Uzasadnienie

Spis treści

[1 Wstęp 3](#_Toc136511038)

[2 Uzasadnienie poszczególnych przepisów 19](#_Toc136511039)

[2.1 Zmiany w ustawie o KSC 19](#_Toc136511040)

[2.1.1 Zmiany w definicjach, katalogu podmiotów krajowego systemu cyberbezpieczeństwa zakresu przedmiotowego 19](#_Toc136511041)

[2.1.2 Przepisy o operatorach usług kluczowych oraz SOC 27](#_Toc136511042)

[2.1.3 Zmiany w przepisach dotyczących dostawców usług cyfrowych 33](#_Toc136511043)

[2.1.4 Przepisy o obowiązkach przedsiębiorców komunikacji elektronicznej w krajowym systemie cyberbezpieczeństwa 34](#_Toc136511044)

[2.1.5 Zmiany w przepisach dotyczących podmiotów publicznych 44](#_Toc136511045)

[2.1.6 ISAC i wykaz ISAC 44](#_Toc136511046)

[2.1.7 Nowe obowiązki zespołów CSIRT GOV, CSIRT MON i CSIRT NASK 47](#_Toc136511047)

[2.1.8 Zadania CSIRT INT 53](#_Toc136511048)

[2.1.9 Ocena bezpieczeństwa 54](#_Toc136511049)

[2.1.10 Zmiany w przepisach o przetwarzaniu danych 57](#_Toc136511050)

[2.1.11 Zmiany w przepisach o organach właściwych do spraw cyberbezpieczeństwa 59](#_Toc136511051)

[2.1.12 Zadania i obowiązki CSIRT sektorowych oraz CSIRT Telco 60](#_Toc136511052)

[2.1.13 Zmiany dot. systemu S46, zadań MON oraz nadzoru 63](#_Toc136511053)

[2.1.14 Krajowy system certyfikacji cyberbezpieczeństwa 66](#_Toc136511054)

[2.1.15 Rekomendacje Pełnomocnika. Nowi członkowie oraz zadania Kolegium 76](#_Toc136511055)

[2.1.16 Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka 78](#_Toc136511056)

[2.1.17 Ostrzeżenie 93](#_Toc136511057)

[2.1.18 Zmiany w przepisach o administracyjnych karach pieniężnych 95](#_Toc136511058)

[2.1.19 Strategiczna sieć bezpieczeństwa 99](#_Toc136511059)

[2.1.20 Przyznanie częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz 110](#_Toc136511060)

[2.1.21 Finansowanie strategicznej sieci bezpieczeństwa 113](#_Toc136511061)

[2.1.22 Zmiany w art. 93 113](#_Toc136511062)

[2.1.23 Zmiany w załącznikach do ustawy 114](#_Toc136511063)

[2.2 Zmiany w innych ustawach 114](#_Toc136511064)

[2.3 Pozostałe przepisy przejściowe i dostosowujące 115](#_Toc136511065)

[3 Pozostałe informacje 118](#_Toc136511066)

# Wstęp

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913), zwana dalej „ustawą o KSC”, uchwalona w 2018 r., tworzy podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym. Ustawa o KSC jest implementacją dyrektywy NIS[[1]](#footnote-2)).

Krajowy system cyberbezpieczeństwa tworzy wiele podmiotów, przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa informacji, a także obsługą incydentów. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów wskazanych w załączniku nr 1 do ustawy o KSC. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym”), który odpowiada za identyfikację i wyznaczanie operatorów usług kluczowych oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze.

Obecnie ani przedsiębiorcy telekomunikacyjni ani dostawcy usług zaufania nie są podmiotami krajowego systemu cyberbezpieczeństwa.

Incydenty wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także incydenty w podmiotach publicznych, są raportowane do jednego z trzech krajowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych dalej ,,CSIRT”). Do zadań zespołów CSIRT należy m.in. klasyfikowanie incydentów jako krytyczne. Ustawa usankcjonowała istnienie trzech zespołów na poziomie krajowym – CSIRT GOV (działającego w Agencji Bezpieczeństwa Wewnętrznego), CSIRT NASK (działającego w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, zwanym dalej „NASK-PIB”) oraz CSIRT MON (prowadzonego przez Ministra Obrony Narodowej). Zespoły CSIRT współpracują ze sobą w ramach Zespołu do spraw incydentów krytycznych.

Sektorowe zespoły cyberbezpieczeństwa

Organ właściwy może powołać sektorowy zespół cyberbezpieczeństwa. Zespół ten odpowiada za wsparcie obsługi incydentów u operatorów usług kluczowych w konkretnym sektorze lub podsektorze. Do tej pory powołano tylko jeden taki zespół, tj. CSIRT KNF (zespół dla sektora finansowego), funkcjonujący przy Komisji Nadzoru Finansowego[[2]](#footnote-3)).

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (zwany dalej ,,Pełnomocnikiem”) jest odpowiedzialny za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik, w randze ministra, sekretarza stanu albo podsekretarza stanu, jest powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań należy zarówno analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa (dokonywana na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT), jak i nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. Pełnomocnik jest ponadto odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa. Inicjuje także krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Kolegium do Spraw Cyberbezpieczeństwa

Kolegium do Spraw Cyberbezpieczeństwa (zwane dalej ,,Kolegium”) jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Kolegium opiniuje sprawy planowane do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 118 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (zwane dalej „Prawem telekomunikacyjnym”). Przewodniczącym Kolegium jest Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego oraz Sekretarz Kolegium. W posiedzeniach Kolegium uczestniczą także: Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK-PIB. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów, w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa, może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa.

Potrzeba i cele projektu ustawy nowelizującej

Ustawa, kształtując krajowy system cyberbezpieczeństwa, umożliwiła podjęcie prac nad jego dalszym rozwojem. Doświadczenia zebrane na przestrzeni lat funkcjonowania tego systemu w Polsce wskazują na konieczność wprowadzenia rozwiązań, wymagających dokonania zmian na poziomie ustawowym.

Mimo stworzonej przez obowiązujące przepisy możliwości powoływania sektorowych zespołów cyberbezpieczeństwa, zespoły takie nie były dotychczas powoływane. Wyjątek stanowi zespół, powołany przy Komisji Nadzoru Finansowego, dla najbardziej dojrzałego ze wszystkich sektorów, tj. sektora finansowego – CSIRT KNF. Zespół ten powstał w oparciu o wewnętrzne środki i zasoby kadrowe Urzędu Komisji Nadzoru Finansowego. Funkcjonowanie tego zespołu wskazuje, że ustanowienie CSIRT sektorowych dla każdego z kluczowych sektorów polskiej gospodarki ma kluczowy wpływ na podniesienie skuteczności reagowania na incydenty. Dzięki temu operatorzy usług kluczowych będą w stanie szybciej i bardziej efektywnie radzić sobie z incydentami, gdyż otrzymają bezpośrednie wsparcie w reagowaniu na incydenty.

Zauważono także potrzebę zwiększenia zakresu uprawnień Pełnomocnika w obszarze zapewniania koordynacji współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa, której wzmocnienie jest niezbędne z punktu widzenia zwiększenia efektywności odpowiedzi na nowe cyberzagrożenia, a także jest zgodne z oczekiwaniem ustawodawcy co do koordynacyjnej funkcji Pełnomocnika.

Jednym z najczęściej występujących problemów związanych z funkcjonowaniem krajowego systemu cyberbezpieczeństwa jest brak powołania przez operatorów usług kluczowych odpowiednio ukształtowanych struktur odpowiedzialnych za cyberbezpieczeństwo. Do problemów utrudniających skuteczną obsługę incydentów należą także: nieodpowiadający faktycznym potrzebom zakres posiadanych przez pracowników operatora kwalifikacji oraz ograniczony dostęp do informacji o cyberzagrożeniach.

Wyniki przeprowadzonych na zlecenie Ministra Cyfryzacji analiz wskazują na zróżnicowany, często wywołujący zastrzeżenia, poziom zabezpieczeń e-usług oferowanych przez samorządy. Potwierdzeniem są ustalenia pokontrolne zawarte w wystąpieniu pokontrolnym Najwyższej Izby Kontroli z 2019 r., z którego wynika, że negatywnie oceniono aż 70% kontrolowanych jednostek samorządu terytorialnego w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji[[3]](#footnote-4)). NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji.

W kontekście podnoszenia poziomu cyberbezpieczeństwa kluczowe znaczenie ma zapewnienie dostępu do wiedzy eksperckiej dotyczącej cyberzagrożeń. Jednym ze sposobów na zapewnienie takiego dostępu jest tworzenie ISAC. Pierwsze ISAC (eng. *Information Sharing and Analysis Center*) powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku. ISAC gromadzi informacje o podatnościach i cyberzagrożeniach, a następnie przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w systemie wymiany takich informacji. Taka formuła współpracy znacząco wpływa na poprawę cyberbezpieczeństwa i jest praktykowana w państwach Unii Europejskiej.

Przykładem sektorowego ISAC na poziomie europejskim jest *European Energy Information Sharing & Analysis Centre* (EE ISAC)[[4]](#footnote-5)). Został on zorganizowany z inicjatywy przemysłu energetycznego. W ramach EE ISAC wymieniają informacje dostawcy usług, przedsiębiorstwa użyteczności publicznej, instytucje naukowe, organizacje rządowe i pozarządowe (m.in. członkiem EE ISAC są Polskie Sieci Elektroenergetyczne Spółka Akcyjna). W Europie działa również amerykański *Financial Services Information Sharing and Analysis Center[[5]](#footnote-6)),* zrzeszający około 7 000 instytucji finansowych z całego świata.

Również zdaniem ENISA do prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym a prywatnym[[6]](#footnote-7)). Centra ISAC stanowią platformę takiej współpracy zapewniając wymianę informacji na temat przyczyn, incydentów, cyberzagrożeń, jak również dzielenie się doświadczeniem, wiedzą i analizami.

Rozporządzenie w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013[[7]](#footnote-8))), zwane dalej „Aktem o cyberbezpieczeństwie”, zachęca do tworzenia ISAC[[8]](#footnote-9)).

Do tej pory powstało w Polsce tylko jedno centrum wymiany informacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa. Wskazane jest, aby w Polsce powstało więcej organizacji ISAC, co zdecydowanie powinno przyczynić się do ułatwienia dostępu do specjalistycznej wiedzy i do wymiany informacji o stosowanych rozwiązaniach, tzw. dobrych praktykach.

Coraz większe znaczenie dla bezpieczeństwa usług kluczowych ma niezawodność usług telekomunikacyjnych. Stacjonarne sieci szerokopasmowe są uzupełniane przez sieci mobilne nowej generacji (sieci 5G i kolejnych generacji). Komisja Europejska wielokrotnie, m.in. w opublikowanych w marcu 2019 r. zaleceniach dot. cyberbezpieczeństwa sieci 5G, podkreślała, że kwestia zapewnienia bezpieczeństwa wdrażanej technologii 5G jest priorytetem. Potwierdzenie tego znajduje swój wymiar w opublikowanym w styczniu 2020 r. zestawie środków dot. minimalnej harmonizacji i standaryzacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G, określanym jako 5G Toolbox[[9]](#footnote-10)). Zestaw obejmuje zarówno rozwiązania o charakterze strategicznym, technicznym, jak i o charakterze wspierającym. Celami zestawu narzędzi są, po pierwsze, bezpieczeństwo sieci 5G, a po drugie – uspójnienie polityk państw członkowskich w obszarze bezpieczeństwa technologii 5G. 5G Toolbox definiuje zestaw środków zabezpieczających na poziomie strategicznym i technicznym oraz wskazuje działania wspierające stosowanie tych środków, niezbędne do ograniczenia ryzyk cyberbezpieczeństwa w sieciach 5G, które będą „kręgosłupem” Jednolitego Rynku Cyfrowego UE. Wśród opisanych w 5G Toolbox środków są środki o charakterze:

* strategicznym – m.in. większe uprawnienia dla organów właściwych, w tym w zakresie oceny bezpieczeństwa łańcucha dostaw, większe wymagania dla przedsiębiorców telekomunikacyjnych oraz ocena ryzyka dostawców sprzętu lub oprogramowania,
* technicznym – m.in. badanie bezpieczeństwa oprogramowania i urządzeń – czego odzwierciedleniem są na gruncie prawa krajowego uprawnienia Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz zespołów CSIRT poziomu krajowego: CSIRT GOV, CSIRT MON, CSIRT NASK, wynikające z art. 33 ustawy o KSC,
* wspierającym – m.in. dotyczące prac nad europejskim programem standaryzacji i certyfikacji cyberbezpieczeństwa.

Wprowadzenie zmian do ustawy o KSC jest elementem działań na rzecz wdrożenia zaleceń z 5G Toolbox w Polsce.

Europejski Kodeks Łączności Elektronicznej (EKŁE)[[10]](#footnote-11)) umożliwia (w odróżnieniu od poprzedniej regulacji tzw. dyrektywy ramowej) uspójnienie procedury zgłaszania i reagowania na incydenty na poziomie krajowym. Na możliwość zharmonizowania procedury zgłaszania incydentów w rozumieniu ustawy o KSC z incydentami raportowanymi przez przedsiębiorców telekomunikacyjnych wskazuje się także w opublikowanym eksperckim opracowaniu *Synergies in Cybersecurity Incident Reporting*[[11]](#footnote-12)*)*. Jest to dokument przygotowany przez Grupę Współpracy NIS we współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (zwaną dalej „ENISA”) oraz Komisją Europejską. W opracowaniu tym wprost wskazano, że państwa mogą dokonać harmonizacji procedur z dyrektywy NIS, EKŁE oraz rozporządzenia eIDAS, dzięki m.in. posiadaniu podobnych założeń w klasyfikacji incydentów, określaniu progów incydentów. Co więcej, podkreślono fakt, że usługi objęte tymi trzema reżimami prawnymi mają krytyczne znaczenie dla społeczeństwa.

Jak już wspomniano wcześniej, sieć 5G będzie jednym z kluczowych elementów mających znaczenie cyberbezpieczeństwa na poziomie państwa. W związku z tym, kwestie związane z budową i funkcjonowaniem sieci 5G nie mogą zostać pominięte w kształtowaniu otoczenia prawnego funkcjonowania krajowego systemu cyberbezpieczeństwa, którego celem jest zapewnienie tego bezpieczeństwa. Ponadto, sieć 5G będzie miała kluczowe znaczenie dla funkcjonowania wszystkich sektorów gospodarki. Pozostawienie jej (podmiotów świadczących dostarczających sieci 5G, czyli operatorów telekomunikacyjnych) poza krajowym systemem cyberbezpieczeństwa znacząco ograniczyłoby możliwość reagowania na pojawiające się cyberzagrożenia.

Obecnie funkcjonują odrębne systemy zgłaszania naruszeń (jak określane są incydenty telekomunikacyjne w obowiązującym Prawie telekomunikacyjnym) przez przedsiębiorców telekomunikacyjnych oraz incydentów przez operatorów usług kluczowych. Przedsiębiorcy telekomunikacyjni zgłaszają naruszenia do Prezesa Urzędu Komunikacji Elektronicznej, podczas gdy operatorzy usług kluczowych zgłaszają incydenty bezpośrednio do właściwych CSIRT’ów. Proponowane w projekcie ustawy zmiany usprawnią przepływ informacji o naruszeniach - incydentach. Stworzony zostanie jednolity system oraz ujednolicone zostaną procedury w zakresie reagowania na incydenty. Rolę koordynacyjną w tym systemie pełnić będą CSIRT poziomu krajowego, każdy w obrębie swojej właściwości podmiotowej.

Bezpieczeństwo sektora telekomunikacji ma wpływ na poprawne funkcjonowanie innych sektorów gospodarki. Incydent telekomunikacyjny może łatwo spowodować np. niedostępność usług bankowych, a więc wstrzymać wykonywanie usług w innym sektorze. W związku z powyższym w projekcie ustawy wprowadzono rozwiązania zwiększające przepływ informacji o incydentach, dzięki którym zarówno CSIRT’y poziomu krajowego, jak i operatorzy usług kluczowych będą sprawniej uzyskiwali informacje o incydentach występujących w innych sektorach. Warto podkreślić, że zespoły CSIRT odpowiadają za szacowanie ryzyka na poziomie krajowym, związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami. Dzięki projektowanym zmianom uzyskają pełen obraz cyberbezpieczeństwa na poziomie krajowym.

Jednocześnie projektowane zmiany umożliwią podłączanie się przedsiębiorców komunikacji elektronicznej do systemu do zgłaszana i reagowania na incydenty, rozwijanego przez ministra właściwego ds. informatyzacji, czyli systemu S46.

Krajowy system certyfikacji cyberbezpieczeństwa

W związku z rosnącą liczbą zagrożeń w cyberprzestrzeni oraz coraz istotniejszą rolą systemów informacyjnych w życiu społeczeństwa, konieczne jest zapewnienie sprawdzonych i bezpiecznych rozwiązań technologicznych zarówno dla sektora publicznego, jak i prywatnego.

Należy także zwrócić uwagę na wzrost liczby cyberprzestępstw, zwłaszcza związanych z wykorzystaniem złośliwego oprogramowania, takiego jak ransomware. Jednym z instrumentów sprzyjających ograniczaniu tego wzrostu jest zapewnienie każdemu zainteresowanemu dostępu do technologii umożliwiających bezpieczne przetwarzanie danych.

Ze względu na wielką różnorodność wykorzystywanych technologii, istotne jest stosowanie jednolitych standardów w zakresie bezpieczeństwa na terenie całej Unii Europejskiej.

Proponowane w ustawie rozwiązania tworzą prawno-organizacyjne warunki funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa, który zapewni wszystkim zainteresowanym podmiotom możliwość testowania, badania produktów ICT, usług ICT i procesów ICT oraz otrzymywania certyfikatów cyberbezpieczeństwa opartych na europejskich programach, a także powszechnie uznawanych na obszarze Unii Europejskiej.

Stworzenie takiego systemu wynika również z bezwzględnie obowiązujących przepisów prawa europejskiego, zawartych w Akcie o cyberbezpieczeństwie. Akt o Cyberbezpieczeństwie z 2018 r. ustanowił europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów.

Akt o cyberbezpieczeństwie nakłada na wszystkie państwa członkowskie obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa, który będzie nadzorował rynek i kontrolował prawidłowość działań w zakresie certyfikacji. W celu wdrożenia rozwiązań przewidzianych w tym akcie normatywnym w Polsce, konieczne jest również wprowadzenie do polskiego systemu prawa przepisów związanych z akredytacją podmiotów uprawnionych do wydawania certyfikatów oraz procedur związanych z działaniem tego systemu, regulujących np. kwestie zatwierdzania certyfikatów o poziomie zaufania „wysoki”.

Przyjęte w ustawie rozwiązania sprawią, że polskie firmy będą mogły swobodnie konkurować na rynku europejskim. Trzeba tu wskazać, że w wielu państwach Europy Środkowej rynek certyfikacji jest mniej rozwinięty niż w Polsce. W związku z tym, przyjęcie procedowanych przepisów może umożliwić polskim przedsiębiorcom przyciągnięcie klientów z regionu.

Przyjęte rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja w dziedzinie cyberbezpieczeństwa będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku.

Certyfikaty

Akt o cyberbezpieczeństwie przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, określające poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. W odniesieniu do każdego z tych poziomów będą określane odrębne wymagania, jakie musi spełniać produkt, by uzyskać certyfikat danego poziomu. Wymagania dla konkretnych produktów będą określane w europejskich lub krajowych programach certyfikacji cyberbezpieczeństwa. Każdy z wydawanych certyfikatów będzie musiał wskazywać jakiego poziomu dotyczy. Również szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji.

Certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym. Ustawa tworzy ramy w jakich będzie wykonywana, równocześnie nie nakładając żadnych obowiązków na podmioty działające na rynku. Każdy chętny będzie więc mógł zarówno rozpocząć działalność w tym zakresie, jak i uzyskać certyfikację swojego produktu, usługi czy procesu ICT, równocześnie nie będąc do tego zobowiązanym.

Przyjęte rozwiązania służą również realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią”. Ustanowienie krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa stanowią działania służące realizacji drugiego celu szczegółowego Strategii – podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. W zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy z dnia 13 kwietnia 2016 r**.** o systemie oceny zgodności i nadzoru rynku (Dz. U. 2022 r. poz. 1854). Stosowane przepisy proceduralne będą więc dobrze znane i sprawdzone, a nowym elementem będą jedynie wymagania określane dla każdego z poziomów zaufania.

Podjęcie prac związanych z utworzeniem krajowego systemu certyfikacji cyberbezpieczeństwa wynika z jednej strony zarówno z potrzeby dania impulsu do rozwoju rynku w obszarze certyfikacji, jak i zapewnienie bezpiecznych technologii dla zainteresowanych, a z drugiej strony, z konieczności wdrożenia do polskiego porządku prawnego Aktu o cyberbezpieczeństwie.

Strategiczna sieć bezpieczeństwa

Dotychczasowe doświadczenia, jak również różnorodność stosowanych rozwiązań, a co za tym idzie rozproszenie środków, które są wykorzystywane do modernizacji istniejących sieci telekomunikacyjnych, wykorzystywanych na potrzeby realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego przez kluczowe urzędy i podmioty działające w Rzeczypospolitej Polskiej wskazują na konieczność uruchomienia bezpiecznej sieci telekomunikacyjnej.

Szczególne zasady przeznaczania określonego zasobu z pasma 700 MHz

Decyzja harmonizacyjna (Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii) wskazuje wyraźnie, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa Public Protection & Disaster Relief (PPDR), należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.

**Zgodność projektu ustawy z celami strategicznymi Rady Ministrów**

Projekt ustawy służy realizacji celów Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią”, jakimi są podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym. Projekt realizuje także cel szczegółowy Strategii, odnoszący się do rozwoju krajowego systemu cyberbezpieczeństwa poprzez ewaluację przepisów prawa dotyczących cyberbezpieczeństwa. Ponadto, projekt realizuje cele Strategii w odniesieniu do zapewnienia bezpieczeństwa łańcucha dostaw i utworzenia krajowego systemu certyfikacji cyberbezpieczeństwa.

Jednocześnie wprowadzenie w życie projektowanych zmian w ustawie o krajowym systemie cyberbezpieczeństwa zrealizuje kamień milowy reformy C3.1. Krajowego Planu Odbudowy. Zgodnie z tym wymogiem wprowadzone zostaną ramy prawne umożliwiające tworzenie sektorowych sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), tworzenie Centrów Wymiany i Analizy Informacji (ISAC) oraz wzmocni mechanizmy współpracy administracji rządowej z jednostkami samorządu terytorialnego w zakresie reagowania na incydenty bezpieczeństwa.

