej. Interpretując przedmiotowy przepis w kontekście całości ustawy – w szczególności podmiotów objętych krajowych systemem cyberbezpieczeństwa (art. 4), jak i obecnym zakresem *Krajowych Ram*[14], takie zawężenie zakresu strategii należy uznać za bezzasadne. Również w cytowanym już wyżej *Załączniku* dotyczącym skutecznego wdrożenia Dyrektywy NIS, podkreślono, iż w odniesieniu do zasady harmonizacji minimalnej, przywołanej w art. 3 Dyrektywy NIS, państwa członkowskie mogą obejmować zakresem strategii, sektory spoza usług kluczowych i cyfrowych, wskazanych w załącznikach do przedmiotowego aktu. W tym kontekście zalecane jest uwzględnienie wszystkich istotnych wymiarów społeczeństwa i gospodarki – w szczególności administracji publicznej oraz innych sektorów omawianych w wytycznych OECD i ITU[15].

## Zakres podmiotów podlegających karze pieniężnej oraz wysokość kary pieniężnej (art. 57)

Zgodnie z art. 57 ust. 1 projektu ustawy, karom pieniężnym podlegają wyłącznie operatorzy usług kluczowych. Biorąc pod uwagę postulat tworzenia skonsolidowanego krajowego systemy cyberbezpieczeństwa, zasadne byłoby, aby rozszerzyć ten zakres co najmniej o podmioty publiczne (w rozumieniu rozdziału 4 projektu ustawy) oraz we odpowiednim, niekolidującym z postanowieniami sektorowych aktów Komisji Europejskiej (art. 47 ust. 1 pkt 2 lit. b projektu ustawy, motyw 57 dyrektywy

[13] Art. 7 ust. 1 Dyrektywy NIS: Każde państwo członkowskie przyjmuje krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych oraz obejmujące co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III.

[14] *Krajowe Ramy*, s. 6.

[15] *Załącznik do Komunikatu Komisji do Parlamentu Europejskiego i Rady Pełne Wykorzystanie Potencjału Bezpieczeństwa Sieci i Informacji – Zapewnienie Skutecznego Wdrożenia Dyrektywy NIS,* COM(2017) 476 final, s. 5-7.

NIS) – również dostawców usług cyfrowych (szczególnie w przypadku ich wykorzystania przez podmioty publiczne lub operatorów usług kluczowych – art. 19 ust. 2 projektu ustawy).

Wysokość kar pieniężnych wskazana w art. 57 ust. 2-3 projektu ustawy w niedostatecznym stopniu odpowiada wymogowi skuteczności, proporcjonalności i odstraszającego charakteru sankcji, zgodnie z art. 21 Dyrektywy NIS. Biorąc pod uwagę wagę wyzwania budowy efektywnego systemu cyberbezpieczeństwa, jak i rolę oraz charakter przedsiębiorstw, które zostaną uznane za operatorów usług kluczowych, kary pieniężne powinny realnie spełniać funkcje prewencyjną (także w kontekście ograniczeń stopnia odpowiedzialności – np. art. 12 ust. 2 projektu ustawy). Zaproponowana w projekcie ustawy wysokość kar pieniężnych tego wymogu nie spełnia. Warto również rekomendować projektodawcy, aby uwzględnić w tym zakresie wytyczne z *Załącznika*, aby określić wysokość kary w postaci wartości procentowej światowego obrotu z poprzedniego roku obrotowego – podobnie jak w przypadku nowelizacji ustawy o ochronie danych osobowych.

### Właściwość w zakresie decyzji o nałożeniu kary pieniężnej (art. 58 ust. 1 w związku z art. 47 ust. 2 pkt 3)

Zgodnie z art. 58 ust. 1 projektu ustawy, organem właściwym z zakresie nakładania kar pieniężnych na operatorów usług kluczowych, jest organ właściwy dla danego sektora wyznaczony zgodnie z art. 38 ust. 1 projektu ustawy. Biorąc pod uwagę charakter (np. strukturę własnościową) większości podmiotów, które zostaną uznane za operatorów usług kluczowych (m.in. wskazani w OSR), należy rozważyć, na ile nie wpłynie to niekorzystnie na stopień faktycznej realizacji przedmiotowej kompetencji a w konsekwencji utrzymanie (uzyskiwanie, podnoszenie) odpowiedniego poziomu cyberbezpieczeństwa przez te podmioty. Potencjalnym rozwiązaniem w tej kwestii byłaby centralizacja – przekazanie kompetencji organowi nadrzędnemu lub innemu, który nie pozostaje w bezpośredniej relacji z operatorem usług kluczowych potencjalnie podlegającemu karze (przy zachowaniu przez organ właściwy uprawnień nadzorczych, kontrolnych oraz możliwości wezwania do usunięcia naruszenia – art. 58 ust. 2 projektu ustawy).