**Zmiany wprowadzane do krajowego systemu cyberbezpieczeństwa**

CSIRT sektorowy

Sektorowy zespół cyberbezpieczeństwa zastąpiono CSIRT sektorowymi. W przeciwieństwie do dotychczasowego, fakultatywnego trybu ustanawiania zespołu, w projekcie przewidziano obowiązek ustanowienia przez organ właściwy CSIRT sektorowego dla danego sektora lub podsektora.

CSIRT sektorowy będzie odpowiadał za przyjmowanie zgłoszeń o incydentach pochodzących od operatorów usług kluczowych w danym sektorze lub podsektorze, dla którego został ustanowiony, a także za reagowanie na zgłoszone incydenty. Zakres obowiązków zostanie zatem poszerzony w stosunku do dotychczasowych rozwiązań – obecnie sektorowy zespół cyberbezpieczeństwa wspiera jedynie operatorów usługi kluczowej w reagowaniu na incydenty. CSIRT sektorowy będzie dokonywał również dynamicznej analizy ryzyka i incydentów, a także będzie gromadził informacje o cyberzagrożeniach.

CSIRT INT

W związku z rosnącą liczbą cyberataków na jednostki sektora publicznego konieczne jest dodatkowe wzmocnienie podmiotów z tego sektora. Szczególnie narażone na ataki są placówki dyplomatyczne i konsularne, których położenie i wrażliwy charakter przetwarzanych przez nie informacji sprawia, że udzielenie im wsparcia jest szczególnie utrudnione. Wychodząc naprzeciw tym problemom, powołuje się CSIRT INT, który będzie prowadzony przez szefa Agencji Wywiadu. Jego zadaniem będzie zapewnienie wsparcia placówkom dyplomatycznym i konsularnym w zakresie cyberbezpieczeństwa.

ISAC

Centra Wymiany i Analiz Informacji tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, mają być jednostkami wspierającymi podmioty krajowego systemu cyberbezpieczeństwa. Ich zadaniem będzie analiza informacji o cyberzagrożeniach i podatnościach oraz wymiana informacji o najlepszych praktykach.

SOC

Do krajowego systemu cyberbezpieczeństwa wprowadzono pojęcie Operacyjnych Centrów Bezpieczeństwa (zwanych dalej ,,SOC”). Te nowe podmioty zastąpią dotychczasowe struktury odpowiedzialne za cyberbezpieczeństwo u operatorów usług kluczowych. SOC posiadają ugruntowaną na rynku pozycję zespołów realizujących wszystkie funkcje związane z monitorowaniem i zarządzaniem cyberbezpieczeństwem, zarówno w strukturze wewnętrznej, jak i usług świadczonych na rzecz innych jednostek.

Włączenie przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa

Wymaganiami w zakresie cyberbezpieczeństwa zostaną objęci przedsiębiorcy komunikacji elektronicznej przez których rozumie się przedsiębiorców telekomunikacyjnych lub podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów.

Procedura uznania dostawcy za dostawcę wysokiego ryzyka

Odporność na cyberzagrożenia zależy w dużym stopniu od bezpieczeństwa sprzętu ICT, procesów ICT i usług ICT. Dotyczy to zarówno systemów teleinformatycznych, sieci telekomunikacyjnych, jak i przemysłowych systemów sterowania. Z tego względu w projekcie ustawy uwzględniono postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania wykorzystywanego przez kluczowe podmioty gospodarki za dostawcę wysokiego ryzyka. Postępowanie w tej kwestii będzie prowadził minister właściwy do spraw informatyzacji. Postępowanie będzie oparte o transparentną procedurę określoną w Kodeksie postępowania administracyjnego z pewnymi odmiennościami. Każdorazowo, prowadząc postępowanie, minister właściwy do spraw informatyzacji będzie zasięgał opinii Kolegium na temat dostawcy sprzętu lub oprogramowania i dostarczanych przez niego produktów ICT, usług ICT, procesów ICT. W opinii będą uwzględniane zarówno aspekty techniczne, jak i pozatechniczne, mające wpływ na bezpieczeństwo narodowe. Postępowanie będzie kończyło się decyzją administracyjną w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, która będzie podlegać zaskarżeniu do sądu administracyjnego.

Projektowane rozwiązanie nawiązuje do oceny profili ryzyka dostawców, będącej jednym z narzędzi strategicznych (Strategic Measure – SM03), uzgodnionych przez państwa członkowskie Unii Europejskiej, Komisję Europejską i ENISA w 5G Toolbox.

Podmioty krajowego systemu cyberbezpieczeństwa (przede wszystkim operatorzy usług kluczowych, dostawcy usług cyfrowych) oraz przedsiębiorcy telekomunikacyjni będący dużymi przedsiębiorcami, w przypadku wydania decyzji zostaną zobowiązani do wycofania z użycia, określonego w decyzji, w sprzętu lub oprogramowania pochodzące od takiego dostawcy, w terminie 7 lat od wydania decyzji administracyjnej. Natomiast w przypadku gdy produkty, usługi i procesy ICT, objęte decyzją, znajdują się w zakresie objętym wykazem kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług, stanowiącym załącznik nr 3 do ustawy, przedsiębiorcy będą musieli wycofać je w ciągu 5 lat. Podkreślenia wymaga fakt, że obowiązkowi wycofania będą podlegały produkty, usługi i procesy ICT wskazane w decyzji ministra właściwego do spraw informatyzacji – a więc nie wszystkie produkty, usługi i procesy ICT oferowane przez dostawcę wysokiego ryzyka.

Zapobieganie incydentom krytycznym i zwiększenie skuteczności reagowania na incydenty krytyczne

W celu zapobiegania incydentom krytycznym i zwiększenia skuteczności reagowania na nie będą mogły być wydawane ostrzeżenia Pełnomocnika – w przypadku uzyskania informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego.

Krajowe programy certyfikacji cyberbezpieczeństwa

Projekt ustawy przewiduje tworzenie krajowych programów certyfikacji cyberbezpieczeństwa, na podstawie których przeprowadzana będzie certyfikacja. W programach zawarte zostaną techniczne standardy, które będą musiały spełniać produkty, usługi i procesy ICT. Ponadto, programy będą określały szczegóły związane z procesem certyfikacji, jak również procedury sanacyjne w przypadku, gdy po certyfikacji ujawnią się wady produktów. Wszystkie te elementy muszą być bardzo ściśle dostosowane do konkretnego produktu, usługi czy procesu ICT. Na etapie planowania prac minister właściwy do spraw informatyzacji będzie mógł zlecić przygotowanie ekspertyz, opinii czy projektów dokumentacji podmiotom prywatnym. Pozwoli to wykorzystać wiedzę i doświadczenie podmiotów prywatnych przy przygotowywaniu projektu krajowego programu certyfikacji cyberbezpieczeństwa. Ponadto, narzędzia te będę również służyły zbadaniu czy w danym obszarze przygotowanie takiego programu byłoby w zasadne. W szczególności może on powierzyć przygotowanie takiego projektu jednostkom przez siebie nadzorowanym np. Naukowej i Akademickiej Sieci Komputerowej czy Instytutowi Łączności. Następnie, w ramach zwykłej procedury legislacyjnej, będzie przygotowywane rozporządzenie Rady Ministrów, ustanawiającego dany program. Na tym etapie możliwość wypowiedzenia się o kształcie danego programu będzie miał każdy zainteresowany organ administracji publicznej (art. 59d).

Elementy programu zostały sformułowane na wzór przepisów Aktu o cyberbezpieczeństwie, dotyczących europejskich programów certyfikacji cyberbezpieczeństwa. Dzięki temu wymagania i standardy wobec krajowych i europejskich programów certyfikacji będą bardzo do siebie zbliżone, co sprawi, że nie będzie konieczne tworzenie osobnej terminologii dla krajowych programów certyfikacji. Umożliwi to więc wykorzystanie w jak największym stopniu praktyk wypracowanych w ramach europejskich programów certyfikacji. Ponadto, certyfikaty cyberbezpieczeństwa wydane na podstawie krajowych programów certyfikacyjnych będą mogły, dzięki przyjętym rozwiązaniom, łatwo zostać uznane w innych krajach UE. Możliwe także będzie rozszerzenie rynku certyfikacji przez objęcie programami produktów, usług i procesów ICT nieujętych w europejskich programach certyfikacyjnych. Bliskość z programami europejskimi umożliwi też stosunkowo łatwe przenoszenie programów krajowych na poziom europejski. Będzie to bardzo ważnym narzędziem do kreowania polskiej polityki w zakresie certyfikacji cyberbezpieczeństwa na poziomie europejskim (art. 59 d–g).

Proces certyfikacji będzie prowadzony przez jednostki oceniające zgodność akredytowane przez Polskie Centrum Akredytacji na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i systemach nadzoru rynku. Wykorzystanie już obowiązujących przepisów zapewni możliwie najsprawniejsze wprowadzenie w życie systemu certyfikacji cyberbezpieczeństwa. Polskie Centrum Akredytacji będzie sprawowało nadzór nad akredytacją jednostek oceniających zgodność. Będzie też na bieżąco wymieniać się informacjami z ministrem właściwym do spraw informatyzacji, co zapewni skuteczną kontrolę nad całym systemem (art. 59h).

W przypadku certyfikatów odwołujących się do najniższego z poziomów uzasadnienia zaufania, sami dostawcy sprzętu lub oprogramowania będą mogli wydawać deklaracje zgodności, by wskazać, że ich produkt spełnia dane wymagania (art. 59p–r). Dostawcy sprzętu lub oprogramowania uzyskają zatem możliwość skorzystania z programów certyfikacyjnych przy jednoczesnym ograniczeniu kosztów uczestnictwa w tych programach.

Strategiczna sieć bezpieczeństwa

W projekcie ustawy przewidziano utworzenie bezpiecznej sieci telekomunikacyjnej na potrzeby realizacji przez kluczowe organy i podmioty działające w Rzeczypospolitej Polskiej zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, a także określono sposób powołania operatora tej sieci oraz warunki, które musi spełniać ten podmiot.

W tym celu zostanie powołany operator strategicznej sieci bezpieczeństwa, który będzie wyznaczany, przez Prezesa Rady Ministrów spośród podmiotów spełniających łącznie następujące warunki:

1. będących jednoosobową spółką Skarbu Państwa,
2. będących przedsiębiorcą telekomunikacyjnym,
3. posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań, o których mowa w art. 76d ust. 1 lub które zobowiązały się do jej pozyskania,
4. posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
5. posiadających świadectwo bezpieczeństwa przemysłowego
6. dających rękojmię należytego wykonywania zadań operatora strategicznej sieci bezpieczeństwa.

Operator ten będzie świadczył usługi telekomunikacyjne, jak również inne usługi dla wskazanych w ustawie podmiotów. Do ustawy wprowadzono możliwość pierwokupu przez OSSB sieci telekomunikacyjnych pozostających we własności Skarbu Państwa lub samorządu terytorialnego. Przyjęcie takiego rozwiązania zapewni sprawną i zoptymalizowaną kosztowo budowę infrastruktury telekomunikacyjnej, wykorzystywanej na potrzeby realizacji zadań, o których mowa powyżej.

Zmiana podziału ustawy w związku z rozbudową aktu normatywnego

Znacznemu poszerzeniu, w stosunku do obowiązującej ustawy, ulega jej zakres przedmiotowy. Wprowadzenie do ustawy o krajowym systemie cyberbezpieczeństwa przepisów kształtujących krajowy system certyfikacji cyberbezpieczeństwa oraz rozwiązań związanych z utworzeniem i funkcjonowaniem strategicznej sieci bezpieczeństwa, jak również obszerność wprowadzanych zmian, powodują, że niezbędne jest dokonanie podziału ustawy na działy, co służy zachowaniu przejrzystości ustawy. W konsekwencji ustawa została podzielona na cztery działy. Pierwszy dział zawiera ogólne postanowienia, drugi – przepisy dotyczące krajowego systemu cyberbezpieczeństwa, które stanowią niezmiennie podstawową regulację ustawy, wraz z postanowieniami odnoszącymi się do nowego zespołu norm prawnych określających „krajowy system certyfikacji cyberbezpieczeństwa”. Trzeci dział składa się z przepisów dotyczących funkcjonowania strategicznej sieci bezpieczeństwa, zaś czwarty to przepisy końcowe.

Przewidywane skutki społeczne, gospodarcze, prawne i finansowe wprowadzanych zmian

Skutki społeczne

Dzięki wprowadzanym rozwiązaniom, obejmującym utworzenie CSIRT sektorowych, SOC zewnętrznych, SOC wewnętrznych i ISAC, zostanie zwiększona skuteczność funkcjonowania krajowego systemu cyberbezpieczeństwa.

Powołanie CSIRT sektorowych pozwoli na utworzenie jednostek, dzięki którym usprawnione zostanie funkcjonowanie i zwiększona skuteczność systemu reagowania na incydenty. Ponadto, dzięki powołaniu CSIRT sektorowego w każdym sektorze powstanie baza wiedzy o cyberzagrożeniach i podatnościach danego sektora. Funkcjonowanie CSIRT sektorowych wpłynie na skrócenie czasu obsługi incydentów w sektorze, które będą obsługiwane z uwzględnieniem szczególnych uwarunkowań danego sektora. Natomiast centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa.

Przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw i skłoni przedsiębiorców do stosowania bezpieczniejszych, sprawdzonych rozwiązań. To z kolei, dzięki zwiększeniu zakresu wykorzystania rozwiązań odpornych na cyberataki, będzie służyło podniesieniu poziomu bezpieczeństwa obywateli.

Skutki gospodarcze

Celem projektowanych zmian jest wzmocnienie krajowego systemu cyberbezpieczeństwa. Wprowadzane projektem ustawy rozwiązania zobowiązują bowiem m.in. przedsiębiorców świadczących usługi kluczowe do dbania o cyberbezpieczeństwo. Skutkiem projektowanych przepisów może być konieczność poniesienia dodatkowych kosztów związanych z dostosowaniem się poszczególnych podmiotów krajowego systemu cyberbezpieczeństwa do wymogów wynikających z ustawy. Na marginesie należy zauważyć, że wielu przedsiębiorców już obecnie posiada operacyjne centra bezpieczeństwa, bowiem podobny do projektowanego wymóg istnieje w obowiązującej ustawie. Dzięki dalszemu inwestowaniu przez podmiot we własne cyberbezpieczeństwo zyskuje on zaufanie podmiotów, którym świadczy usługi i potencjalnych kontrahentów.

Dostosowanie się do nowych wymogów pozwoli przedsiębiorcom zwiększyć skuteczność działań podejmowanych przez przedsiębiorców w zakresie cyberbezpieczeństwa w ich działalności, co przełoży się na bezpieczne prowadzenie biznesu i minimalizację ryzyka strat.

Dzięki zawartym w ustawie rozwiązaniom podniesione zostaną standardy w zakresie cyberbezpieczeństwa. Prywatni przedsiębiorcy będą mieli ułatwiony wybór bezpiecznych rozwiązań technologicznych. Ponadto, nowe regulacje gwarantują, że certyfikaty uzyskane w ramach systemu certyfikacji dla produktów, usług czy procesów ICT będą honorowane na terenie całej Unii Europejskiej. Projektowana ustawa zawiera szereg rozwiązań zapewniających właściwe standardy postępowania przy ocenie zgodności, co daje dodatkowe gwarancje jakości.

Krajowy system certyfikacji cyberbezpieczeństwa będzie też stanowił cenne uzupełnienie krajowego systemu cyberbezpieczeństwa. Stworzy bowiem precyzyjny system oceny produktów ICT, dzięki czemu identyfikowane będą produkty spełniające najlepsze standardy w dziedzinie bezpieczeństwa. Projektowane przepisy nie nakładają żadnych dodatkowych obowiązków na podmioty niezainteresowane uczestnictwem w tym systemie. Przyjęty model nie tworzy też barier dostępu do rynku.

Skutki finansowe

Tworzenie nowych struktur w ramach krajowego systemu cyberbezpieczeństwa będzie wymagało dodatkowych nakładów finansowych. Należy jednak podkreślić, że jest to inwestycja w bezpieczeństwo państwa. Incydenty bezpieczeństwa komputerowego są coraz częstsze i bardziej zaawansowane. Drastycznie wzrosła liczba incydentów cyberbezpieczeństwa oraz samych cyberataków, których ofiarami padają urzędy, szpitale, ale także coraz więcej ataków obserwujemy w sektorze prywatnym oraz w stosunku do obywateli. W 2021 r. zespół CSIRT NASK obsłużył 29 483 unikalnych incydentów. Jest to znaczący wzrost w stosunku do 2019 r., w którym CSIRT NASK odnotował 10 420 incydenty. Istnieje także stałe zagrożenie działaniami wywiadowczymi w cyberprzestrzeni.

Szkody powstałe wskutek tych działań (np. zaszyfrowanie danych, wykradzenie danych, uniemożliwienie lub utrudnienie świadczenia usług publicznych) są bardzo poważne i bardzo często mają również istotny wymiar finansowy. Inwestycja w dostosowanie krajowego systemu cyberbezpieczeństwa do wyzwań wynikających z postępującej gwałtownie cyfryzacji pozwoli ograniczyć prawdopodobieństwo powstania tych szkód, a w przypadku ataków – znacząco zmniejszyć ich negatywne skutki. Wobec powyższego poniesienie dodatkowych nakładów finansowych jest jak najbardziej zasadne.

Przyjęcie przepisów o krajowym systemie certyfikacji cyberbezpieczeństwa będzie miało korzystne skutki dla całego sektora przedsiębiorstw. Obecnie firmy ponoszą coraz większe straty w wyniku działalności cyberprzestępców. Wprowadzenie certyfikacji w dziedzinie cyberbezpieczeństwa sprawi, że firmy uzyskają lepszy dostęp do rozwiązań gwarantujących najwyższy poziom bezpieczeństwa. Ponadto, samo zbudowanie systemu certyfikacji cyberbezpieczeństwa przyczyni się do wzrostu świadomości w omawianym obszarze. W efekcie straty ponoszone przez sektor przedsiębiorstw powinny ulec zmniejszeniu.

Skutki prawne

Powstaną nowe rejestry pomagające właściwym instytucjom wykonywać ich zadania ustawowe – wykaz SOC oraz wykaz ISAC.

Minister właściwy do spraw informatyzacji będzie mógł przeprowadzić postępowanie w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

Pełnomocnik Rządu do spraw Cyberbezpieczeństwa oraz minister właściwy do spraw informatyzacji uzyskają nowe narzędzia w zakresie zapobiegania cyberzagrożeniom i zwiększenia skuteczności reagowania na incydenty krytyczne. Również przewodniczący Kolegium do spraw Cyberbezpieczeństwa zostanie wyposażony w szereg nowych kompetencji (m.in. będzie mógł wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1 ustawy; zlecić CSIRT GOV CSIRT MON lub CSIRT NASK przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług albo analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT; będzie również mógł wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka).

Krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował:

* uprawnieniami do nadzoru nad systemem certyfikacji cyberbezpieczeństwa oraz
* narzędziami do usuwania z obiegu prawnego certyfikatów wydanych wbrew przepisom ustawy oraz do kontrolowania podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Ponadto, przepisy ustanawiają podstawę prawną i procedury przyjmowania krajowych programów certyfikacji cyberbezpieczeństwa.

Niniejszą ustawą zostaną zmienione następujące ustawy:

* ustawa z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym[[12]](#footnote-13)) – do katalogu spółek w których nie mogą być zbyte akcje lub prawa z akcji należące do Skarbu Państwa zostanie dodana spółka wyznaczona na operatora strategicznej sieci bezpieczeństwa.

Źródła finansowania projektowanych zmian

Wejście w życie projektowanej regulacji będzie stanowić podstawę do ubiegania się o dodatkowe środki z budżetu państwa. Szczegółowy opis źródeł finansowania zawarty jest w ocenie skutków regulacji.

Wyniki przeprowadzonych konsultacji

W dniach 30.06–8.07.2020 r. przeprowadzone zostały prekonsultacje robocze w ramach zespołu doraźnego Kolegium ds. Cyberbezpieczeństwa. Swoje uwagi zgłosiło Ministerstwo Obrony Narodowej, Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy i Prezes Urzędu Komunikacji Elektronicznej.

W wyniku zgłoszonych uwag projekt został przeredagowany i przeprowadzono drugą turę prekonsultacji w ramach zespołu doraźnego Kolegium.

W ramach konsultacji publicznych skierowano zaproszenie do przedstawienia stanowisk do 51 podmiotów, wyznaczając termin 14 dni. Jednakże,   z uwagi na prośby ze strony partnerów społecznych, Minister Cyfryzacji (pismem z 17 września 2020 r.) przedłużył czas na zgłaszanie uwag o kolejne 14 dni – łącznie na uwagi było 28 dni.

Konsultacje publiczne oraz opiniowanie odbyły się w terminie od 8 września do 6 października 2020 r., przy czym przyjmowano także uwagi przesłane w późniejszym terminie, o ile zgłaszający uwagi przekazał informację o zamiarze ich zgłoszenia przed upływem terminu wyznaczonego na przeprowadzenie konsultacji publicznych.

# Uzasadnienie poszczególnych przepisów

## Zmiany w ustawie o KSC

### Zmiany w definicjach, katalogu podmiotów krajowego systemu cyberbezpieczeństwa, zakresu przedmiotowego

Postanowienia ogólne zostają objęte zakresem działu pierwszego (przed art. 1 zostało dodane oznaczenie działu – Postanowienia ogólne). Nowelizacją są również wprowadzane zmiany w poszczególnych przepisach wchodzących w zakres tego działu.

#### Zmiany w art. 1

Wobec poszerzenia projektowaną ustawą zakresu przedmiotowego ustawy o krajowym systemie cyberbezpieczeństwa w art. 1 wprowadzono odpowiednie zmiany – w ust. 1 tego artykułu zostały dodane pkt 1a oraz 4–6, zgodnie z którymi zakres przedmiotowy ustawy obejmuje także:

* zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa sieci lub usług komunikacji elektronicznej i zgłaszania incydentów telekomunikacyjnych,
* krajowy system certyfikacji cyberbezpieczeństwa,
* zasady i tryb wyznaczania operatora strategicznej sieci bezpieczeństwa oraz jego zadania,
* zasady przyznania zasobów częstotliwości z zakresu 703–733 MHz oraz 758–788 MHz.

Dostosowaniu do projektowanych zmian o charakterze systemowym uległ art. 1 ust. 2. W związku z wynikającym z implementacji art. 40 i 41 EKŁE włączeniem do krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, konieczne jest uchylenie pkt 1 w art. 1 ust. 2, zgodnie z którym przepisów obowiązującej ustawy nie stosuje się do tych przedsiębiorców.

Jednocześnie projekt ustawy przewiduje, że do dostawców usług zaufania będą stosować się przepisy o ostrzeżeniu.

#### Nowe brzmienie art. 2

Uporządkowany i uzupełniony został słowniczek pojęć używanych w ustawie o krajowym systemie cyberbezpieczeństwa (art. 1 pkt 3 dotyczący art. 2 ustawy o krajowym systemie cyberbezpieczeństwa). Wprowadzone zostały do niego definicje takich pojęć, jak: akredytacja, certyfikat, cyberzagrożenie, deklaracja zgodności, dostawca, incydent telekomunikacyjny, ISAC, jednostka oceniająca zgodność, krajowy certyfikat cyberbezpieczeństwa, krajowa deklaracja zgodności, krajowy program certyfikacji cyberbezpieczeństwa, krajowy poziom uzasadnienia zaufania, obsługa incydentu, ocena zgodności, proces ICT, produkt ICT, przedsiębiorca komunikacji elektronicznej, SOC wewnętrzny, SOC zewnętrzny, usługa ICT, usługi komunikacji elektronicznej.

Definicja akredytacji (pkt 1) odwołuje się do akredytacji w rozumieniu art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93[[13]](#footnote-14)), zwane dalej „rozporządzeniem 765/2008”. Zgodnie z tym rozporządzeniem akredytacja oznacza poświadczenie przez krajową jednostkę akredytującą, że jednostka oceniająca zgodność spełnia wymagania określone w normach zharmonizowanych oraz – w stosownych przypadkach – wszelkie dodatkowe wymagania, w tym wymagania określone w odpowiednich systemach sektorowych konieczne do realizacji określonych czynności związanych z oceną zgodności.

Wprowadza się nową definicję bezpieczeństwa sieci lub usług komunikacji elektronicznej (pkt 2). Pod tym pojęciem rozumie się zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność integralność lub poufność tych sieci lub usług, jak i przetwarzanych informacji objętych tajemnicą komunikacji elektronicznej, a także innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy. Przepis stanowi wdrożenie art. 2 pkt 21 EKŁE.

Akt o cyberbezpieczeństwie wprowadził definicję cyberbezpieczeństwa, która różni się od tej stosowanej na gruncie obowiązującej ustawy. Z tego względu wprowadzono nową definicję cyberbezpieczeństwa, zgodną z Aktem o cyberbezpieczeństwie – są to działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami (pkt 11). Natomiast dotychczasowemu brzmieniu definicji cyberbezpieczeństwa odpowiada definicja bezpieczeństwa systemów informacyjnych (art. 2 pkt 3). Zmiany te nie powodują zmian w zakresie konkretnych obowiązków nałożonych obowiązującą ustawą na podmioty krajowego systemu cyberbezpieczeństwa. Nowe definicje są zgodne z przepisami zawartymi w Akcie o cyberbezpieczeństwie. Wprowadzane zmiany definicyjne nie tylko zapewniają zgodność z polskim porządkiem prawnym, ale również odpowiednią przejrzystość przepisów.

Ponadto, projektowana ustawa posługuje się pojęciami certyfikat (pkt 4) oraz krajowy certyfikat cyberbezpieczeństwa (pkt 25). Certyfikat odnosi się do wszystkich certyfikatów w dziedzinie cyberbezpieczeństwa, tj. zarówno tych wydanych w ramach krajowych, jak i europejskich programów certyfikacji. Z kolei krajowy certyfikat cyberbezpieczeństwa dotyczy tylko dokumentów wydanych na podstawie krajowych programów certyfikacji . Certyfikaty te będą traktowane jednakowo. Wiele kwestii związanych z europejskimi certyfikatami zostało określonych w Akcie o cyberbezpieczeństwie. Przepisy te nie odnoszą się jednak do certyfikatów krajowych. Z tego też względu w projekcie ustawy znalazły się przepisy regulujące kwestie związane z wydawaniem certyfikatów krajowych. Analogiczna sytuacja występuje w przypadku deklaracji zgodności i krajowych deklaracji zgodności (pkt 26). Te ostatnie zostały wprowadzone aby zagwarantować, że również w wypadku certyfikatów krajowych możliwe będzie potwierdzenie zgodności przez samego przedsiębiorcę w określonych przypadkach. Konsekwencją tych zmian była konieczność dostosowania pozostałych przepisów ustawy.

W niezmienionej formie pozostawiono dotychczasowe definicje zespołów CSIRT GOV, CSIRT MON oraz CSIRT NASK (pkt. 5–7).

Wprowadzono definicję CSIRT sektorowego (pkt 9) – przez który należy rozumieć Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora. Definicja ta jest utrzymana w podobnej konwencji jak definicje poszczególnych zespołów CSIRT poziomu krajowego.

Zaproponowano także definicję CSIRT INT (pkt 8) – jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, prowadzony przez Szefa Agencji Wywiadu na rzecz Agencji Wywiadu oraz jednostek organizacyjnych podległych ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowanych.

Wprowadzono również definicję CSIRT Telco (pkt 10) – jako Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego działającego na rzecz przedsiębiorców komunikacji elektronicznej.

Pojęcie „zagrożenie cyberbezpieczeństwa” zostało zastąpione pojęciem „cyberzagrożenia” (art. 2 pkt 12), które zostało wprowadzone w Akcie o cyberbezpieczeństwie, a jego definicja jest bardzo zbliżona do funkcjonującej w naszym systemie prawnym definicji „zagrożenia cyberbezpieczeństwa”. Nie jest zasadne utrzymywanie w systemie prawnym obu tych pojęć i dlatego pozostawiono jedynie sformułowanie „cyberzagrożenie”. Pojęcie „cyberzagrożenie” jest zgodne z najnowszą terminologią w dziedzinie cyberbezpieczeństwa stosowaną w państwach członkowskich Unii Europejskiej. W związku z tą zmianą dostosowano definicję podatności (art. 2 pkt 31) zastępując wyrazy „zagrożenie cyberbezpieczeństwa” wyrazem „cyberzagrożenie”.

Definicja dostarczania sieci telekomunikacyjnej (pkt 14) odwołuje się do definicji z art. 2 pkt 5 ustawy –Prawo komunikacji elektronicznej. Jest ona potrzebna z uwagi na dodawany nowy rozdział 4a.

Definicja deklaracji zgodności została sformułowana analogicznie do definicji deklaracji z ustawy o systemach oceny zgodności i nadzoru rynku.

Nowością jest definicja dostawcy – tutaj projekt odwołuje się do art. 2 pkt 3–6 rozporządzenia 765/2008. Dostawcą jest:

* producent - każda osoba fizyczna lub prawna, która wytwarza produkt lub która zleca zaprojektowanie lub wytworzenie produktu i oferuje ten produkt pod własną nazwą lub znakiem towarowym;
* upoważniony przedstawiciel - osoba fizyczna lub prawna mająca siedzibę w Unii Europejskiej, posiadająca pisemne pełnomocnictwo od producenta do występowania w jego imieniu w zakresie określonych zadań w odniesieniu do obowiązków producentów wynikających z odpowiedniego prawodawstwa wspólnotowego;
* importer - każda osoba fizyczna lub prawna, mająca siedzibę w Unii Europejskiej, wprowadzająca na rynek wspólnotowy produkt z kraju trzeciego;

lub

* dystrybutor - każda osoba fizyczna lub prawna w łańcuchu dostaw, inna niż producent lub importer, która udostępnia produkt na rynku.

Definicja jest wprowadzana w związku z przepisami dotyczącymi krajowego systemu certyfikacji cyberbezpieczeństwa, a także przepisami odnoszącymi się do postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

Dostosowaniu do zmiany wynikającej ze zmiany brzmienia definicji cyberbezpieczeństwa ulega definicja incydentu (pkt 16) – w miejsce wyrazu „cyberbezpieczeństwo” wprowadzane są wyrazy „bezpieczeństwo systemów informacyjnych”.

Wobec zmiany zakresu przedmiotowego ustawy, konieczne stało się zdefiniowanie nowego rodzaju incydentu, czyli incydentu telekomunikacyjnego (pkt 20). Jest to każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. Definicja ta nawiązuje do art. 2 pkt 42 EKŁE. Jednocześnie w definicji incydentu krytycznego (pkt 17) uwzględniono, że incydentem krytycznym może być również incydent telekomunikacyjny.

Incydent telekomunikacyjny jest zdarzeniem ściśle związanym z przedsiębiorcami komunikacji elektronicznej. Jego wyodrębnienie obok „incydentu” wynika z konieczności implementacji EKŁE. Akt ten inaczej definiuje incydent telekomunikacyjny niż dyrektywa NIS. Odnosi się bowiem do pojęcia bezpieczeństwa sieci lub usług komunikacji elektronicznej, tymczasem w dyrektywie NIS incydent odnosi się do pojęcia bezpieczeństwa systemów informacyjnych. Incydent telekomunikacyjny wprost, pod kątem językowym, odnosi się do usług komunikacji elektronicznej. Stąd też, aby zapewnić pełne wdrożenie EKŁE w tym zakresie, wprowadzono definicję incydentu telekomunikacyjnego. Wszędzie tam, gdzie przepisy odnoszą się do przedsiębiorców komunikacji elektronicznej, projekt odnosi się do pojęcia incydentu telekomunikacyjnego. Dzieje się tak nie tylko przy rozdziale 4a, ale np. przy art. 26 dot. właściwości i kompetencji zespołów CSIRT poziomu krajowego, które będą reagować na incydenty telekomunikacyjne zgłaszane przez przedsiębiorców komunikacji elektronicznej.

Pozostawiono dotychczasowe definicje incydentu poważnego (pkt 18) oraz istotnego (pkt 19), oraz incydentu w podmiocie publicznym (pkt 21).

Definicja ISAC (art. 2 pkt 22), czyli centrum wymiany i analizy informacji na temat podatności cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa wprost nawiązuje do angielskiego rozwinięcia tego skrótu – Information Sharing and Analysis Center.

Przy definicji jednostki oceniającej zgodność – projekt odwołuje się do art. 2 pkt 13 rozporządzenia 765/2008. Jednostka oceniająca zgodność to jednostka, która wykonuje czynności z zakresu oceny zgodności, w tym wzorcowanie, badanie, certyfikację i inspekcję.

Wprowadza się definicję komunikatu elektronicznego (pkt 24) – która odsyła do definicji z art. 2 pkt 19 Prawa komunikacji elektronicznej jest to każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej. Definicja ta nie obejmuje informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania użytkownika otrzymującego informację. Definicja ta jest potrzebna z uwagi na uprawnienie przedsiębiorców telekomunikacyjnych do blokowania komunikatów elektronicznych stwarzających zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej.

Wprowadzone zostały pojęcia produktu ICT (art. 2 pkt 34), usługi ICT (art. 2 pkt 45) oraz procesu ICT (art. 2 pkt 33). Te trzy pojęcia służą objęciu systemem certyfikacji jak największego zakresu dostępnych na rynku świadczeń. Produkt oznacza „element lub grupę elementów systemów informacyjnych”. Będzie więc obejmował praktycznie wszystkie przypadki oprogramowania oraz urządzeń podlegających certyfikacji. Usługi ICT to wszelkie działania związane z przetwarzaniem informacji za pośrednictwem systemów informacyjnych. Proces ICT oznacza „zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT”. Są to więc wszelkiego rodzaju działania związane z tworzeniem systemów informacyjnych i ich bieżącym utrzymaniem.

W art. 2 pkt 38 i 39 wprowadza się definicję SOC wewnętrznych i SOC zewnętrznych. Są to zespoły pełniące funkcję operacyjnego centrum bezpieczeństwa odpowiednio wewnątrz struktury operatora usługi kluczowej (SOC wewnętrzny) oraz zewnętrzne, działające na jego rzecz (SOC zewnętrzny). Definicja wprost nawiązuje do terminu przyjętego powszechnie w praktyce (Security Operations Center) różnicując jedynie formę świadczenia usług SOC w zależności od tego, czy operator usługi kluczowej realizuje zadania przy pomocy własnych zasobów, czy też zleca, na podstawie umowy, realizację tych zadań wyspecjalizowanemu podmiotowi zewnętrznemu.

Dodano definicję przedsiębiorcy komunikacji elektronicznej (art. 2 pkt 35) odnosi się do definicji zawartej w art. 2 pkt 39 ustawy – Prawo komunikacji elektronicznej. Jest to przedsiębiorca telekomunikacyjny lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów. Z kolei definicja przedsiębiorcy telekomunikacyjnego (pkt 36) odnosi się do art. 2 pkt 40 ustawy – Prawo komunikacji elektronicznej.

Pozostawiono dotychczasową definicję ryzyka (pkt 37), a także szacowania ryzyka (pkt 40). Zachowano również dotychczasową definicję systemu informacyjnego (pkt 41).

Definicja sytuacji szczególnego zagrożenia (art. 2 pkt 42) odwołuje się do definicji z art. 2 pkt 65 ustawy -Prawo komunikacji elektronicznej. Obejmuje ona sytuacje, które wymagają współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy, zarządzania kryzysowego, utrzymania porządku publicznego oraz obronności i bezpieczeństwa państwa:

- w przypadku wystąpienia sytuacji kryzysowej, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2023 r. poz. 122),

- w czasie obowiązywania stanów nadzwyczajnych,

- w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,

Ponadto, definicja ta obejmuje sytuację stanowiącą bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej.

Definicja telekomunikacyjnego urządzenia końcowego odwołuje się do definicji z art. 2 pkt 71 ustawy - Prawo komunikacji elektronicznej.

Definicja usługi komunikacji elektronicznej (art. 2 pkt 47) odwołuje się do definicji z art. 2 pkt 76 ustawy - Prawo komunikacji elektronicznej. Określa te usługi jako usługi świadczone za pośrednictwem sieci telekomunikacyjnej, zwykle za wynagrodzeniem, z wyłączeniem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci telekomunikacyjnych lub usług komunikacji elektronicznej. Usługi komunikacji elektronicznej obejmują:

a) usługi dostępu do Internetu w rozumieniu art. 2 akapit drugi pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiającego środki dotyczące dostępu do otwartego Internetu i dotyczące opłat detalicznych za uregulowane usługi łączności wewnątrzunijnej oraz zmieniającego dyrektywę 2002/22/WE, a także rozporządzenie (UE) nr 531/2012 (Dz. Urz. UE L 310 z 26.11.2015, str. 1–18, z późn. zm.),

b) usługi komunikacji interpersonalnej,

c) usługi polegające całkowicie lub głównie na przekazywaniu sygnałów, w tym usługi transmisyjne stosowane na potrzeby świadczenia usług komunikacji maszyna - maszyna oraz na potrzeby nadawania.

Pozostawiono dotychczasowe brzmienie definicji zarządzania incydentem (pkt 48) oraz zarządzania ryzykiem (pkt 49).

Po art. 2 zostanie dodane oznaczenie działu II – Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa (art. 1 pkt 4 projektu ustawy).

#### Zmiany w art. 3

Dotychczasową treść art. 3 oznaczono jako ustęp pierwszy. Dodano ustęp drugi zgodnie z którym ustawa ma zastosowanie we wszystkich stanach gotowości obronnej państwa. Uzupełnienie ustawy o powyższe sformułowanie pozwoli uniknąć wątpliwości co do ograniczeń w funkcjonowaniu krajowego systemu cyberbezpieczeństwa. Tym samym wzmocniony zostanie defensywy potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa. Zapis ten zapewni ciągłość realizacji kompetencji przez krajowy system cyberbezpieczeństwa w stanach pokoju, kryzysu i wojny. Umożliwi współdziałanie lub współpracę podmiotów krajowego systemu cyberbezpieczeństwa w realizacji zadań operacyjnych związanych z zabezpieczeniem potrzeb obronnych w stanie pokoju jak i ich realizacji w wyższych stanach gotowości obronnej państwa.

#### Nowy art. 3a

W związku z pojawiającymi się wątpliwościami dotyczącymi uprawnień podmiotów krajowego systemu cyberbezpieczeństwa przy obsłudze incydentu został dodany art. 3a, w którym doprecyzowano, że w przypadku wystąpienia incydentu podmioty te mogą, w ramach obsługi incydentów, w szczególności podejmować działania w celu: wykrywania źródła lub dokonywania analizy ruchu sieciowego powodujących wystąpienie incydentu oraz czasowego ograniczenia ruchu sieciowy z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu. W przypadku wielu cyberataków takie działania są niezbędne w celu ochrony systemu, przy czym w praktyce działania te mogą naruszyć okresowo prawa określonych użytkowników. Z powyższych względów konieczne jest wskazanie wprost, że takie działania są dopuszczalne prawnie, jednakże wyłącznie w określonej sytuacji.

#### Zmiana art. 4

W nowelizacji art. 4, który zawiera katalog podmiotów krajowego systemu cyberbezpieczeństwa wprowadza się szereg zmian. Proponuje się także dodanie nowych podmiotów: przedsiębiorców komunikacji elektronicznej, CSIRT Telco, CSIRT INT oraz ISAC znajdujące się w wykazie ISAC. Ponadto w katalogu uwzględniono:

* Urząd Komisji Nadzoru Finansowego (UKNF pierwotnie znajdował się w krajowym systemie cyberbezpieczeństwa jako jednostka budżetowa; jednakże w związku ze zmianą ustawy o nadzorze nad rynkiem finansowym zmienił formę prawną działania – stał się państwową osobą prawną, wobec czego już nie był w systemie [[14]](#footnote-15))),
* uczelnie, Polską Akademię Nauk i jej instytuty, międzynarodowe instytuty naukowe, Centrum Łukasiewicz wraz z instytutami oraz Polską Akademię Umiejętności, odwołując się do ustawy z 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce.

W konsekwencji wprowadzonych w art. 2 zmian, w art. 4 pkt 16 zamieniono wyrazy „podmiotów świadczących usługi cyberbezpieczeństwa” na wyrazy „SOC zewnętrzne”. Z kolei sektorowe zespoły cyberbezpieczeństwa zastąpiono CSIRT sektorowymi.

Funkcjonujący obecnie krajowy system cyberbezpieczeństwa nie obejmuje innych istotnych dla funkcjonowania państwa podmiotów, takich jak:

* Państwowe Gospodarstwo Wodne Wody Polskie,
* instytucje rozwoju:
  + Polski Fundusz Rozwoju,
  + Polska Agencja Rozwoju Przedsiębiorczości,
  + Korporacja Ubezpieczeń Kredytów Eksportowych Spółka Akcyjna,
  + Polska Agencja Inwestycji i Handlu Spółka Akcyjna,
  + Agencja Rozwoju Przemysłu Spółka Akcyjna.

Państwowe Gospodarstwo Wodne Wody Polskie jako podmiot zajmujący się gospodarką wodną realizuje ważne zadania publiczne – zapobieganie suszom i powodziom oraz zapewnianie dobrej jakości wody dla mieszkańców Polski, zapewniając również Informatyczny System Osłony Kraju (ISOK). Z kolei instytucje rozwoju realizują zadania w obszarze wsparcia lub usług świadczonych przedsiębiorcom. W szczególności Polski Fundusz Rozwoju S.A. realizuje program Tarczy Antykryzysowej. Z tych powodów zasadne jest ich dodanie do katalogu podmiotów krajowego systemu cyberbezpieczeństwa.

Do krajowego systemu cyberbezpieczeństwa zostaną dodane także samodzielne publiczne zakłady opieki zdrowotnej, które podczas pandemii COVID-19 pełnią szczególną rolę. Dlatego konieczne jest objęcie tych podmiotów obowiązkami z art. 21–23 ustawy o krajowym systemie cyberbezpieczeństwa, a także zapewnienie im wsparcia właściwego zespołu CSIRT poziomu krajowego w przypadku wystąpienia incydentu w podmiocie publicznym.

### Przepisy o operatorach usług kluczowych oraz SOC

#### Zmiany w art. 7

W art. 7 dodano przepis umożliwiający ministrowi właściwemu do spraw informatyzacji wpisanie z urzędu operatora usługi kluczowej z sektora infrastruktury cyfrowej do wykazu operatorów usług kluczowych. Jest to spowodowane tym, że minister właściwy do spraw informatyzacji jest organem właściwym do spraw cyberbezpieczeństwa dla operatorów usług kluczowych z tego sektora. Jednocześnie minister prowadzi wykaz operatorów usług kluczowych. Na podstawie dotychczasowych przepisów minister musiał składać sam do siebie wnioski o wpisanie do tego wykazu, co nie ma racjonalnego uzasadnienia.

Jak wskazuje doktryna termin sześciu miesięcy na wystąpienie organu właściwego ds. cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych nie gwarantuje aktualności wykazu[[15]](#footnote-16)). Projektodawca proponuje więc, aby organ właściwy do spraw cyberbezpieczeństwa dokonał tej czynności niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych (zmiana w art. 7 ust. 4). Ponadto w propozycji nowelizacji art. 7 ust. 5 dodaje się możliwość podpisania wniosku o wpisanie operatora usługi kluczowej do wykazu operatorów także podpisem osobistym. Podpis osobisty został uregulowany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych[[16]](#footnote-17)). Jest to zaawansowany podpis elektroniczny umieszczony w warstwie elektronicznej dowodu osobistego. Podpisanie danych podpisem osobistym ma taki sam skutek wobec podmiotu publicznego co podpis własnoręczny[[17]](#footnote-18)).

#### Zmiany w art. 8

Art. 8 obecnie obowiązującej ustawy określa wymagania, co do systemu zarządzania bezpieczeństwem informacji (SZBI), który operator usługi kluczowej ma obowiązek wdrożyć w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. SZBI powinno zapewniać stosowanie środków zapobiegających i ograniczających wpływ incydentów na system informacyjny wykorzystywany do świadczenia usługi kluczowej. Jednym z tych środków jest dbałość o aktualizację oprogramowania (art. 8 pkt 5 lit. b). Projektodawca proponuje doprecyzować ten przepis poprzez zastąpienie nieostrego sformułowania „dbałość o aktualizację oprogramowania” sformułowaniem „regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji”. Operator usługi kluczowej będzie odtąd obowiązany systematycznie przeprowadzać aktualizacje oprogramowania. Przepis ma zapobiegać sytuacji, w której aktualizacje były dokonywane zbyt rzadko. Jednocześnie podejmując decyzję o aktualizacji, operator usługi kluczowej powinien dokonać analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz ocenić poziom krytyczności poszczególnych aktualizacji. Celem tej analizy jest zabezpieczenie przed sytuacją, w której konkretna aktualizacja oprogramowania w istocie zagraża bezpieczeństwu świadczonej usługi kluczowej. Należy podkreślić, że to operator usługi kluczowej jest odpowiedzialny za bezpieczeństwo swoich systemów informacyjnych. Dlatego nie powinien bezrefleksyjnie kierować się zaleceniami producenta sprzętu, ale powinien samodzielnie oceniać wpływ aktualizacji na jego systemy.

#### Zmiany w art. 9

Do tej pory operatorzy usługi kluczowej mieli obowiązek wyznaczyć jedną osobę do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa oraz przekazać jej dane do organu właściwego do spraw cyberbezpieczeństwa oraz do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa. Proponuje się zmianę polegającą na tym, że operatorzy będą obowiązani wyznaczyć nie jedną, a dwie takie osoby. Dzięki temu zawsze będzie dostępna osoba, z którą zespoły CSIRT będą mogły skontaktować się w razie potrzeby, np. w celu przekazania informacji o zidentyfikowanym cyberzagrożeniu. Proponuje się także uproszczenie sposobu przekazywania danych tych osób. Operator usługi kluczowej przekaże je wyłącznie organowi właściwemu do spraw cyberbezpieczeństwa, który z kolei niezwłocznie przekaże je do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego. Tak więc zamiast wysyłać informacje do 3 instytucji (organ właściwy, CSIRT poziomu krajowego i sektorowy zespół cyberbezpieczeństwa) zgłoszenie zostanie przekazane tylko do jednej – organu właściwego do spraw cyberbezpieczeństwa.

#### Zmiany w art. 10

W nowelizowanym art. 10 ust. 2 pkt 2 rozszerzono obowiązki nadzoru operatora usługi kluczowej nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego. Do tej pory operator miał chronić dokumenty przed niewłaściwym użyciem lub utratą integralności. Rozszerzono to o ochronę dokumentów przed uszkodzeniem, zniszczeniem, utratą oraz nieuprawnionym dostępem. Operator usługi kluczowej zostanie przez to obowiązany zapewnienia pełnej ochrony dokumentacji.

#### Zmiany w art. 11

Zgodnie z nowymi zmianami w art. 11 operator usługi kluczowej będzie zgłaszał, za pomocą systemu teleinformatycznego, o którym mowa w art. 46, incydenty poważne do CSIRT sektorowego, który następnie niezwłocznie przekaże je do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. W ten sposób zostanie ograniczony ustawowy obowiązek zgłaszania incydentów poważnych do jednego podmiotu, jednocześnie wzmacniając rolę CSIRT sektorowych. Uprości to procedurę zgłaszania incydentów przez operatorów usług kluczowych.

Operator usługi kluczowej może być także przedsiębiorcą telekomunikacyjnym. Potencjalnie jest możliwa sytuacja, gdy to samo zdarzenie będzie zarówno incydentem poważnym jak i poważnym incydentem telekomunikacyjnym. Dla uproszczenia obowiązków proponuje się (nowe ust. 3a–3b w art. 11), żeby zgłoszenie takiego incydentu było przekazywane do właściwego CSIRT sektorowego. Zespół ten niezwłocznie przekaże zgłoszenie także do CSIRT Telco. Operator usługi kluczowej będzie obowiązany w tej sytuacji współpracować również z CSIRT Telco.

#### Zmiany w art. 13

Zmiany w artykule 13 wskazują, że co do zasady operator usługi kluczowej będzie przekazywał inne fakultatywne informacje o incydentach, cyberzagrożeniach, podatnościach itd. do właściwego dla niego CSIRT sektorowego. Zespół ten przekaże te informacje dalej do CSIRT poziomu krajowego, jeżeli jest to zasadne. Zmiana wzmacnia pozycję CSIRT sektorowego stawiając go bliżej operatora usługi kluczowej z danego sektora.

#### Zmiany w art. 14

W nowelizacji zostało zaproponowane zupełnie nowe brzmienie art. 14. Wskazano w nim, że zadania operatorów usług kluczowych w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach SOC wewnętrznych i SOC zewnętrznych. SOC będzie więc:

* wdrażał system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej (art. 8),
* wyznaczał osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa (art. 9),
* prowadził i nadzorował dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej (art. 10 ust. 1–3),
* obsługiwał incydenty, zgłaszał incydenty poważne do właściwego CSIRT sektorowego (art. 11 ust. 1–3 oraz art. 12),
* przekazywał inne informacje o incydentach, cyberzagrożeniach (art. 13).

Obecnie zadania te wykonują wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Sam zakres zadań nie zmieni się.

Zgodnie z projektowanym ust. 2 SOC może być powołany wewnątrz organizacji danego operatora usługi kluczowej (SOC wewnętrzny) lub stanowić odrębny podmiot (SOC zewnętrzny). W tym drugim przypadku operator usługi kluczowej jest obowiązany poinformować organ właściwy do spraw cyberbezpieczeństwa o zawarciu umowy z zewnętrznym podmiotem realizującym zadania SOC, jego danych kontaktowych i zakresie świadczonej usługi na rzecz tego operatora.

Należy podkreślić, że każdy z operatorów usług kluczowych może swobodnie wybrać w jakim modelu prowadzony jest SOC zewnętrzny lub SOC wewnętrzny. Nie musi on być jedną konkretną jednostką w jego strukturze, jego zadania mogą być realizowane przez pracowników różnych komórek wewnętrznych danej organizacji. Możliwe jest również zawarcie umowy z kilkoma podmiotami zewnętrznymi w kwestii usług SOC i dowolnie rozdzielić pomiędzy nimi zadania. Możliwy jest także częściowy outsourcing tzn., że część zadań będzie wykonywana w SOC wewnętrznym, a część w SOC zewnętrznym. Niezależnie od wybranego modelu operator usługi kluczowej ponosi odpowiedzialność za zapewnienie ciągłości usługi kluczowej.

Wprowadza się także możliwość, aby SOC zewnętrzny mógł być utworzony na rzecz operatora usługi kluczowej przez organ tworzący lub nadzorujący operatora usługi kluczowej (ust. 3).

Wyraźnie wskazano, że SOC wewnętrzny może świadczyć swoje usługi na rzecz innych podmiotów (ust. 4). Jest to przydatne w sytuacji np. grupy kapitałowej, w której może się znajdować kilku operatorów usług kluczowych. Takie rozwiązanie pomoże zoptymalizować koszty ponoszone przez operatorów usług kluczowych. Należy przy tym zauważyć, że SOC wewnętrzny świadczący usługi również dla innego operatora usługi kluczowej będzie dla niego SOC zewnętrznym i w zakresie tej działalności będzie podlegał nadzorowi ministra właściwego do spraw informatyzacji.

Nowe brzmienie art. 14 ust. 5 nakazuje SOC wewnętrznym i SOC zewnętrznym wprowadzić, na podstawie przeprowadzonego szacowania ryzyka, zabezpieczenia zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych informacji, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów informacyjnych, a także eksploatacji i architektury systemów informacyjnych. Przepis ten upraszcza obowiązki operatorów usług kluczowych. W obecnym brzmieniu ustawy wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa są obowiązane:

1) spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej;

2) dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty, zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi;

3) stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

Warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo zostały określone w rozporządzeniu Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w *sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[[18]](#footnote-19)).* Proponuje się rezygnację z precyzowania tych warunków w rozporządzeniu – w zamian SOC wewnętrzny czy SOC zewnętrzny będą obowiązane przeprowadzić szacowanie ryzyka i wprowadzić odpowiednie zabezpieczenia, proporcjonalne do oszacowanego ryzyka.

Jeżeli operator usługi kluczowej zawiera z podmiotem trzecim umowę o świadczenie usług SOC to o umowie i jej szczegółach będzie obowiązany niezwłocznie poinformować organ właściwy ds. cyberbezpieczeństwa.

W niezbędnych sytuacjach SOC wewnętrzne i SOC zewnętrzne mają zapewnić bezpieczny zdalny dostęp do swoich systemów informacyjnych dla obsługiwanego operatora usługi kluczowej. Istotne jest, aby opracować procedury i stosować środki, które zminimalizują zagrożenie wycieku danych z SOC. Podobny przepis znajduje się w ww. rozporządzeniu i jego celem jest umożliwienie realizacji zadań zdalnie.

Zgodnie z art. 14 ust. 8 do umów o świadczenie usług SOC stosuje się przepisy prawa polskiego. Przepis ten stanowi gwarancję, że zagraniczne podmioty świadczące usługi z zakresu cyberbezpieczeństwa będą musiały stosować polskie przepisy. Ponadto, infrastruktura SOC powinna znajdować się na terytorium Rzeczypospolitej Polskiej, a personel posiadać odpowiednie poświadczenia bezpieczeństwa osobowego – do poziomu *poufne*. Nakaz posiadania infrastruktury SOC na terytorium RP zapewni możliwość skutecznej kontroli wykonywania obowiązków SOC, a także ograniczy wpływ podmiotów zagranicznych na funkcjonowanie SOC. Z kolei wymóg posiadania przez personel (tj. pracowników i osoby realizujących zadania w SOC na podstawie stosunków cywilnoprawnych) poświadczenia bezpieczeństwa do poziomu poufne umożliwi bezpieczne przekazywanie informacji niejawnych dot. podatności i cyberzagrożeń do SOC.

Nawiązując do powszechnej międzynarodowej praktyki (publikowanie informacji na podstawie wzoru zawartego w pkt. 3.3 dokumentu RFC 2350[[19]](#footnote-20))) wprowadza się obowiązek, aby SOC zewnętrzne były obowiązane udostępniać na stronie internetowej podstawowe informacje o swojej działalności. W celu zrealizowania tego obowiązku wystarczy zamieścić krótki plik tekstowy na stronie internetowej SOC zewnętrznego.

Podsumowując, zmiany w art. 14 mają ułatwić wykonywanie zadań przez operatorów usług kluczowych. Podkreślić przy tym należy, że w związku ze zmianami w art. 14 straci moc rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w *sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[[20]](#footnote-21)).*

#### Nowy art. 14a

Aby odpowiednie urzędy i służby miały dostęp do danych SOC w zakresie swoich ustawowych kompetencji, minister właściwy do spraw informatyzacji będzie prowadził wykaz SOC. Zostanie on uregulowany w nowym art. 14a. W wykazie znajdą się zarówno SOC wewnętrzne jak i SOC zewnętrzne.

Głównym celem funkcjonowania wykazu SOC jest ułatwienie ministrowi właściwemu do spraw informatyzacji realizacji funkcji nadzoru na SOC. Obecnie istniejące rejestry czy ewidencje nie pozwalają na dokładne ustalenie podmiotów, które świadczą usługi SOC na rzecz operatorów usług kluczowych. Ponadto obecny art. 14 ust. 3 nie uprawnia do przekazywania informacji o podmiotach świadczących usługi z zakresu cyberbezpieczeństwa do ministra właściwego do spraw informatyzacji od organów właściwych do spraw cyberbezpieczeństwa, CSIRT poziomu krajowego i sektorowych zespołów cyberbezpieczeństwa.

Wykaz będzie zawierał podstawowe dane o podmiocie prowadzącym SOC, na rzecz jakich podmiotów jest prowadzony, siedzibę i adres SOC wewnętrznego lub SOC zewnętrznego, numer NIP, numer we właściwym rejestrze oraz datę wpisania i wykreślenia z wykazu SOC. Wpis do wykazu będzie następował na wniosek organu właściwego do spraw cyberbezpieczeństwa. Organ będzie posiadał o tym informacje, ponieważ operator usługi kluczowej będzie miał obowiązek przekazywać informacje o powołaniu SOC wewnętrznego lub zawarcia umowy z SOC zewnętrznym. W przypadku gdy dla operatora usług kluczowych organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji (który jednocześnie prowadzi wykaz SOC), to ten minister nie będzie składał sam do siebie wniosków tylko wpisze informacje o SOC z urzędu. Oczywiście będzie możliwa zmiana danych w wykazie SOC, jeśli zostanie zmieniona firma podmiotu prowadzącego SOC. Wnioski o wpis, zmianę danych czy wykreślenie danych będą sporządzane w postaci elektronicznej i opatrywane kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Ułatwi to przekazywanie danych do wykazu SOC i usprawni pracę pracowników obsługujących ministra właściwego do spraw informatyzacji.

Wprowadza się regułę zgodnie z którą wpis, wykreślenie oraz zmiana danych w wykazie SOC będą czynnościami materialno-technicznymi, w związku z czym nie będą podlegały zaskarżeniu. Jest to związane z tym, że czynności te nie kreują żadnych uprawnień i nie nakładają żadnych obowiązków na podmioty wpisane do wykazu. Są one jedynie pochodną zadań ustawowych SOC.

Do wykazu mogą być wpisane podmioty, które nie są częścią krajowego systemu cyberbezpieczeństwa, a zajmują się reagowaniem na incydenty, ich zapobieganiem, zarządzaniem jakością zabezpieczeń jak również aktualizowaniem ryzyk. Muszą one posiadać zdolność do ochrony informacji niejawnych. Dodatkowym wymogiem jest również podpisanie porozumienia z ministrem właściwym do spraw informatyzacji w sprawie korzystania z systemu teleinformatycznego opisanego w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Celem tego przepisu jest możliwość nawiązania współpracy z innym podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, który mógłby przekazywać informacje o cyberzagrożeniach i dzięki temu wspierać rozwój krajowego systemu cyberbezpieczeństwa.

W celu umożliwienia wykonywania swoich zadań dane z wykazu SOC będą udostępniane CSIRT MON, CSIRT NASK, CSIRT GOV i właściwemu ze względu na sektor CSIRT sektorowemu, jak również operatorowi usługi kluczowej w dotyczącym go zakresie. Zakłada się, że będzie to stały dostęp i nie będzie konieczności składania wniosku o dostęp do danych wykazie SOC.

Dane z wykazu SOC mogą być udzielane w zakresie niezbędnym do realizacji ich ustawowych zadań: organowi właściwemu do spraw cyberbezpieczeństwa, Policji, Żandarmerii Wojskowej, Straży Granicznej, Centralnemu Biuru Antykorupcyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego, sądom, prokuraturze, organom Krajowej Administracji Skarbowej, Służbie Ochrony Państwa. Udzielenie informacji będzie możliwe po złożeniu stosownego wniosku przez ww. podmioty. Umożliwia się udostępnianie danych z wykazu SOC poprzez system S46, o którym mowa w art. 46 ustawy o KSC.

### Zmiany w przepisach dotyczących dostawców usług cyfrowych

Nie wprowadza się szczególnych zmian w rozdziale 4 dotyczącym obowiązków dostawców usług cyfrowych. Jedyne zmiany dotyczą art. 17 ust. 2 - we wprowadzeniu do wyliczenia w zdaniu drugim wyraz „*cyberbezpieczeństwo”* zamienia się na „*bezpieczeństwo systemów informacyjnych”*. Jest to związane ze zmianami definicyjnymi. Z kolei w punkcie 1, który obecnie brzmi: „*bezpieczeństwo systemów informacyjnych i obiektów”*, usuwa się wyrazy „*systemów informacyjnych i”*, ponieważ stanowiłoby to niepotrzebne powtórzenie. Przepis finalnie otrzyma brzmienie:

*2. Dostawca usługi cyfrowej podejmuje właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają bezpieczeństwo systemów informacyjnych odpowiednie do istniejącego ryzyka oraz uwzględniają:*

*1) bezpieczeństwo obiektów.*

### Przepisy o obowiązkach przedsiębiorców komunikacji elektronicznej w krajowym systemie cyberbezpieczeństwa

Proponuje się dodanie rozdziału 4a „Obowiązki przedsiębiorców komunikacji elektronicznej”, w którym będą uregulowane kwestie dotyczące obowiązku stosowania przez przedsiębiorców komunikacji elektronicznej środków zapewniających bezpieczeństwo sieci i usług komunikacji elektronicznej.

#### Nowy art. 20a

Współczesne społeczeństwo informacyjne jest zależne od usług dostarczanych przez przedsiębiorców komunikacji elektronicznej, bez których nie jest możliwy przepływ informacji. Z tego powodu, zarówno na poziomie europejskim jak i krajowym istotne jest, aby sieci telekomunikacyjne i usługi komunikacji elektronicznej zapewniały odpowiednio wysoki poziom bezpieczeństwa.

Obecnie przedsiębiorcy telekomunikacyjni już na podstawie dotychczas obowiązujących przepisów Działu VIIA Prawa telekomunikacyjnego są obowiązani stosować środki techniczne i organizacyjne celu zapewnienia bezpieczeństwa lub integralności sieci lub usług. Ponadto byli obowiązani poinformować Prezesa Urzędu Komunikacji Elektronicznej o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, o podjętych działaniach zapobiegawczych i środkach naprawczych oraz podjętych przez przedsiębiorcę działaniach. Prezes UKE jednak nie posiadał kompetencji reagowania na te naruszenia. Zauważyć należy, że podmioty świadczące publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów do tej pory w ogóle nie były prawnie obowiązane stosować środki bezpieczeństwa związane z usługami komunikacji interpersonalnej. Wyjątkiem w tym zakresie były wymogi narzucone unijnymi przepisami o ochronie danych osobowych.

Proponowane przepisy z jednej strony stanowią ewolucję przepisów działu VIIA Prawa telekomunikacyjnego, a z drugiej stanowią wdrożenie EKŁE. Przedsiębiorcy telekomunikacyjni od lat są obowiązani do zapewnienia środków bezpieczeństwa świadczonych usług – więc nowe przepisy nie nakładają zupełnie nowych obowiązków. Główną zmianą w tym zakresie będzie obowiązek obsługi incydentów telekomunikacyjnych oraz obowiązek zgłaszania poważnych incydentów telekomunikacyjnych do CSIRT Telco – co jest zgodne z EKŁE. Wzmocniona zostanie rola Prezesa UKE w zakresie badania środków technicznych i organizacyjnych stosowanych przez przedsiębiorców komunikacji elektronicznej.

W tym celu w art. 20a ust. 1 nakładany jest na przedsiębiorcę komunikacji elektronicznej ogólny obowiązek brania pod uwagę w swojej działalności możliwości wystąpienia sytuacji szczególnego zagrożenia. Katalog tych sytuacji obejmuje stan nadzwyczajny, sytuację kryzysową oraz bezpośrednie zagrożenie dla bezpieczeństwa sieci i usług komunikacji elektronicznej. Przepis ten odzwierciedla obecny art. 176a ust. 1 – ustawy z dnia 16 lipca 2004 r.- Prawo telekomunikacyjne. Przedsiębiorcy komunikacji elektronicznej będą obowiązani do prowadzenia systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia (art. 20 ust. 2 pkt 1). Po zidentyfikowaniu ryzyk będą obowiązani wdrożyć środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka (art. 20 ust. 2 pkt 2). Przepisy te są implementacją art. 40 ust. 1 EKŁE.

W motywie 95 EKŁE prawodawca unijny zwrócił uwagę, że podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów zazwyczaj nie sprawują rzeczywistej kontroli nad transmisją sygnałów w sieciach. Sytuacja taka może również w niektórych sytuacjach dotyczyć dostawcy usług łączności interpersonalnej wykorzystującej numery. W takich sytuacjach środki techniczne i organizacyjne mające zapewnić bezpieczeństwo sieci i usług komunikacji elektronicznej powinny być łagodniejsze. Uwzględniono to w projektowanych przepisach wskazując, że środki techniczne i organizacyjne podejmowane przez przedsiębiorców komunikacji elektronicznej powinny zapewniać poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, co również uwzględnia sytuację dostawcy usług łączności interpersonalnej wykorzystującej numery. Inne środki będą stosować duzi operatorzy sieci mobilnych, dysponujący infrastrukturą telekomunikacyjną, a inne mali przedsiębiorcy jak np. osiedlowi dostawcy usługi dostępu do Internetu.

W art. 20a ust. 2 pkt 2 wskazane zostały obligatoryjne obszary środków technicznych i organizacyjnych, które wynikają z motywu 94 EKŁE. Przykładowo środki te można podzielić na[[21]](#footnote-22)):

* środki dot. zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej, np.:
  + bezpieczeństwo fizyczne i środowiskowe,
  + bezpieczeństwo łańcuchów dostaw,
  + kontrola dostępu do sieci,
  + zapewnienie integralności sieci;
* środki dotyczące postępowania w sytuacji szczególnego zagrożenia:
  + procedury obsługi incydentu telekomunikacyjnego,
  + zdolności w zakresie wykrywania incydentów telekomunikacyjnych,
  + procedury raportowania incydentów telekomunikacyjnych oraz komunikacji;
* środki dotyczące odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej np.:
  + zapewnienie planów ciągłości działania usług,
  + zapewnienie zdolności do odtwarzania awaryjnego usług i sieci;
* środki w zakresie monitorowania, audytowania i testowania np.:
  + przygotowanie polityk monitorowania i logowania,
  + przeprowadzanie ćwiczeń w zakresie planów ciągłości działania,
  + testowanie sieci i usług,
  + przeprowadzania oceny bezpieczeństwa sieci i usług komunikacji elektronicznej.

Każdy przedsiębiorca komunikacji elektronicznej będzie dokumentował prowadzenie analizy ryzyka oraz wdrożenie środków bezpieczeństwa (art. 20a ust. 2 pkt 3). Dokumentowanie tych środków jest zgodne z powszechnie uznanymi normami technicznymi (ISO 27001), jak również pozwala na rozliczalność tych działań oraz skuteczne przeprowadzenie audytu i kontroli.

Aby uprościć prowadzenie dokumentacji, w art. 20a ust. 3 wskazano, że przedsiębiorcy komunikacji elektronicznej sporządzający plan działania w sytuacji szczególnego zagrożenia, będą dokumentować w tym planie wdrożenie środków technicznych i   organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2.

Bardzo ważne jest zapewnienie przepływu informacji między zespołami CSIRT, Prezesem UKE oraz przedsiębiorcami komunikacji elektronicznej. Dlatego proponuje się, aby co do zasady przedsiębiorcy komunikacji elektronicznej byli obowiązani wyznaczyć dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Dane tych osób będą przekazywane do Prezesa UKE. Z obowiązku wyznaczenia ww. osób wyłącza się mikroprzedsiębiorców, małych przedsiębiorców oraz średnich przedsiębiorców – mogłoby to być zbyt duże obciążenie dla tej grupy podmiotów.

Podobnie jak w obecnie obowiązujących przepisach (art. 175d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne), proponuje się, aby minister właściwy do spraw informatyzacji mógł określić, dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej, minimalny zakres środków technicznych i organizacyjnych w stosowanych celu zapewnienia bezpieczeństwa sieci i usług komunikacji elektronicznej. Przy wydawaniu rozporządzenia minister weźmie pod uwagę

* rekomendacje międzynarodowe o charakterze specjalistycznym (będą to mogły być w szczególności normy techniczne, dokumenty ENISA, akty wykonawcze Komisji Europejskiej wydane na podstawie art. 40 ust. 5 EKŁE, czy też inne dokumenty specjalistyczne organizacji międzynarodowych);
* skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej;
* potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej.

Podkreślić należy, że przewiduje się możliwość wydawania kilku rozporządzeń na podstawie art. 20a ust. 6 – odrębnie dla każdego rodzaju działalności.

Konieczność zapewnienia ministrowi właściwemu do spraw informatyzacji takiej kompetencji wynika z faktu krytycznego znaczenia usług telekomunikacyjnych dla społeczeństwa informacyjnego. Jak wyżej wspomniano wiele usług jest zależnych od usług telekomunikacyjnych, przykładowo centra przetwarzania danych potrzebują redundantnych łączy telekomunikacyjnych, aby mogły świadczyć swoje usługi. Dlatego konieczne jest, aby dla tego sektora minister mógł wydać minimalne wymagania co do środków bezpieczeństwa, aby zapewnić jednolity poziom bezpieczeństwa danego rodzaju usług komunikacji elektronicznej.

#### Nowy art. 20b

W art. 20b ust. 1 uregulowano uprawnienie Prezesa UKE do dokonywania oceny podjętych przez przedsiębiorcę komunikacji elektronicznej środków zapewniający bezpieczeństwo sieci i usług. Na jego żądanie przedsiębiorca poinformuje go o podjętych środkach. Obowiązek ten jest zgodny z art. 41 ust. 2 lit. a EKŁE.

W wyniku przeprowadzonej przez Prezesa UKE oceny mogą powstać uzasadnione wątpliwości co do stosowania przez przedsiębiorcę komunikacji elektronicznej właściwych środków technicznych i organizacyjnych. Proponuje się, żeby w takiej sytuacji Prezes UKE mógł nałożyć, w drodze decyzji, na przedsiębiorcę komunikacji elektronicznej obowiązek:

* właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych[[22]](#footnote-23)), w określonym przez Prezesa UKE terminie (art. 20b ust. 4 pkt 1) co stanowi implementację art. 41 ust. 1 EKŁE lub,
* poddania się audytowi bezpieczeństwa, którego wyniki przedsiębiorca udostępnia Prezesowi UKE (art. 20b ust. 4 pkt 2), co stanowi implementację art. 41 ust. 2 lit. b EKŁE.

Uprawnienie Prezesa UKE do nałożenia, w drodze decyzji administracyjnej, obowiązku właściwego zastosowania lub uzupełnienia środków technicznych lub organizacyjnych służy m. in. przeciwdziałaniu ryzykom związanych z błędną konfiguracją sieci, które może prowadzić do poważnych incydentów telekomunikacyjnych, lub ryzykom związanym z niewystarczającą kontrolą dostępu. O takich ryzykach wspomina Toolbox 5G[[23]](#footnote-24)). Prezes UKE będzie mógł także, na podstawie tego artykułu nakazać uzupełnić środki organizacyjne, np. związane z bezpieczeństwem fizycznym obiektów infrastruktury telekomunikacyjnej lub dostępem osób z zewnątrz, np. serwisantów dostawcy, do kluczowej infrastruktury. Określając termin na wdrożenie dodatkowych środków Prezes UKE powinien kierować się z jednej strony koniecznością jak najszybszego ich wdrożenia, a z drugiej powinien być to obiektywnie termin realny do wykonania przez przedsiębiorcę.

Celem audytu bezpieczeństwa byłaby ocena zastosowanych przez przedsiębiorcę środków zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej. Audyt będzie musiał być przeprowadzony przez podmiot niezależny od przedsiębiorcy komunikacji elektronicznej, który został zobligowany do przeprowadzenia audytu. Do tego audytu będą stosowane odpowiednio art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5 ustawy o KSC. Odpowiednie stosowanie przepisów art. 15 ust. 2 ustawy o krajowym systemie cyberbezpieczeństwa (w zakresie spełniania wymogów formalnych przez podmioty przeprowadzające audyt) wynika z różnic w wymaganych wiedzy i doświadczeniu, w zależności od zakresu przedmiotowego audytu, który ma być przeprowadzony. Przy przeprowadzaniu audytów, o których mowa w art. 20b, nie zawsze wystarczające będzie spełnienie przesłanki „praktyki w zakresie audytu bezpieczeństwa systemów informacyjnych”, gdyż niezbędne mogą być wiedza i doświadczenie w zakresie funkcjonowania specyficznych rozwiązań telekomunikacyjnych.

#### Nowy art. 20c

W art. 20c uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej po wykryciu incydentu telekomunikacyjnego. Będzie obsługiwał każdy incydent telekomunikacyjny, który u niego wystąpi. Dla przykładu oznacza to, że dostawca usługi dostępu do Internetu będzie obowiązany zainterweniować, jeżeli np. z powodów technicznych nastąpi przerwa lub pogorszenie jakości świadczenia tej usługi. Oczywiście rodzaje podejmowanych działań w ramach obsługi incydentu telekomunikacyjnego będą się różniły w zależności od przyczyny incydentu telekomunikacyjnego czy sieci lub usług dotkniętych tym incydentem. Obowiązek ten zwiększy bezpieczeństwo świadczonych usług komunikacji elektronicznej.

Przedsiębiorca komunikacji elektronicznej zapewni dostęp do rejestrowanych incydentów zespołom CSIRT poziomu krajowego i CSIRT Telco. Jest to związane z tym, że CSIRT poziomu krajowego może zmienić klasyfikację konkretnego incydentu telekomunikacyjnego, a także z uprawnieniami zespołów CSIRT w związku z reagowaniem na incydenty telekomunikacyjne.

Równocześnie będzie mógł przekazywać do zespołów CSIRT informacje o cyberzagrożeniach, podatnościach i incydentach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci lub usług komunikacji elektronicznej także o wykorzystywanych technologiach. Uprawnienie to wzmacnia przepływ informacji między przedsiębiorcami komunikacji elektronicznej a zespołami CSIRT. W oparciu o tą wiedzę zespoły CSIRT będą mogły dokonać analizę podatności czy analizę zagrożeń co zwiększy ich możliwości reagowania na incydenty telekomunikacyjne. Wiąże się to także z zadaniem zespołów CSIRT wskazanym w art. 32 ust. 4.

#### Nowy art. 20d

Przepis art. 20d reguluje zasady zgłaszania incydentów telekomunikacyjnych przez przedsiębiorców komunikacji elektronicznej. Obowiązkowemu zgłoszeniu będzie podlegał poważny incydent telekomunikacyjny. Przedsiębiorca komunikacji elektronicznej będzie obowiązany uznać incydent telekomunikacyjny za poważny incydent telekomunikacyjny, jeżeli spełni on progi określone w rozporządzeniu ministra właściwego do spraw informatyzacji (art. 20d ust. 1 pkt 1). Innymi słowy obowiązek informacyjny będzie dotyczył szczególnego rodzaju incydentów telekomunikacyjnych, które w znaczny i istotny sposób oddziałują na funkcjonowania społeczeństwa – z tego powodu państwo powinno być poinformowane o tym fakcie oraz powinno mieć odpowiednie możliwości reakcji na tego rodzaju zdarzenie.

Przedsiębiorcy telekomunikacyjni będą przekazywać do zespołu CSIRT Telco informację o wystąpieniu poważnego incydentu telekomunikacyjnego nie później niż w ciągu 8 godzin od chwili jego wystąpienia, według aktualnej wiedzy, jaką dysponują w tym czasie (art. 20d ust. 1 pkt 2 oraz 20e ust. 3). Informację tę uzupełnią w trakcie obsługi incydentu telekomunikacyjnego. Co do zasady zgłoszenie będzie przekazywane w postaci elektronicznej, a jeżeli nie będzie to możliwe – przy użyciu innych dostępnych środków komunikacji.

Podczas obsługi poważnego incydentu telekomunikacyjnego przedsiębiorcy komunikacji elektronicznej będą obowiązani współpracować z zespołami CSIRT Telco i właściwym zespołem CSIRT GOV, CSIRT MON lub CSIRT NASK. W ramach tej współpracy będą przekazywać niezbędne dane do tych zespołów, aby ułatwić reagowanie na incydent telekomunikacyjny.

Zespół CSIRT Telco przekaże niezwłocznie, w ciągu ośmiu godzin, informację o tym zgłoszeniu do właściwego dla danego przedsiębiorcy komunikacji elektronicznej zespołu CSIRT GOV, CSIRT MON lub CSIRT NASK. Rozwiązanie to zapewni jeden punkt kontaktowy dla zgłoszeń incydentów telekomunikacyjnych, z drugiej strony zapewni obieg informacji między zespołami CSIRT. Przewiduje się, że przekazywanie informacji między CSIRT będzie odbywało się poprzez system teleinformatyczny, o którym mowa w art. 46 ustawy o KSC.

Art. 20d ust. 3 przewiduje, że minister właściwy do spraw informatyzacji określi w rozporządzeniu progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny. Tworząc upoważnienie ustawowe wzięto pod uwagę parametry istotności wpływu incydentu telekomunikacyjnego wskazane w art. 40 ust. 2 EKŁE. Progi te można podzielić na:

1. ilościowe:
   1. liczbę użytkowników, na których incydent telekomunikacyjny miał wpływ,
   2. czas trwania skutków incydentu telekomunikacyjnego,
   3. obszar, na którym wystąpiły skutki incydentu telekomunikacyjnego;
2. jakościowe:
   1. zakres wpływu incydentu telekomunikacyjnego na funkcjonowanie sieci i usług,
   2. wpływ incydentu telekomunikacyjnego na zachowanie tajemnicy komunikacji elektronicznej,
   3. wpływ incydentu telekomunikacyjnego na świadczenie usług kluczowych oraz funkcjonowanie infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
   4. wpływ incydentu telekomunikacyjnego na połączenia do numerów alarmowych,
   5. wpływ incydentu telekomunikacyjnego na wykonywanie obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wydając rozporządzenie minister weźmie pod uwagę rekomendacje ENISA – agencja ta wydaje rekomendacje celem wsparcia organów regulacyjnych państw UE.

#### Nowy art. 20e

Przepis art. 20e zawiera szczegóły dotyczące zawartości zgłoszenia poważnego incydentu telekomunikacyjnego. Pozwolą one zebrać podstawowe dane o tym incydencie takie jak dane o podmiocie dotkniętym incydentem, liczbę użytkowników, na których poważny incydent telekomunikacyjny miał wpływ oraz wpływ na usługi kluczowe, usługi cyfrowe czy obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Dane te są niezbędne, aby CSIRT Telco mógł skutecznie reagować na poważne incydenty telekomunikacyjne. Ponadto dzięki tym informacjom CSIRT poziomu krajowego zyskają informacje niezbędne do bieżącego szacowania ryzyka na poziomie krajowym.

Przede wszystkim zgłoszenie musi zawierać informacje od kogo pochodzi – od jakiego podmiotu. Potem muszą być wskazane dane osoby (imię, nazwisko, numer telefonu, adres poczty elektronicznej) zgłaszającej incydent oraz dane osoby uprawnionej do zgłaszania wyjaśnień – to mogą być dwie różne osoby albo jedna, która wypełnia dwie funkcje. Istotne jest, aby CSIRT Telco wiedział kto zgłasza incydent telekomunikacyjny i kto może udzielić wyjaśnień.

Następnie muszą być wskazane sieci i usługi komunikacji elektronicznej oraz liczba użytkowników na które poważny incydent telekomunikacyjny miał wpływ a także zasięg geograficzny obszaru, na który incydent telekomunikacyjny miał wpływ.

Projekt zakłada, że zgłoszenie poważnego incydentu telekomunikacyjnego będzie zawierało opis wpływu tego zdarzenia na świadczenie usługi kluczowej przez operatorów usług kluczowych oraz usług cyfrowych przez dostawców usług cyfrowych, jeżeli ten wpływ jest znany. Interpretować to należy w ten sposób – jeżeli przedsiębiorca komunikacji elektronicznej uzyskał informację (np. w drodze negocjacji biznesowych) od swojego usługobiorcy, że jest operatorem usługi kluczowej – to powinien wskazać w zgłoszeniu czy poważny incydent telekomunikacyjny miał wpływ na świadczenie usługi kluczowej. To samo w przypadku dostawców usług cyfrowych – szczególnie tych dostawców świadczących usługi przetwarzania w chmurze – centra przetwarzania danych wymagają, do swojego codziennego funkcjonowania, niezawodnych, redundantnych łączy telekomunikacyjnych. Natomiast jeśli przedsiębiorca komunikacji elektronicznej obiektywnie nie jest w stanie wskazać, czy poważny incydent telekomunikacyjny wpłynął na operatorów usług kluczowych czy dostawców usług cyfrowych to wtedy nie musi wypełniać tej części zgłoszenia. Podobny przepis znajduje się w art. 12 ust. 1 pkt 4 lit. e ustawy o KSC.

W zgłoszeniu powinien być także opisany wpływ poważnego incydentu telekomunikacyjnego na:

* połączenia z numerami alarmowymi – o każdym przypadku niedostępności numerów ustalonych w ustawie lub w planie numeracji krajowej dla publicznych sieci telekomunikacyjnych udostępnianych służbom ustawowo powołanym do niesienia pomocy państwo powinno wiedzieć, ponieważ numery te służą pomocy obywatelom;
* możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego – chodzi o obowiązki określone obecnie w dziale VIII. *Obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego* ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne a później w art. 39 i następnych ustawy –Prawo komunikacji elektronicznej; są to m. in. zadania i obowiązki w zakresie przygotowania i utrzymywania wskazanych elementów sieci telekomunikacyjnych dla zapewnienia telekomunikacji na potrzeby systemu kierowania bezpieczeństwem narodowym. Są to kluczowe obowiązki z punktu widzenia obronności państwa, dlatego jeżeli wydarzył się poważny incydent telekomunikacyjny to państwo powinno wiedzieć w jaki sposób wpływa to na realizację tych obowiązków.

Ze względu na współzależność sieci telekomunikacyjnych incydenty telekomunikacyjne w jednym państwie mogą mieć wpływ na usługi w drugim państwie Unii Europejskiej – np. w przypadku tranzytu połączeń. Dlatego zgłoszenie poważnego incydentu telekomunikacyjnego powinno zawierać informację o transgranicznych skutkach tego zdarzenia – dzięki temu CSIRT MON, CSIRT NASK lub CSIRT GOV będą w stanie ocenić czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej.

W zgłoszeniu powinno być także wskazane jakie działania zapobiegawcze i naprawcze podjął przedsiębiorca komunikacji elektronicznej w związku z poważnym incydentem telekomunikacyjnym. Przykładowo – czy np. dokonano zabezpieczenia logów. Jest to istotne, ponieważ dzięki temu CSIRT Telco czy CSIRT poziomu krajowego będą wiedziały co zostało zrobione, a w czym należy pomóc zgłaszającemu podczas reagowania na to zdarzenie.

Oczywiście przewiduje się, że zgłoszenie może zawierać inne istotne informacje – pozostawia się to do decyzji zgłaszającego.

Ważne jest samo zgłoszenie poważnego incydentu telekomunikacyjnego, nawet jeżeli przedsiębiorca nie ma pełnej informacji o tym zdarzeniu. Jest to naturalne, dopiero po dłuższej analizie można uzyskać informacje o np. przyczynie tego zdarzenia. Dlatego wprowadza się regułę, że zgłaszający ma przekazać informacje znane mu w chwili dokonywania zgłoszenia, ale w trakcie obsługi incydentu telekomunikacyjnego musi uzupełnić te zgłoszenie.

Uprawnia się przedsiębiorcę komunikacji elektronicznej do przekazywania w niezbędnym zakresie w zgłoszeniu poważnego incydentu telekomunikacyjnego informacji mających charakter tajemnic prawnie chronionych, w tym tajemnicy przedsiębiorstwa, jeżeli są one konieczne do obsługi incydentu telekomunikacyjnego. Informacje te powinny być wyraźnie oznaczone w zgłoszeniu, aby zespół CSIRT miał świadomość, że informacja ta podlega szczególnej ochronie.

Nadaje się uprawnienie dla CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco do zwrócenia się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

#### Nowy art. 20f

Art. 20f reguluje obowiązki informacyjne przedsiębiorcy komunikacji elektronicznej wobec użytkowników końcowych. Przepis ust. 1 nakłada obowiązki dotyczące wzmacniania świadomości użytkowników z zakresu bezpieczeństwa. Na stronie internetowej przedsiębiorcy komunikacji elektronicznej będą więc publikowane podstawowe informacje o:

* potencjalnych zagrożeniach związanych z korzystaniem przez użytkowników z usług komunikacji elektronicznej;
* rekomendowanych środkach ostrożności i najbardziej popularnych sposobach zabezpieczania telekomunikacyjnych urządzeń końcowych przed oprogramowaniem złośliwym lub szpiegującym;
* przykładowych konsekwencjach braku lub nieodpowiedniego zabezpieczenia telekomunikacyjnych urządzeń końcowych.

Dzięki temu użytkownicy będą mieli dostęp do wiedzy, która umożliwi im bezpieczne korzystanie z usług komunikacji elektronicznej.

Kolejne ustępy dotyczą już sytuacji, w której doszło do wystąpienia szczególnego i znacznego[[24]](#footnote-25) zagrożenia wystąpienia incydentu telekomunikacyjnego. W takiej sytuacji przedsiębiorca komunikacji elektronicznej będzie miał obowiązek informować  użytkowników, na których takie zagrożenie może mieć wpływ, o możliwych środkach, które użytkownicy ci mogą podjąć oraz związanych z tym kosztach. Przedsiębiorca poinformuje tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej. Obowiązek ten spowoduje, że uprzedzeni wcześniej użytkownicy będą w stanie zabezpieczyć się przed zagrożeniem.

Podkreślić przy tym należy, że nie jest intencją projektodawcy nakładanie obowiązku informowania użytkowników o każdym zagrożeniu wystąpienia incydentu telekomunikacyjnego. Takie podejście spowodowałoby znaczne obciążenie działów bezpieczeństwa przedsiębiorców. Ponadto, po pewnym czasie wysyłania częstych wiadomości o drobnych zagrożeniach użytkownicy mogliby zacząć je ignorować, co byłoby niepożądane. Tak jak wyżej wspomniano – obowiązki te będą się pojawiały w sytuacji szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego. Pomocą dla przedsiębiorcy komunikacji elektronicznej przy dostosowaniu się do tych wymogów będą publikacje ENISA[[25]](#footnote-26)).

Ponadto, przedsiębiorca komunikacji elektronicznej będzie zobowiązany poinformować o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny, co stanowi implementację art. 40 ust. 3 zdanie drugie EKŁE.

#### Nowy art. 20g

W art. 20g uregulowano obowiązki przedsiębiorcy komunikacji elektronicznej do blokowania komunikatu oraz ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej. Takie działanie możliwe jest w przypadku stwierdzenia zagrożenia dla bezpieczeństwa sieci i usług oraz tylko w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny zagrożenia. W ten sposób utrzymuje się dotychczasowe obowiązki z art. 175c ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Dotychczasowy art. 175c ust. 4 stanowił, że przedsiębiorca telekomunikacyjny nie odpowiada za niewykonanie lub nienależyte wykonanie usług telekomunikacyjnych w zakresie wynikającym z art. 175c ust. 1. Zdecydowano się zrezygnować z tego rodzaju wyłączenia odpowiedzialności z mocy ustawy. Blokowanie komunikatu elektronicznego tudzież przerwanie świadczenia usługi komunikacji elektronicznej powinno być środkiem ostatecznym mającym zapewnić bezpieczeństwo sieci lub usług komunikacji elektronicznej. Przedsiębiorca komunikacji elektronicznej, aby zwolnić się z odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi powinien móc wykazać, że zastosowanie środków z art. 20g było niezbędne, konieczne oraz nie było innych środków umożliwiających w danej sytuacji zareagowanie na zagrożenie.

#### Nowy art. 20h

W art. 20h uregulowano obowiązki informacyjne Prezesa UKE. Prezes UKE m. in. przekazuje informację o wystąpieniu incydentu telekomunikacyjnego do organów regulacyjnych innych państw członkowskich oraz sprawozdania roczne, zawierające informacje o incydentach telekomunikacyjnych, zgodnie z art. 40 ust. 2 ostatnie zdanie EKŁE. Przepis ten wypełnia więc obowiązki informacyjne Polski wobec Unii Europejskiej, której jednym z celów jest zapewnienie wysokiego poziomu odporności sieci i usług komunikacji elektronicznej na swoim terytorium. Bez tych danych nie jest możliwe prowadzenie ewaluacji dotychczasowej polityki w tym obszarze.

Ponadto, zgodnie z art. 40 ust. 2 zdanie trzecie EKŁE umożliwiono Prezesowi UKE publikowanie informacji w Biuletynie Informacji Publicznej o wystąpieniu poważnego incydentu telekomunikacyjnego, jeżeli jest to uzasadnione interesem publicznym. Przedsiębiorca komunikacji elektronicznej będzie musiał opublikować tą informację na swojej stronie internetowej po poinformowaniu przez Prezesa UKE.

Prezes UKE będzie mógł nałożyć, w drodze decyzji, na przedsiębiorcę komunikacji elektronicznej obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób jej publikacji, jeżeli sposoby opublikowania informacji na Biuletynie Informacji Publicznej UKE czy na stronie przedsiębiorcy komunikacji elektronicznej w niewystarczającym stopniu służą ochronie interesu publicznego.

Celem tych przepisów jest zapewnienie możliwości poinformowania społeczeństwa np. o przyczynach nagłej niedostępności usług komunikacji elektronicznej, która dotknęłaby duże miasto czy nawet większy obszar. Brak informacji o przyczynach takich zdarzeń mógłby doprowadzić do paniki czy do niezadowolenia społecznego, co byłoby niepożądane.

### Zmiany w przepisach dotyczących podmiotów publicznych

#### Zmiany w art. 21

Zmiana w art. 21 polega na wprowadzeniu obowiązku wyznaczenia przez podmioty publiczne nie jednej, a dwóch osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Pozwoli to na zapewnienie sprawnej komunikacji między zespołami CSIRT poziomu krajowego a podmiotami publicznymi podczas trwania incydentu w podmiocie publicznym, a także na co dzień, bowiem zespoły CSIRT przesyłają często ostrzeżenia o cyberzagrożeniach.

#### Zmiany w art. 22

W art. 22 dodane zostały ust. 1a oraz 3–7, które regulują zgłaszanie incydentów w podmiocie publicznym przez Agencję Wywiadu oraz jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym . Wskazane podmioty będą zgłaszały incydenty oraz przekazywały dane osób do kontaktu do nowo utworzonego CSIRT INT. Specyfika tych jednostek, zwłaszcza ich działanie poza granicami RP, sprawia, że konieczne jest zapewnienie im dodatkowego wsparcia. To wsparcie zostanie zapewnione przez CSIRT INT prowadzony przez Agencję Wywiadu. Będzie on wspierał te jednostki w obsłudze incydentów oraz przekazywał informacje o ich sytuacji do CSIRT GOV. W związku z tym został on również wyposażony w uprawnienia do przetwarzania odpowiednich danych. Tak ukształtowane rozwiązanie zwiększy cyberbezpieczeństwo szczególnie wrażliwych podmiotów publicznych.

### ISAC i wykaz ISAC

Po rozdziale 5 zostanie dodany rozdział 5a dotyczący ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Do tej pory nic nie stało na przeszkodzie, aby były tworzone podmioty na wzór ISAC, na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji, partnerstw publiczno-prywatnych lub luźnych jednostek organizacyjnych. Nowelizacja tego nie zmienia, daje jedynie możliwość funkcjonowania ISAC w ramach krajowego systemu cyberbezpieczeństwa.

Przepis umożliwia zawarcie porozumienia między ISAC a ministrem właściwym do spraw informatyzacji o korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 uKSC. System ten pozwala na wymianę informację o podatnościach, incydentach i cyberzagrożeniach między podmiotami krajowego systemu cyberbezpieczeństwa. Korzyścią dla ISAC z podpisania porozumienia byłoby uzyskanie informacji z systemu S46, które będzie mógł wykorzystać w swojej działalności. Z drugiej strony będzie obowiązany również do współpracy z zespołami CSIRT poziomu krajowego i wymiany informacji.

Podpisanie porozumienia z ministrem należy traktować jako akt wpisania się ISAC do krajowego systemu cyberbezpieczeństwa. Uprawnienie do jego podpisania ma charakter całkowicie fakultatywny – zarówno po stronie ISAC jak i ministra. Należy tutaj zauważyć, że minister właściwy do spraw informatyzacji jest odpowiedzialny za utrzymanie systemu S46 – w tym również za jego bezpieczeństwo i ten fakt powinien minister wziąć pod uwagę decydując się na podpisanie porozumienia z ISAC.

ISAC często nie mają osobowości prawnej. Zazwyczaj mają charakter porozumienia. Dlatego wprowadzono obowiązek, aby podmioty tworzące ISAC wyznaczyły przedstawiciela w celu zawarcia porozumienia z ministrem, oraz do informowania ministra o zmianach dot. ISAC czy też jego rozwiązania (ust. 3).

W celu promocji formuły ISAC prowadzony będzie wykaz ISAC przez ministra właściwego do spraw informatyzacji. W wykazie będą publikowane dane o ISAC, które podpisały porozumienie z ministrem (ust. 4). Wykaz będzie zawierał podstawowe informacje o ISAC, nazwę, siedzibę, numer w rejestrze, dane o osobie reprezentującej ISAC[[26]](#footnote-27), dane kontaktowe (ust. 5).

Wprowadza się rozwiązania mające na celu zapewnienie aktualności wykazu:

* wpis do wykazu nastąpi niezwłocznie, najpóźniej w ciągu 7 dni od zawarcia porozumienia (ust. 6),
* ISAC będzie wykreślany z wykazu ISAC w przypadku rozwiązania porozumienia albo rozwiązania ISAC (ust. 7),
* zmiana danych w wykazie ISAC będzie następowała na wniosek[[27]](#footnote-28)) jednego z podmiotów tworzących ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu (ust. 8).

Czynnością konstytutywną jest podpisanie porozumienia między ISAC a ministrem. Rozwiązanie porozumienia oraz rozwiązanie ISAC będzie powodowało zaprzestanie korzystania z systemu S46 przez ISAC. Stąd też wykaz ISAC odzwierciedla tylko stan faktyczny, wpis oraz wykreślenie z wykazu nie kreuje praw i obowiązków. Dlatego wprowadzono przepis zgodnie z którym wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno–technicznymi (ust. 10).

Wykaz będzie publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, z wyjątkiem danych osobowych osoby reprezentującej ISAC. Takie rozwiązanie zapewni dostęp do wykazu dla obywateli (ust. 11).

W przepisie ust. 12 wprowadza się obowiązek współpracy ISAC wpisanego do wykazu ISAC z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów. Istotą tego obowiązku jest to, aby nastąpiła swego rodzaju ekwiwalentność – w zamian za dostęp do systemu S46 i informacji w nim zgromadzonych ISAC będzie dzielił się wynikami swojej działalności i w ten sposób wspierał zespoły CSIRT.

Minister będzie mógł przeprowadzić kontrolę działalności ISAC (ust. 13). Wzorcem kontroli będą:

* przepisy prawa – przepisy ustawy o krajowym systemie cyberbezpieczeństwa oraz inne przepisy dotyczące funkcjonowania ISAC czy też dotyczące bezpieczeństwa informacji,
* zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa określone w porozumieniu z ministrem.

Jeżeli ISAC nie będzie realizował swoich obowiązków lub naruszał zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa to minister właściwy ds. informatyzacji będzie mógł zwrócić się do ISAC o usunięcie nieprawidłowości w określonym terminie lub wykreślić taki podmiot z wykazu ISAC (ust. 15). Celowo tutaj użyto funktora „lub” – celem jest umożliwienie ministrowi dokonanie samego wystąpienia czy też od razu wypowiedzenia porozumienia. Możliwa jest również sytuacja, w której minister najpierw występuje o usunięcie nieprawidłowości, a następnie widząc, że ISAC ich nie usunął – wypowiedzieć porozumienie.

### Nowe obowiązki zespołów CSIRT GOV, CSIRT MON i CSIRT NASK

#### Zmiany w art. 26

Zgodnie z nową treścią art. 26 ust. 2 zespoły CSIRT GOV, CSIRT MON i CSIRT NASK będą mogły udzielić wsparcia w obsłudze incydentów i incydentów telekomunikacyjnych wszystkim podmiotom krajowego systemu cyberbezpieczeństwa oraz operatorom infrastruktury krytycznej.

Ponadto w nowym ust. 2a wprowadza się również nowe uprawnienie Pełnomocnika. Będzie mógł zlecić zapewnienie ww. wsparcia:

* CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji;
* CSIRT GOV – za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego;
* CSIRT MON – za zgodą Ministra Obrony Narodowej.

Obydwie zgody będą mogły być wyrażone z wykorzystaniem środków porozumiewania się na odległość. Powyższe rozwiązanie umożliwi udzielenie najlepszego możliwego wsparcia określonemu podmiotowi w przypadku wystąpienia incydentu, który będzie wymagał szczególnych kompetencji do jego obsługi. Dzięki temu Pełnomocnik będzie dysponował skutecznym narzędziem do reagowania na incydenty.

W art. 26 ust. 3 dodane zostały nowe zadania zespołów CSIRT poziomu krajowego.

Będą to:

* gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych
* przygotowywanie
  + na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych,
  + na zlecenie Pełnomocnika analiz skutków incydentów i incydentów telekomunikacyjnych oraz przebiegu obsługi incydentów i incydentów telekomunikacyjnych,
  + rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa.

Zadania te pozwolą zespołom CSIRT na gromadzenie informacji niezbędnych dla ich codziennego funkcjonowania. Zespoły CSIRT staną się również zapleczem analitycznym dla Pełnomocnika oraz przewodniczącego Kolegium, dzięki czemu uzyskają oni pełny obraz cyberbezpieczeństwa na poziomie krajowym. Zespoły CSIRT posiadają unikalną wiedzę na temat tego jak faktycznie funkcjonuje krajowy system cyberbezpieczeństwa – dlatego też powinny otrzymać kompetencję do przygotowywania rekomendacji w zakresie usprawniania tego systemu.

W związku z dodaniem przedsiębiorców komunikacji elektronicznej do krajowego systemu cyberbezpieczeństwa zachodzi konieczność uzupełnienia zadań CSIRT poziomu krajowego w tym zakresie. Dlatego zespoły te będą zajmować się monitorowaniem incydentów telekomunikacyjnych na poziomie krajowym, szacowaniem ryzyka związanego z zaistniałymi incydentami telekomunikacyjnymi, przekazywaniem informacji dotyczących incydentów telekomunikacyjnym podmiotom krajowego systemu cyberbezpieczeństwa, reagowaniem na incydenty telekomunikacyjne, klasyfikowaniem incydentów telekomunikacyjnych jako incydenty krytyczne.

Zespoły CSIRT poziomu krajowego będą również uprawnione do prowadzenia działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa poprzez

* wykonywanie oceny bezpieczeństwa – szczegółowe przepisy dot. tej kompetencji zawiera nowy rozdział 6b Ocena bezpieczeństwa,
* identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych[[28]](#footnote-29).

W cyberbezpieczeństwie bardzo istotny jest ciągły rozwój kadry z uwagi na zmieniające się zagrożenia. Dlatego do zadań CSIRT poziomu krajowego dodaje się również udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRT GOV, CSIRT MON lub CSIRT NASK, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.

Wprowadzono nowe brzmienie art. 26 ust. 4. Celem tych zmian jest, aby CSIRT GOV, CSIRT MON oraz CSIRT NASK wspólnie z CSIRT sektorowymi, CSIRT INT czy CSIRT Telco porozumiały się i opracowały procedury koordynacji obsługi incydentów i incydentów telekomunikacyjnych, przy których potrzebne są działania wielu zespołów CSIRT. Przykładowo może się zdarzyć sytuacja, że incydent poważny jest także incydentem istotnym jak również poważnym incydentem telekomunikacyjnym – sytuacja ta będzie angażowała właściwy CSIRT sektorowy, CSIRT Telco oraz jeden z CSIRT poziomu krajowego. Dlatego CSIRT powinny mieć opracowaną wspólną procedurę obsługi takich przypadków.

W związku z dodaniem nowych podmiotów w skład krajowego systemu cyberbezpieczeństwa należało ustalić, który z zespołów CSIRT poziomu krajowego będzie przyjmował od nich zgłoszenia incydentów. Proponuje się, że CSIRT GOV będzie właściwy dla przyjmowania incydentów zgłaszanych przez:

* Państwowe Gospodarstwo Wodne Wody Polskie,
* instytucje rozwoju,
* Urzędu Komisji Nadzoru Finansowego.

Natomiast CSIRT NASK będzie przyjmował zgłoszenia incydentów zgłaszanych przez

* Centrum Łukasiewicz,
* instytutów działających w ramach Centrum Łukasiewicz,
* instytutów badawczych,
* międzynarodowych instytutów badawczych,
* Polskiej Akademii Nauk,
* Polskiej Akademii Umiejętności,
* samodzielnych publicznych zakładów opieki zdrowotnej,
* uczelni.

Do CSIRT MON będą zgłaszali incydenty telekomunikacyjne ci przedsiębiorcy komunikacji elektronicznej, którzy są:

* podmiotami podległymi Ministrowi Obrony Narodowej lub przez niego nadzorowanymi,
* przedsiębiorcami realizującymi zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny.

Natomiast do CSIRT GOV będą zgłaszali incydenty telekomunikacyjne przedsiębiorcy komunikacji elektronicznej, którzy są wymienieni w art. 26 ust. 7.

Dla pozostałych przedsiębiorców komunikacji elektronicznej właściwym CSIRT będzie CSIRT NASK.

W związku z pismem Komisji Europejskiej Ref. Ares(2019)2130481 z dnia 26 marca 2019 r. w zakresie zmiany terminu przekazania przez państwa członkowskie sprawozdania rocznego dotyczącego informacji o zgłoszonych przez operatorów usług kluczowych incydentach poważnych i zgłoszonych przez dostawców usług cyfrowych incydentach istotnych, informacje o zgłoszonych incydentach od roku 2020, dane za rok poprzedni muszą być przekazywane do dnia 15 lutego każdego roku. Dlatego też zmieniono termin przekazania tych danych przez zespoły CSIRT poziomu krajowego do Pojedynczego Punktu Kontaktowego z 30 maja na 31 stycznia (zmiana w art. 26 ust. 3 pkt 12).

W art. 26 dodano ust. 9a, wedle którego rozbudowa i modernizacja infrastruktury teleinformatycznej CSIRT NASK służącej realizacji jego zadań może być dofinansowana w formie dotacji celowej ze środków budżetu państwa, z części której dysponentem jest minister właściwy do spraw informatyzacji.

W ust. 11 poprawia się błąd zawarty w ustawie – zamienia się wyrazy „Ministra Cyfryzacji” na wyrazy „ministra właściwego do spraw informatyzacji” co zapewni zgodność z ustawą z dnia 4 września 1997 r. o działach administracji rządowej[[29]](#footnote-30)).

W art. 26 dodaje się ust. 12, zgodnie z którym Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy ds. informatyzacji poinformują Pełnomocnika o zawarciu przez CSIRT poziomu krajowego porozumienia w sprawie powierzenia sobie wzajemnie wykonywania zadań w stosunku do niektórych rodzajów podmiotów krajowego systemu cyberbezpieczeństwa. Pełnomocnik opublikuje komunikat o zawarciu porozumienia na stronie podmiotowej w Biuletynie Informacji Publicznej.

#### Zmiany w art. 31

Zgodnie z nowym ust. 1a CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgodnią sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej przez przedsiębiorców komunikacji elektronicznej. Ponadto dodaje się obowiązek publikacji przez Pełnomocnika komunikatu o sposobie dokonywania zgłoszeń incydentów do CSIRT poziomu krajowego.

#### Zmiany w art. 32

Zmiana w art. 32 ust. 4 ma charakter redakcyjny. Dodaje się CSIRT sektorowy oraz CSIRT Telco a także zastępuje się wyrazy „operatora usługi kluczowej, dostawcy usługi cyfrowej lub podmiotu publicznego, o którym mowa w art. 4 pkt 7–15” pojęciem podmiotów krajowego systemu cyberbezpieczeństwa.

#### Zmiany w art. 33

W art. 33 dodaje się w ust. 1a obowiązek przeprowadzenia przez CSIRT poziomu krajowego badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT. Podkreślić należy, że zespoły CSIRT miały uprawnienie do przeprowadzenia takiego badania od początku obowiązywania ustawy o KSC.

W art. 33 w ust. 1b–1e dodaje się również przepisy precyzujące uprawnienia CSIRT poziomu krajowego przy przeprowadzaniu badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, których wykorzystanie może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

Zmiany te uprawniają zespół CSIRT poziomu krajowego, prowadzący badanie, do podejmowania technik mających na celu: obserwację i analizę pracy, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez urządzenie informatyczne lub oprogramowanie.

Takie szczególne uprawnienia są konieczne, aby zespoły CSIRT poziomu krajowego mogły skutecznie przebadać urządzenia i oprogramowanie pod kątem zagrożeń bezpieczeństwa narodowego.

Ponadto CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie będą związane postanowieniami umów licencyjnych badanych urządzeń i oprogramowania, które ograniczają możliwość przeprowadzenia badania.

Wskazane wyżej uprawnienia zespołu prowadzącego badanie są konieczne do zapewnienia ochrony bezpieczeństwa państwa. Niektóre postanowienia umów licencyjnych mogłyby uniemożliwić realizację tego zadania. Zespół CSIRT prowadzący badanie nie powinien być ograniczony licencją twórcy złośliwego oprogramowania, którego wykorzystanie zagraża bezpieczeństwu państwa w tym np. bezpieczeństwu infrastruktury krytycznej. W zakresie badania sprzętu lub oprogramowania należy zwrócić uwagę, że standardowe umowy licencyjne nie przewidują możliwości dokonywania badania sprzętu pod kątem jego bezpieczeństwa ani też testowania konkretnych rozwiązań zastosowanych w danym produkcie. Konieczność uzyskania zgody właściciela licencji na takie działania często jest niemożliwa do uzyskania w drodze umowy zawieranej na ogólnych zasadach. Producenci nie mają bowiem interesu w umożliwianiu podmiotom zewnętrznym takich działań. Równocześnie rosnąca liczba cyberzagrożeń oraz zależność kluczowych usług od systemów teleinformatycznych sprawia, że konieczne jest by administracja publiczna dysponowała narzędziem, które pozwoli jej przeprowadzić takie badanie. Brak tych przepisów mógłby prowadzić do powstania sytuacji, w której CSIRT poziomu krajowego musiałby uzyskać zgodę dostawcy potencjalnie niebezpiecznego sprzętu na przeprowadzenie jego badania, nawet w wypadku gdyby powstało uzasadnione podejrzenie, że dany produkt może być wykorzystany do wywołania incydentu. W związku z powyższym przepis ten jest niezbędny dla zapewnienia bezpieczeństwa podmiotom krajowego systemu cyberbezpieczeństwa.

W obecnym art. 33 uKSC nie zostało wskazane w jaki sposób powinny być publikowane rekomendacje Pełnomocnika dotyczące stosowania urządzeń informatycznych lub oprogramowania. Dlatego proponuje się, aby były one publikowane w Biuletynie Informacji Publicznej (BIP) na stronie podmiotowej Pełnomocnika (nowy ust. 4c). W ślad za tą zmianą proponuje się zmianę w ust. 5 – termin 7 dni na złożenie przez podmiot krajowego systemu cyberbezpieczeństwa zastrzeżenia do rekomendacji będzie liczony od momentu opublikowania rekomendacji w BIP, a nie od momentu otrzymania przez podmiot tych rekomendacji.

#### Zmiany w art. 34

Art. 34 ust. 1 dostosowano do zmian instytucjonalnych – dodano w nim obowiązek współpracy CSIRT INT, CSIRT sektorowego, CSIRT Telco oraz SOC zewnętrznych z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań

#### Nowy art. 34a

Art. 34a zapewnia wymianę informacji o incydentach telekomunikacyjnych pomiędzy zespołami CSIRT poziomu krajowego, CSIRT Telco z Prezesem UKE. Przepis ten umożliwia realizację obowiązku informowania organów regulacyjnych w innych państwach członkowskich UE w związku z wystąpieniem incydentu telekomunikacyjnego, jeśli Prezes UKE uzna charakter tego incydentu za istotny. Ponadto Prezes UKE otrzyma informacje umożliwiające przygotowanie sprawozdań do Komisji Europejskiej i ENISA o poważnych incydentach telekomunikacyjnych. Z kolei zespoły CSIRT poziomu krajowego muszą uzgodnić z Prezesem UKE sposób i tryb przekazywania informacji o incydentach telekomunikacyjnych. Przepis ten jest implementacją art. 40 ust. 2 EKŁE.

#### Nowy art. 34b

Zgodnie z nowym art. 34b na CSIRT MON, CSIRT NASK i CSIRT GOV zostanie nałożony obowiązek współpracy z Prezesem UKE oraz z CSIRT Telco przy wykonywaniu ustawowych zadań.

#### Zmiany w art. 35

Zmiana w art. 35 ust. 5 polega na tym, że CSIRT GOV, CSIRT MON i CSIRT NASK będą mogły przekazywać informacje o podatnościach, incydentach krytycznych i cyberzagrożeniach do publikacji w Biuletynie Informacji Publicznej Pełnomocnika. Do tej pory informacje takie mogły być publikowane w Biuletynie Informacji Publicznej na stronie podmiotowej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego. Nie zmieniają się za to przesłanki w których taka publikacja jest możliwa. Publikacja takich informacji powinna przyczynić się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów oraz nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych. Podobny charakter (dot. incydentów poważnych i istotnych) mają zmiany w art. 37 ustawy o KSC.

#### Zmiany w art. 36

W art. 36 ust. 2 rozszerza się skład Zespołu do spraw Incydentów Krytycznych (dalej: „Zespół”). W skład Zespołu wejdą także przedstawiciele Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Związane jest to z nowymi zadaniami: Pełnomocnika – wydawanie ostrzeżeń, oraz ministra właściwego do spraw informatyzacji. Ponadto umożliwia się Pełnomocnikowi uczestnictwo w posiedzeniach Zespołu.

#### Nowy art. 36a

Zmiana w art. 36a umożliwia Prezesowi Rady Ministrów zobowiązanie, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego (RZZK), Ministra Obrony Narodowej do udzielenia wsparcia zespołowi CSIRT poziomu krajowego koordynującemu obsługę incydentu krytycznego, przez jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Obecne przepisy przewidują, że Dyrektor Rządowego Centrum Bezpieczeństwa, działając na podstawie decyzji Zespołu, może zwrócić się do Prezesa Rady Ministrów o zwołanie RZZK. Może się tak wydarzyć, jeżeli incydent krytyczny jest sytuacją kryzysową, wymagającą działania na poziomie rządowym. Proponowany artykuł wpisuje się w ten model działania, umożliwiając udzielenie wsparcia zespołowi CSIRT przez wyspecjalizowane w zakresie cyberbezpieczeństwa jednostki podległe lub nadzorowane przez Ministra Obrony Narodowej. Decydującą rolę będzie miał tutaj Prezes Rady Ministrów, działający w oparciu o opinię RZZK. Podkreślić należy, że dotychczasowa praktyka wskazuje, że zarówno Zespół do spraw Incydentów Krytycznych jak i RZZK są ciałami, które w sytuacjach nagłych są w stanie zebrać się szybko. Zaproponowane rozwiązanie jest zatem adekwatne.

### Zadania CSIRT INT

#### Nowy art. 36b

W nowym art. 36b wprowadzony został CSIRT INT, który będzie wspierał placówki dyplomatyczne i konsularne. Przepis ten reguluje zadania jakie zostały wskazane dla nowego CSIRT’u. Przede wszystkim będzie on wspierał ww. podmioty w reagowaniu na incydenty. Zadania te są analogiczne do zadań CSIRT’ów sektorowych. Wprowadzenie tego nowego CSIRT-u zwiększy cyberbezpieczeństwo podmiotów publicznych, które ze względu na swoje szczególne położenie są szczególnie narażone na ataki. Nowy Zespół reagowania na incydenty komputerowe, prowadzony przez Agencję Wywiadu, będzie dysponował najlepszymi dostępnymi środkami do udzielania wsparcia podmiotom położonym poza granicami kraju. CSIRT INT będzie również blisko współpracował w tym zakresie z CSIRT GOV. Art. 36b reguluje podstawowe zadania jakie zostały postawione przed CSIRT INT. Będzie on pełnił rolę analogiczną do roli CSIRT sektorowych dla podmiotów podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych. Najważniejszym zadaniem będzie przekazywanie zgłoszeń o incydentach do CSIRT GOV. Ponadto CSIRT INT będzie wspierał te podmioty przy obsłudze incydentów oraz przekazywał im informacje o najlepszych praktykach w dziedzinie cyberbezpieczeństwa. Będzie on również mógł prowadzić testy bezpieczeństwa.

#### Nowy art. 36c

Art. 36c reguluje szczegółowo kwestię przesyłania zgłoszeń podmiotów publicznych przez CSIRT INT do CSIRT GOV. Zgłoszenia te muszą być przesłane do CSIRT GOV w ciągu 8 godzin od ich otrzymania. Jest to niezbędne ze względu na koordynacyjną rolę CSIRT GOV. By sprawnie koordynować obsługę incydentów u wszystkich podlegających mu podmiotów musi mieć aktualne dane o ich sytuacji. To rozwiązanie jest kluczowe dla zapewnienia prawidłowego przepływu informacji między podmiotami krajowego systemu cyberbezpieczeństwa, uwzględniając jednocześnie, aby obowiązek nałożony na ww. rodzaj podmiotów publicznych odbywał się jednotorowo.

### Ocena bezpieczeństwa

#### Nowy art. 36d

Wprowadzono nowy rozdział 6b, który dotyczy możliwości przeprowadzania przez CSIRT GOV, CSIRT MON, CSIRT NASK, CSIRT sektorowe, CSIRT INT lub CSIRT Telco oceny bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa. Przepisy tego rozdziału były wzorowane na art. 32a ustawy z dnia 24 maja 2002 r. o *Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[[30]](#footnote-31)*),* zwana dalej „ustawa o ABW i AW”. Wprowadzono jednak kilka istotnych zmian w stosunku do pierwowzoru. Przede wszystkim wyłącza się stosowanie tego przepisu do ocen bezpieczeństwa systemów teleinformatycznych podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy o ABW i AW. Bez tego wyłączenia powstałyby dwie podstawy prawne do przeprowadzania ocen bezpieczeństwa wobec podmiotów krajowego systemu cyberbezpieczeństwa, które są jednocześnie operatorami infrastruktury krytycznej. Nie jest to sytuacja pożądana.

Ponadto wyłącza się stosowanie rozdziału 6b do systemów teleinformatycznych akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych. Są to systemy służące przetwarzaniu informacji niejawnych i tutaj pierwszeństwo powinny mieć przepisy ustawy o ochronie informacji niejawnych.

Wprowadzono jasne określenie właściwości CSIRT poziomu krajowego do przeprowadzania ocen bezpieczeństwa – nawiązuje ono do ogólnej właściwości zespołów CSIRT określonej w art. 26 ust. 5–7. CSIRT sektorowe będą mogły przeprowadzać ocenę bezpieczeństwa wobec operatorów usług kluczowych w danym sektorze. CSIRT INT będzie mógł przeprowadzić ocenę bezpieczeństwa wobec jednostek podległych lub nadzorowanych przez Ministra Spraw Zagranicznych. CSIRT Telco będzie mógł przeprowadzić ocenę bezpieczeństwa wobec przedsiębiorców komunikacji elektronicznej.

Wprowadza się również regułę, że przeprowadzanie oceny bezpieczeństwa powinno być uzgodnione z właściwym CSIRT poziomu krajowego. Jest to po to, aby w tym samym czasie nie były prowadzone oceny bezpieczeństwa przez kilka zespołów. Jednocześnie wprowadza się obowiązek poinformowania odpowiednio organu właściwego do spraw cyberbezpieczeństwa czy Prezesa UKE o zamiarze wykonania oceny bezpieczeństwa.

#### Nowy art. 36e

Ocena bezpieczeństwa będzie mogła być przeprowadzona wyłącznie za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w postaci pisemnej lub elektronicznej pod rygorem nieważności. Jest to duża różnica względem art. 32a ustawy o ABW i AW, gdzie to Szef ABW decyduje o włączeniu systemu teleinformatycznego operatora infrastruktury krytycznej do rocznego planu przeprowadzania ocen bezpieczeństwa.

Celem oceny bezpieczeństwa jest pomoc w identyfikacji podatności. Ma ona charakter prewencyjny. Jednakże prowadzenie tej oceny nie może zaszkodzić systemowi informacyjnemu, a szerzej podmiotowi, który korzysta z tego systemu i świadczy usługi dla swoich klientów. Dlatego wprowadza się zasadę, zgodnie z którą czynności przeprowadzane w ramach oceny bezpieczeństwa powinny w jak najmniejszym stopniu zakłócać funkcjonowanie tego systemu lub ograniczać jego dostępność (art. 36e ust. 2). Tym bardziej nie jest dopuszczalne, aby działania te doprowadziły do nieodwracalnego zniszczenia danych w systemie poddanym ocenie. Przepis ten stanowi więc ogólną dyrektywę dla osób przeprowadzających ocenę bezpieczeństwa i stanowi gwarancję dla podmiotu krajowego systemu cyberbezpieczeństwa wobec którego prowadzona jest ocena bezpieczeństwa.

Po uzyskaniu zgody od podmiotu krajowego systemu cyberbezpieczeństwa, CSIRT przeprowadzający ocenę bezpieczeństwa będzie obowiązany uzgodnić tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa (art. 36e ust. 3).

Zespół CSIRT przeprowadzający ocenę bezpieczeństwa otrzyma dwa ważne uprawnienia, które są niezbędne do skutecznego przeprowadzenia takiej oceny (art. 36e ust. 4 i 5).

Po pierwsze będzie uprawniony do wytworzenia lub pozyskania urządzeń lub oprogramowania przystosowanych do popełnienia przestępstw określonych w art. 165 § 1 pkt 4[[31]](#footnote-32)), art. 267 § 3[[32]](#footnote-33)), art. 268a[[33]](#footnote-34)) § 1 albo § 2 w związku z § 1, art. 269 § 1[[34]](#footnote-35)) lub 2 albo art. 269a[[35]](#footnote-36)) Kodeksu karnego aby móc sprawdzić, czy oceniany system jest podatny na tego rodzaju oprogramowanie.

Po drugie używając ww. urządzeń lub programów zespół CSIRT będzie uprawniony do dostępu do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Będzie mógł uzyskać dostęp do całości lub części ocenianego systemu. Wprowadza się przy tym kontratyp zgodnie z którym osoba wykonująca te czynności nie popełnia przestępstwa, o którym mowa w art. 267 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

Bez tego rodzaju szczególnych uprawnień zespół CSIRT nie będzie w stanie zidentyfikować podatności, które mogą być wykorzystane przez przestępców komputerowych do zaatakowania podmiotu krajowego systemu cyberbezpieczeństwa.

Aby zapewnić gwarancje dla podmiotu, u którego jest przeprowadzana ocena wprowadza się przepis na mocy którego informacje uzyskane w wyniku oceny stanowią tajemnicę prawnie chronioną (art. 36e ust. 6). Zespół CSIRT nie będzie mógł wykorzystać ich do realizacji innych zadań ustawowych. Informacje te będą podlegały niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

Końcowym etapem oceny bezpieczeństwa będzie sporządzenie przez CSIRT raportu, który będzie zawierał podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego (art. 36e ust. 7). Raport będzie przekazany do podmiotu, którego system był poddany ocenie bezpieczeństwa. Dzięki temu podmiot będzie mógł przeanalizować np. jak jego personel, odpowiedzialny za bezpieczeństwo systemu, zachowywał się podczas oceny bezpieczeństwa; czy procedury bezpieczeństwa zadziałały prawidłowo, a także czy i jakie podatności zostały wykryte podczas oceny bezpieczeństwa.

#### Nowy art. 36f

W wyniku prowadzonej przez zespół CSIRT oceny bezpieczeństwa może zostać zidentyfikowana podatność, która może występować w innych systemach informacyjnych, które np. wykorzystują to samo oprogramowanie zawierające podatność. W takiej sytuacji zasadne jest, aby zespół CSIRT był obowiązany poinformować o tym:

* ministra właściwego do spraw informatyzacji – z uwagi na to, że minister jest właściwy w sprawach systemów i sieci teleinformatycznych administracji publicznej[[36]](#footnote-37))
* Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa – z uwagi na to, że do zadań Pełnomocnika należy ocena funkcjonowania krajowego systemu cyberbezpieczeństwa, a także może on przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie (art. 63 ustawy o KSC).

#### Nowy art. 36g

Artykuł 36g zawiera upoważnienie ustawowe dla Rady Ministrów do określenia w drodze rozporządzenia sposobu niszczenia materiałów zawierające informacje, które zespół CSIRT uzyskał w trakcie przeprowadzania oceny bezpieczeństwa, a także tryb działania komisji jak i wzór protokołu. Przy wydaniu rozporządzenia powinien być wzięty pod uwagę rodzaj materiałów podlegających zniszczeniu. W szczególności chodzi tutaj o tajemnice prawnie chronione, zgodnie z art. 36e ust. 6.

### Zmiany w przepisach o przetwarzaniu danych

#### Zmiany w art. 37

W art. 37 dodano wyłączenie stosowania ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego[[37]](#footnote-38)), do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów. Wskazać należy, że zgłoszenie incydentu może zawierać wrażliwe dane dot. kluczowych dla państwa podmiotów gospodarczych, takich właśnie jak operatorzy usług kluczowych czy dostawcy usług cyfrowych. Udostępnienie informacji o tym, że u konkretnego operatora usługi kluczowej, np. elektrociepłowni, szpitalu czy kopalni, wystąpiły podatności w systemach informacyjnych czy incydenty poważne może zachęcić przestępców lub podmioty nieprzychylne Państwu do dokonania cyberataku na te podmioty. Z tego też powodu projektodawca uważa, że znajdzie zastosowanie artykuł 1 ust. 2 dyrektywy 2019/1024[[38]](#footnote-39)) ze względu na konieczność ochrony bezpieczeństwa narodowego.

#### Zmiany w art. 39

Zmiany w art. 39 umożliwią przetwarzanie danych pozyskanych w związku z incydentami i cyberzagrożeniami przez odpowiednio CSIRT sektorowe i CSIRT INT. W przypadku CSIRT sektorowych jest to zmiana wynikająca z zamiany pojęcia „sektorowy zespół cyberbezpieczeństwa” na CSIRT sektorowy.

Projekt umożliwia również przetwarzanie danych w tym danych osobowych pozyskanych przez CSIRT Telco w związku z wykonywaniem zadań związanych z reagowaniem na incydenty telekomunikacyjne. Należy wskazać, że modyfikacja przepisów polega na dopisaniu CSIRT Telco – nie są zmienione ogólne zasady przetwarzania danych przez zespoły CSIRT.

Wyjaśnienia wymaga konieczność nadania uprawnienia CSIRT Telco do przetwarzania danych osobowych pozyskanych w związku z incydentami telekomunikacyjnymi.

Incydenty telekomunikacyjne mogą być związane z różnymi rodzajami danych, w tym z danymi osobowymi. Jako przykład można wskazać zdarzenie, w którym dzienniki połączeń konsumentów zostały wykradzione lub numery telefonów użytkowników końcowych oraz numery IMSI zostały upublicznione. Atak na sieć, z której korzysta podmiot świadczący usługi OTT może spowodować utratę poufności i dostęp do wiadomości o użytkownikach np. komunikatorów internetowych. Z kolei wskutek ataku mogłaby zostać zaszyfrowana baza abonentów przedsiębiorcy komunikacji elektronicznej, wskutek czego tymczasowo niemożliwe lub utrudnione może być świadczenie usług komunikacji elektronicznej.

Aby skutecznie zareagować na tego rodzaju zdarzenia, zespoły CSIRT Telco oraz zespoły CSIRT poziomu krajowego muszą otrzymać niezbędne dane m. in. po to, aby dokonać czynności z zakresu informatyki śledczej. Niezbędne będzie przekazanie dzienników zdarzeń (logów), które mogą zawierać informacje kto, kiedy, jakiej czynności dokonał. Innym przykładem będzie przekazanie zaszyfrowanej bazy danych abonentów. Wśród tych danych często będą znajdować się dane osobowe, jak wskazano wyżej. Może być też tak, że w skład tych danych będą znajdować się informacje umożliwiające identyfikację osób, które przyczyniły się do powstania incydentu telekomunikacyjnego. W tej sytuacji niezbędne jest zapewnienie możliwości przetwarzania przez ww. zespoły CSIRT danych osobowych. Podkreślić należy, że zarówno prawodawstwo unijne jak i proponowane przepisy nakazują zgłaszanie incydentów telekomunikacyjnych spełniających określone progi ilościowe i jakościowe. Progi te będą określone w rozporządzeniu. Obecnie przedsiębiorcy telekomunikacyjni zgłaszają do Prezesa UKE naruszenia bezpieczeństwa lub integralności sieci lub usług. Liczba tych zgłoszeń nie przekracza obecnie kilkudziesięciu rocznie. Projektowane przepisy są ewolucją obecnych rozwiązań z działu VIIA ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne i ostrożnie można założyć, że liczba zgłaszanych poważnych incydentów telekomunikacyjnych będzie podobna do obecnej liczby zgłoszeń poważnych naruszeń bezpieczeństwa lub integralności sieci lub usług. Co za tym idzie ww. zespoły CSIRT będą przetwarzać dane osobowe pozyskane dopiero przy zaistnieniu szczególnego rodzaju zdarzenia, jakim będzie poważny incydent telekomunikacyjny.

Dane te będą usuwane niezwłocznie po stwierdzeniu, że nie są one konieczne do wykonywania zadań. Ustawa o KSC wprowadziła również obowiązek zachowania w tajemnicy przez zespoły CSIRT informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań, o których mowa w ustawie. Tajemnica ta będzie się również odnosić do danych osobowych pozyskanych w związku ze zgłoszeniem incydentu telekomunikacyjnego.

Podsumowując zespół CSIRT Telco oraz CSIRT poziomu krajowego będą przetwarzały w niezbędnym zakresie dane osobowe pozyskane w trakcie reagowania na poważny incydent telekomunikacyjny. Dane te będą podlegały ochronie i będą usuwane niezwłocznie po stwierdzeniu braku niezbędności przetwarzania.

Wprowadza się również możliwość przetwarzania danych osobowych pozyskanych w związku ze zgłoszeniem incydentu telekomunikacyjnego przez Prezesa UKE. Jest to związane z uprawnieniami kontrolnymi Prezesa UKE wobec przedsiębiorców komunikacji elektronicznej w zakresie wypełniania obowiązków wynikających z rozdziału 4a ustawy o KSC. Tytułem przykładu Prezes UKE będzie mógł w trakcie kontroli sprawdzić czy rzeczywiście przedsiębiorca komunikacji elektronicznej obsługiwał incydenty telekomunikacyjne – będzie mógł to ustalić przeglądając dokumentację wykrytych incydentów telekomunikacyjnych.

Wprowadza się jeszcze dodatkowy przepis regulujący zasady usuwania danych osobowych pozyskanych przez ministra właściwego do spraw informatyzacji, Pełnomocnika, Dyrektora Rządowego Centrum Bezpieczeństwa, Prezesa UKE w związku z wykonywaniem zadań wynikających z ustawy o KSC. Przepis wypełnia lukę prawną, która obecnie występuje w ustawie o KSC.

#### Zmiany w art. 40

Z kolei zmiany w art. 40 umożliwią przetwarzanie informacji stanowiących tajemnice prawnie chronione przez CSIRT sektorowe, CSIRT INT, CSIRT Telco. Jednocześnie zespoły te zostaną obowiązane do zachowania w tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań ustawowych.

### Zmiany w przepisach o organach właściwych do spraw cyberbezpieczeństwa

#### Zmiana w art. 42

Zmiana w art. 42 polega na tym, że wnioski organu właściwego do spraw cyberbezpieczeństwa o zmianę danych w wykazie operatorów usług kluczowych będą składane niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Obecnie organ właściwy do spraw cyberbezpieczeństwa ma 6 miesięcy na przekazanie tych danych. Zmiana ta zapewni aktualność danych zawartych w wykazie operatorów usług kluczowych.

### Zadania i obowiązki CSIRT sektorowych oraz CSIRT Telco

#### Zmiany w art. 44

Proponowana w nowelizacji nowa treść art. 44 wprowadza obowiązek powołania przez organ właściwy do spraw cyberbezpieczeństwa CSIRT sektorowego właściwego dla danego sektora lub podsektora, który będzie wspierał operatorów usług kluczowych tego sektora w obszarze reagowania na incydenty.

Do obligatoryjnych zadań CSIRT sektorowego będzie należało przyjmowanie zgłoszeń o incydentach oraz reagowanie na incydenty. Dotychczas sektorowe zespoły cyberbezpieczeństwa miały za zadanie przyjmować zgłoszenia o incydentach poważnych i reagować na nie. Zmiana ta pozwoli CSIRT sektorowemu uzyskiwać więcej zgłoszeń o incydentach, dzięki czemu zespół będzie mógł szybciej zdobywać doświadczenie i wiedzę w ciągle zmieniającej się sytuacji w cyberprzestrzeni. Przełoży się to na skuteczną pomoc dla operatorów usług kluczowych zmagających się z incydentami. Podkreślić przy tym należy, że nadal operatorzy usług kluczowych będą prawnie obowiązani zgłaszać tylko incydenty poważne do CSIRT sektorowego. Dobrowolnie będą mogli zgłosić każdy incydent, nawet ten który nie spełnia progów incydentu poważnego.

Innymi zadaniami CSIRT sektorowego będzie:

* gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;
* współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
* współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów; przepis podkreśla nadrzędną rolę zespołów CSIRT poziomu krajowego;
* współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

Otrzymają również fakultatywną kompetencję zapewniania dynamicznej analizy ryzyka i incydentów oraz koordynacji incydentów w sektorze a także będą mogły, w uzgodnieniu z operatorem usługi kluczowej, wspierać go w wykonywaniu jego obowiązków określonych w art. 11 ust. 1–3, art. 12 i art. 13 ustawy o KSC. Będą one również uprawnione do przeprowadzania w określonych sytuacjach (zgodnie z rozdziałem 6b) testów bezpieczeństwa. Nie bez powodu wprowadzenie do wyliczenia w ust. 1b brzmi „CSIRT sektorowy może, w szczególności:” – katalog zadań CSIRT sektorowego jest katalogiem otwartym. CSIRT sektorowy powinien być dostosowany do sektora, do podmiotów które wspiera. Zależnie od oceny organu właściwego do spraw cyberbezpieczeństwa ustawowe zadania CSIRT sektorowego mogłyby być uzupełnione o inne np. o wsparcie operatorów usług kluczowych w zakresie zarządzania ciągłością działania, czy o zadania związane z proaktywnym przeciwdziałaniem incydentom, np. tworzeniem oprogramowania bezpieczeństwa czy monitoring technologii[[39]](#footnote-40). Otwartość katalogu jest spowodowana także tym, że nie ma CSIRT, który zapewniałby wszystkie usługi zawarte w metodykach[[40]](#footnote-41)), dlatego niezbędna jest tutaj zdrowa elastyczność. Projekt zakłada, że część zadań CSIRT sektorowego może być ustalona w akcie tworzącym CSIRT (np. w statucie jednostki budżetowej działającej jako CSIRT). Oczywiście te fakultatywne zadania nie mogą prowadzić do nałożenia pozaustawowych obowiązków na operatorów usług kluczowych. Organ właściwy do spraw cyberbezpieczeństwa ustanawiając te zadania powinien się kierować uznanymi metodykami tworzenia takich zespołów oraz koniecznością zapewnienia jak najlepszego wsparcia operatorom usług kluczowych.

CSIRT sektorowy będzie niezwłocznie (maksymalnie w ciągu 8 godzin) przekazywał zgłoszenie o incydencie poważnym do właściwego CSIRT GOV, CSIRT MON albo CSIRT NASK. Takie rozwiązanie gwarantuje, że zespoły CSIRT poziomu krajowego będą posiadały aktualną wiedzę o występowaniu incydentów w systemie. Za nieprzestrzeganie tego obowiązku będzie możliwe ukaranie kierownika danego CSIRT sektorowego.

Dzięki wprowadzonym zmianom operatorom usług kluczowych zostanie zapewnione najlepsze możliwe wsparcie przy obsłudze incydentów. Ponadto nowy system zgłaszania incydentów zmniejsza obciążenia administracyjne ciążące na operatorach usług kluczowych.

Należy przy tym wskazać na doświadczenia płynące z funkcjonowania CSIRT KNF – jedynego obecnie sektorowego zespołu cyberbezpieczeństwa. W 2021 r. CSIRT KNF przekazał podmiotom rynku finansowego 22 ostrzeżenia o zagrożeniach cyberbezpieczeństwa wraz z sugerowanymi działaniami mitygującymi te zagrożenia. Zespół ten systematycznie monitoruje kampanie złośliwego oprogramowania ukierunkowane na instytucje i klientów polskiego rynku finansowego. Prowadzi działalność edukacyjną poprzez szkolenia dla podmiotów nadzorowanych, publikowanie artykułów w prasie czy w mediach społecznościowych[[41]](#footnote-42)). Niezależnie od tego zespół ten wspiera 20 operatorów usług kluczowych w sektorze bankowości i infrastrukturze rynków finansowych w obsłudze incydentów poważnych. W 2021 r. w tym sektorze doszło do 30 incydentów poważnych[[42]](#footnote-43)), a od 1 stycznia do 8 grudnia 2022 r. do 21 incydentów poważnych[[43]](#footnote-44)). Dzięki istnieniu wyspecjalizowanego dla tego sektora zespołu CSIRT podmioty rynku finansowego mogły liczyć na szybką i konkretną pomoc przy incydentach poważnych związanych ze świadczeniem usług bankowości elektronicznej.

Opierając się na tych doświadczeniach projektodawca jest zdania, że powołanie analogicznych zespołów w innych sektorach gospodarki pozytywnie wpłynie na zdolności operatorów usług kluczowych w zakresie cyberbezpieczeństwa.

Uchyla się art. 44 ust. 2 ponieważ główną rolę w przekazywaniu informacji o incydentach o charakterze transgranicznym powinny być zespoły CSIRT poziomu krajowego, które są członkami sieci CSIRT Network.

#### Zmiana art. 44 ust. 4 oraz dodanie ust. 5–11

Zmiana w art. 44 ust. 4 polega na zmianach terminologicznych – wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”.

Organ właściwy do spraw cyberbezpieczeństwa będzie mógł powierzyć realizację zadań CSIRT sektorowego jednostkom podległym lub nadzorowanym[[44]](#footnote-45) albo organowi przez niego nadzorowanemu.

Przykładowo zadania CSIRT sektorowego będą mogły być powierzone jednostce budżetowej podległej danemu organowi właściwemu do spraw cyberbezpieczeństwa. Finansowanie CSIRT sektorowego odbędzie się co do zasady z budżetu państwa – jednostka budżetowa będąca CSIRT sektorowym powinna być ustanowiona dysponentem[[45]](#footnote-46)) środków budżetu państwa drugiego lub trzeciego stopnia z części budżetowej, której dysponentem jest organ właściwy do spraw cyberbezpieczeństwa. Do decyzji organu właściwego do spraw cyberbezpieczeństwa należeć będzie czy zadania CSIRT sektorowego zostaną powierzone istniejącej jednostce budżetowej czy też zostanie w tym celu utworzona nowa jednostka budżetowa zgodnie z art. 12 lub 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

Projekt przewiduje możliwość powierzenia zadań także jednostce nadzorowanej przez organ właściwy do spraw cyberbezpieczeństwa. W szczególności CSIRT sektorowy mógłby zostać utworzony w państwowym instytucie badawczym. Zgodnie z art. 22 pkt 2 lit b ustawy z 30 kwietnia 2010 r. o instytutach badawczych do zadań państwowego instytutu badawczego należy wykonywanie m. in. zadań szczególnie ważnych dla planowania i realizacji polityki państwa, których wykonanie jest niezbędne dla zapewnienia obronności i bezpieczeństwa publicznego które dotyczą monitoringu i zapobiegania skutkom zjawisk i wydarzeń mogących stwarzać zagrożenie publiczne. Niewątpliwie zapobieganie i reagowanie na incydenty poważne stanowi materię bezpieczeństwa publicznego. Z tego powodu zasadne jest powierzenie zadań CSIRT sektorowego państwowemu instytutowi badawczemu. Zgodnie z art. 21 ust. 6 ustawy o instytutach badawczych państwowy instytut badawczy otrzymuje dotację celową na finansowanie realizacji zleconych zadań - w tej formie odbyłoby się finansowanie zadań CSIRT sektorowego.

Wprowadza się także możliwość porozumienia się organów właściwych ds. cyberbezpieczeństwa i wyznaczenia wspólnego CSIRT sektorowego dla kilku sektorów. Organ właściwy będzie mógł także, alternatywnie, porozumieć się z organami prowadzącymi CSIRT GOV, CSIRT MON, CSIRT NASK i powierzyć im realizację zadań CSIRT sektorowego. Tego rodzaju przepisy zapewnią elastyczność i efektywne wykorzystanie zasobów przy powoływaniu zespołów CSIRT sektorowych. Komunikaty o tych porozumieniach będą publikowane w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa oraz w Biuletynie Informacji Publicznej Pełnomocnika.

#### Nowy art. 44a

W art. 44a uregulowano obowiązki zespołu CSIRT Telco. Funkcjonowanie zespołu CSIRT Telco zapewnia Prezes UKE. Będzie on mógł powierzyć prowadzenie zespołu jednostce podległej lub nadzorowanej przez ministra właściwego do spraw informatyzacji. Zadania CSIRT Telco są analogiczne do zadań CSIRT sektorowego, ale odnoszą się do działań w zakresie wsparcia przedsiębiorców komunikacji elektronicznej w obsłudze incydentów telekomunikacyjnych.

#### Nowy art. 44b

Organy właściwe do spraw cyberbezpieczeństwa i Prezes UKE będą raz w roku, do 31 stycznia przedkładać sprawozdania z funkcjonowania CSIRT sektorowych i CSIRT Telco Pełnomocnikowi (art. 44b). Zapewni to Pełnomocnikowi niezbędne informacje do prowadzenia oceny funkcjonowania krajowego systemu cyberbezpieczeństwa zgodnie z art. 62 ust. 1 pkt 1 ustawy o KSC.

#### Art. 45 ust. 1 pkt 6 lit. c – dodanie pkt 7 i 8

Zmiana art. 45 ust. 1 w pkt 6 w lit. c polegająca na dodaniu pkt 7 jest konsekwencją wprowadzenia nowych uprawnień dla ministra właściwego do spraw informatyzacji, tj. prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.

### Zmiany dot. systemu S46, zadań MON oraz nadzoru

#### Zmiany w art. 46

Proponowana w nowelizacji zmiana art. 46 określa dostęp podmiotów krajowego systemu cyberbezpieczeństwa do tworzonego na podstawie tego samego artykułu systemu teleinformatycznego (tzw. systemu S46). Pełnomocnik oraz zespoły CSIRT poziomu krajowego będą miały stały i nieograniczony dostęp do tego systemu. Prezes UKE oraz zespoły CSIRT sektorowe będą miały dostęp do systemu w obszarze swojej właściwości. Wprowadza się obligatoryjne korzystanie przez operatorów usług kluczowych z tego systemu (od 1 stycznia 2024 r., za wyjątkiem zasady, zgodnie z którą w przypadku wyznaczenia operatora usługi kluczowej od 1 lipca 2023 r., obowiązek ten aktualizuje się w ciągu 6 miesięcy). Pozostałe podmioty krajowego systemu cyberbezpieczeństwa będą mogły uzyskać dostęp do systemu po podpisaniu porozumienia z ministrem właściwym do spraw informatyzacji. Wprowadza się przy tym przepis dostosowujący, zgodnie z którym dotychczas zawarte porozumienia w sprawie korzystania z systemu S46 zachowują ważność po wejściu w życie niniejszej nowelizacji, co zapewni ciągłość korzystania z tego systemu po nowelizacji. Ponadto wprowadza się możliwość, aby system umożliwiał wymianę danych kontaktowych o zespołach CSIRT, SOC, ISAC, a także wymianę danych o osobach wyznaczonych do kontaktu przez podmioty krajowego systemu cyberbezpieczeństwa. Zapewni to płynność informacji w ramach krajowego systemu cyberbezpieczeństwa.

Nowy art. 47a

Zgodnie z tym artykułem narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK-PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała. Narzędzia te przekazywane są przez NASK-PIB najważniejszym osobom w państwie w ramach szkoleń z cyberbezpieczeństwa. Narzędzia te są ściśle spersonalizowane i ich ponowne wykorzystanie przez inne osoby nie będzie możliwe. W związku z tym należy uregulować kwestie własności tych przedmiotów. Jako że nie da się ich ponownie wykorzystać powinny przejść na własność osób, które je otrzymały. Przepis precyzuje też, skutki prawne tego przekazania w prawie podatkowym.

#### Zmiana art. 48 pkt 1

Zmiana art. 48 pkt 1 polega na dodaniu CSIRT INT do grona podmiotów, które będą informowane przez Pojedynczy Punkt Kontaktowy o zgłoszonym incydencie poważnym lub incydencie istotnym dotyczącym dwóch lub więcej państw członkowskich Unii Europejskiej.

#### Zmiany w art. 51

W art. 51 pkt 5 w prowadza się dwie zmiany. Zgodnie z obecnym przepisem Minister Obrony Narodowej kieruje działaniami związanymi z obsługą incydentów w czasie stanu wojennego. Trzeba jednak zauważyć, że działania wojenne mogą się rozpocząć zanim zostanie wprowadzony stan wojenny. Proponuje się, żeby Minister kierował tymi działaniami również w czasie wojny. Zgodnie z art. 2 pkt 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny[[46]](#footnote-47)) czas wojny jest to czas działań wojennych prowadzonych na terytorium Rzeczypospolitej Polskiej, których początek i koniec jest określany w trybie postanowienia Prezydenta Rzeczypospolitej Polskiej wydanego na wniosek Rady Ministrów. Będzie więc precyzyjnie określony moment, w którym Minister Obrony Narodowej rozpoczyna realizację tej kompetencji. Inną zmianą w tym przepisie jest doprecyzowanie, że Minister Obrony Narodowej kieruje działaniami związanymi z obsługą incydentów a także koordynuje działania CSIRT NASK i CSIRT GOV w czasie stanu wojennego oraz czasie wojny poprzez CSIRT MON.

Zgodnie z dotychczasowym punktem 8 Minister Obrony Narodowej koordynuje we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji realizację zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa. Zakres koordynacji rozszerzono o czas wojny.

#### Nowy art. 52a

Proponuje się dodanie nowego art. 52a. Funkcjonowanie CSIRT MON zapewnia Minister Obrony Narodowej – w praktyce poprzez podległe mu jednostki, jak Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni czy Służbę Kontrwywiadu Wojskowego.

Zgodnie z art. 17 ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2022 r. poz. 2091) – z chwilą mianowania przez Prezydenta Rzeczypospolitej Polskiej, o ile Prezydent RP nie określi innego terminu przejęcia dowodzenia, Naczelny Dowódca Sił Zbrojnych przejmuje dowodzenie Siłami Zbrojnymi oraz jednostkami organizacyjnymi, podporządkowanymi mu zgodnie z narodowymi planami użycia Sił Zbrojnych do obrony państwa. Natomiast w myśl art. 23 ust. 1 pkt 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny, Dowódca KWOC jest właściwy w zakresie dowodzenia jednostkami wojskowymi i związkami organizacyjnymi Wojsk Obrony Cyberprzestrzeni i podlega Naczelnemu Dowódcy Sił Zbrojnych z chwilą jego mianowania i przejęcia przez niego dowodzenia Siłami Zbrojnymi.

Proponowany przepis zabezpiecza realizację zadań Ministra Obrony Narodowej wynikających z ustawy o krajowym systemie cyberbezpieczeństwa - od chwili mianowania Naczelnego Dowódcy Sił Zbrojnych.

#### Zmiany w rozdziale 11

Zmiany w rozdziale 11 umożliwią Prezesowi UKE nadzór i kontrolę na przedsiębiorcami komunikacji elektronicznej w zakresie bezpieczeństwa sieci lub usług komunikacji elektronicznej oraz zgłaszania incydentów telekomunikacyjnych. Prezes UKE będzie mógł wydawać zalecenia pokontrolne wobec przedsiębiorców komunikacji elektronicznej. Ponadto będzie mógł wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego. Zmiany te pozwolą Prezesowi UKE na skutecznie badanie, czy przedsiębiorcy komunikacji elektronicznej rzeczywiście wykonują swoje obowiązki z zakresu bezpieczeństwa sieci lub usług komunikacji elektronicznej.

### Krajowy system certyfikacji cyberbezpieczeństwa

Po rozdziale 11 zostaje dodany rozdział 11a, zawierający przepisy 59a–59z regulujące krajowy system certyfikacji cyberbezpieczeństwa.

#### Nowy art. 59a

Projektowany art. 59a wyznacza zakres podmiotowy nowego systemu oraz wskazuje organ nadzoru nad jego działaniem. Do systemu będą należały Polskie Centrum Akredytacji, minister właściwy do spraw informatyzacji oraz zainteresowane jednostki oceniające zgodność i przedsiębiorcy certyfikujący swoje produkty. Należy tu podkreślić, że podmioty prywatne nie będą w żaden sposób zmuszone do dołączenia do tego systemu. Obowiązki z niego wynikające będą więc dotyczyć tylko tych, którzy dobrowolnie się im poddadzą. Tyczy się to zarówno jednostek oceniających zgodność jak i wytwórców.

#### Nowy art. 59b

Art. 59b wyznacza zadania dla ministra właściwego do spraw informatyzacji. Zadania te wynikają wprost z przepisów Aktu o cyberbezpieczeństwie i dotyczą nadzoru i kontroli nad podmiotami tego systemu jak również współpracy międzynarodowej w tym zakresie.

Minister właściwy do spraw informatyzacji będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w ustawie o krajowym systemie cyberbezpieczeństwa. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania nowej ustawy.

W ramach obowiązków krajowego organu minister właściwy do spraw informatyzacji będzie prowadzić szereg postępowań administracyjnych dotyczących m.in.:

* zatwierdzania certyfikatów odwołujących się do poziomu zaufania wysoki,
* wydawania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność,
* cofania i ograniczania, zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność,
* cofnięcia certyfikatu wydanego wbrew przepisom ustawy lub wbrew postanowieniom programu certyfikacyjnego,
* nakładania kar pieniężnych.

Wszystkie rozstrzygnięcia w tym zakresie będą wydawane zgodnie z przepisami Kodeksu postępowania administracyjnego, z zastrzeżeniem, że wydawania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających odbędzie się w tzw. postępowaniu uproszczonym, a pozostałe – w ogólnym.

Do obowiązków krajowego organu będą również należeć kwestie współpracy z analogicznymi organami w innych państwach Unii Europejskiej, jak również będzie przeprowadzał wzajemne przeglądy z tymi organami (art. 59b ust. 1 pkt 4). W ramach tych działań organy będą nawzajem oceniać swoje działania i funkcjonowanie krajowych systemów certyfikacji cyberbezpieczeństwa. Konieczność wdrożenia tej procedury wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

#### Nowy art. 59c

Projektowany art. 59c wyznacza rolę Polskiego Centrum Akredytacji (dalej „PCA”), które będzie nadzorowało jednostki oceniające zgodność pod kątem spełnienia przez nie wymogów akredytacji. PCA będzie tu pełniło taką samą rolę jaką pełni w ogólnym systemie oceny zgodności. Zapewni to szybkie wdrożenie nowych przepisów w praktyce.

#### Nowy art. 59d

Zgodnie z projektowanym art. 59d krajowe programy certyfikacji będą określane w drodze rozporządzeń Rady Ministrów. Przy ich tworzeniu będzie brany pod uwagę obecny stan wiedzy w dziedzinie techniki oraz kwestia potrzeb rynku w zakresie cyberbezpieczeństwa. Dzięki temu programy certyfikacyjne będą brały pod uwagę konkretne potrzeby przedsiębiorców oraz promować w tym zakresie najlepsze rozwiązania z tej dziedziny. Podstawą działania krajowego systemu certyfikacji cyberbezpieczeństwa będą jednak europejskie programy certyfikacyjne, dlatego też niniejszy przepis został ukształtowany jako fakultatywny. Dzięki temu organy będą mogły przygotowywać krajowe programy certyfikacyjne w sytuacji, gdy uznają to za korzystne dla rozwoju certyfikacji w Polsce. Przygotowanie projektu krajowego programu certyfikacji cyberbezpieczeństwa jest zadaniem ministra właściwego do spraw informatyzacji. Ze względu na konieczność szerokiego wykorzystania wiedzy specjalistycznej w ramach tych prac minister będzie mógł zlecić przygotowanie takiego dokumentu jednostkom przez siebie nadzorowanym, np. instytutom badawczych takim jak NASK- PIB czy Instytut Łączności. Przepis ten określa również elementy krajowych programów certyfikacji.

Celem krajowych programów certyfikacji cyberbezpieczeństwa jest zapewnienie, by produkty ICT, usługi ICT i procesy ICT, certyfikowane zgodnie z takimi programami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Nie jest możliwe na poziomie ustawy szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT i procesów ICT. Produkty ICT, usługi ICT i procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami, usługami i procesami są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane. W szczególności mając na uwadze, że dotyczy to tak różnych produktów jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT i procesów ICT należy następnie doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych, w przypadku, gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów zapewni skuteczność tych programów. Trzeba wskazać, że ta różnorodność wpływa na wszelkie aspekty tych programów np. w przypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady przez jego aktualizacje podczas gdy wykrycie określonej podatności w przenośnej pamięci USB może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w programie może wymagać zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.

#### Nowy art. 59e

Projektowany art. 59e wprowadza obowiązek dostawcy, który poddaje swój produkt, usługę lub proces ICT ocenie zgodności, do udostępnienia jednostce prowadzącej ten proces wszelkich informacji niezbędnych do zbadania czy produkt ten spełnia wymagania zawarte w odpowiednim procesie certyfikacji. Przepis ten gwarantuje, że jednostki oceniające zgodność będą w stanie zebrać wszystkie informacje niezbędne do sprawnego realizowania ich działań.

Nowy art. 59f

Art. 59f wyznacza elementy krajowych programów certyfikacji oraz określa poziomy uzasadnienia zaufania do których będą odwoływać się certyfikaty. Przepisy te zostały przygotowane na wzór odpowiednich przepisów Aktu o cyberbezpieczeństwie przewidujących trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, które określają poziom cyberbezpieczeństwa jaki gwarantuje dany produkt. Odpowiednio do każdego z tych poziomów będą określane odrębne wymagania jakie musi spełniać produkt by uzyskać certyfikat danego poziomu. Każdy z certyfikatów wydawanych w ramach tego systemu będzie musiał wskazywać jakiego poziomu dotyczy. Szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich i krajowych programach certyfikacji. Dzięki temu możliwa będzie promocja krajowych programów certyfikacyjnych w całej Unii Europejskiej i stosunkowo łatwe przenoszenie ich na poziom europejski. Ponadto takie rozwiązanie zapewni porównywalność certyfikatów krajowych z dokumentami z innych państw członkowskich oraz sprawi, że certyfikaty będą bardziej przejrzyste dla zagranicznych klientów. Ust. 3 tego artykułu precyzuje podstawowe metody oceny czy produkt, usługę lub proces ICT spełnia wymagania określone w programie certyfikacji. Dla każdego z poziomów uzasadnienia zaufania zostały określone odrębne podstawowe metody oceny, w taki sposób by były one proporcjonalne do wymagań jakie będą dotyczyły tych produktów, usług czy procesów ICT.

#### Nowy art. 59g

Art. 59g wprowadza wyraźny obowiązek spełniania wymagań przez produktu, usługi lub procesy ICT, które uzyskały odpowiedni certyfikat lub ocenę zgodności. Przepis ten odnosi się do, określonych wcześniej, poziomów uzasadnienia zaufania wskazując ogólnie jakie wymagania muszą być spełnione przez te produkty, usługi czy procesy ICT. Szczegółowe wymagania będą określane w odpowiednich krajowych programach certyfikacji cyberbezpieczeństwa.

#### Nowy art. 59h

Projektowany art. 59h wyznacza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji. Aby prowadzić badania produktów, usług i procesów ICT podmioty będą musiały uzyskać akredytację PCA. Wymagania dla zainteresowanych zostały określone w załączniku nr 1 do Aktu o cyberbezpieczeństwie. PCA będzie procedować na podstawie przepisów ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Są to przepisy, na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania z ich strony.

Sprawna wymiana informacji między PCA sprawującym nadzór nad akredytacją oraz ministrem właściwym do spraw informatyzacji jest niezbędna do sprawnego działania nowego systemu. W związku z tym PCA będzie informować ministra o dokonanych akredytacjach oraz o odmowie ich dokonania. Proponowane rozwiązania gwarantują, że minister właściwy do spraw informatyzacji będzie należycie poinformowany o wszystkich podmiotach wydających certyfikaty oraz będzie posiadał informacje niezbędne do prowadzenia nadzoru nad tym rynkiem.

#### Nowy art. 59i

Projektowany art. 59i reguluje sytuację, gdy europejski program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku, oprócz akredytacji, te jednostki będą musiały uzyskać zezwolenia ministra właściwego do spraw informatyzacji. Zezwolenia określone w projektowanym art. 59i wynikają wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Jeśli bowiem europejskie programy certyfikacyjne będą zawierały postanowienia o szczególnych wymaganiach w zakresie jednostek oceniających zgodność musi istnieć organ sprawdzający te wymagania oraz zezwalający na ich działanie w ramach określonego programu certyfikacji. Taka regulacja wynika wprost z obowiązku wdrożenia Aktu o cyberbezpieczeństwie. Należy podkreślić, że w związku z tym, iż postępowanie to dotyczy spełnienia formalnych kryteriów, zdecydowano o zastosowaniu w tym przypadku przepisów o postępowaniu uproszczonym. Pozwoli to maksymalnie przyśpieszyć to postępowanie oraz ograniczy formalności. Minister w ramach sprawowanego nadzoru będzie mógł również zmieniać zakres tego zezwolenia jak i cofnąć je w przypadku, gdyby określona jednostka przestała spełniać określone wymagania. Gwarantuje to zachowanie odpowiedniej jakości usług świadczonych przez jednostki oceniające zgodność.

Ust. 4–7 tego artykułu określają precyzyjnie postępowanie w przypadku stwierdzenia, że podmiot, który otrzymał zezwolenie ministra na prowadzenie oceny zgodności w przypadku wprowadzenia w europejskim programie certyfikacji dodatkowych wymogów dla jednostek oceniających zgodność. W przypadku stwierdzenia naruszenia przepisów lub postanowień programu minister będzie mógł zawiesić wydane zezwolenie na określony czas, dając jednostce czas na usunięcie naruszeń. W przypadku gdy, w określonym terminie, naruszenia nie zostaną usunięte minister cofa wydane zezwolenie. Taki sposób postępowania gwarantuje ochronę interesu publicznego, równocześnie dając przedsiębiorcy czas na usunięciu naruszeń nie wymuszając na nim ponownego przechodzenia postępowania o wydanie zezwolenia.

#### Nowy art. 59j–k

Nowo dodane przepisy art. 59j–k wyznaczają ogólne zasady związane z oceną zgodności i zasadami wydawania certyfikatów. Są one utworzone w sposób analogiczny do przepisów dot. systemu oceny zgodności.  Wskazują one wyraźnie, że poddanie produktów, usług i procesów ICT ocenie zgodności jest całkowicie dobrowolne. Warunki przeprowadzania oceny zgodności będą określane w europejskich i krajowych programach certyfikacji. Wskazano również, że tylko pozytywny wynik oceny zgodności jest podstawą do wydania certyfikatu.

Przepisy te określają, kiedy otrzymuje się certyfikat oraz kiedy możliwe jest wydanie deklaracji zgodności. W przypadku najniższego poziomu zaufania producent może sam przeprowadzić badanie produktu, a następnie wskazać w deklaracji zgodności, że produkt spełnia wymagania. Takie rozwiązanie stanowi ważne ułatwienie dla przedsiębiorców chcących uzyskać certyfikację przy możliwie najmniejszych kosztach. Będą mogli bowiem sami przeprowadzić niezbędne badania i wystawić deklarację zgodności. Równocześnie należy tu wspomnieć, że dalsze przepisy penalizują wprowadzanie w błąd w zakresie spełniania wymagań certyfikacyjnych. W związku z tym istnieje zabezpieczenie przed nadużywaniem tego rozwiązania. Otrzymanie certyfikatu wymaga przeprowadzenia badań produktu, usługi lub procesu ICT przez niezależny podmiot. Jest to niezbędna gwarancja dla prawidłowego przebiegu procesu certyfikacji. Należy nadmienić, że możliwość wystawienia deklaracji zgodności dotyczy jedynie najniższego poziomu uzasadnienia zaufania.

#### Nowy art. 59l

Projektowany art. 59l określa zagadnienia związane z wnioskiem o certyfikację w szczególności minimalne wymagania co do treści takiego wniosku. W celu usprawnienia działań podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa wszystkie dokumenty relewantne dla tego wniosku powinny zostać złożone wraz z nim. Projektowane przepisy mają zabezpieczyć prawidłowe i sprawne prowadzenie oceny zgodności.

#### Nowy art. 59m

Projektowany art. 59m wyznacza obowiązek jednostki oceniającej zgodność do przekazania ministrowi właściwemu do spraw informatyzacji danych podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jej cofnięcia. Obowiązek ten jest konieczny, gdyż umożliwia ministrowi sprawowanie skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa.

#### Nowy art. 59n

Projektowany art. 59n daje dodatkową gwarancję dla certyfikatów najwyższego poziomu. Taki certyfikat musi być zatwierdzony przez ministra właściwego do spraw informatyzacji. Dotyczy to zarówno certyfikatów wydanych na podstawie europejskich jak i krajowych programów certyfikacji cyberbezpieczeństwa. Odmowa zatwierdzenia jest możliwa w przypadku, gdy certyfikat został wydany wbrew przepisom lub postanowieniom programu certyfikacyjnego w ramach, którego prowadzona była ta procedura. Do tego postępowania będą stosowane przepisy Kodeksu postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe dla ich stron. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające przebieg procesu oceny zgodności. Przepisy przewidują też, że w przypadku, gdy będzie to konieczne, minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów naukowych o wypowiedzenie się w kwestii danego programu certyfikacji. Wymóg ten służy do przyśpieszenia postępowania przez przekazanie do organu potrzebnych mu dokumentów wraz z wnioskiem wszczynającym postępowanie. Bez tego przepisu organ musiałby wystąpić o te dokumenty co przedłużyłoby cały proces. Przepis ten reguluje również kwestie cofania certyfikatów wydanych niezgodnie z ustawą lub przepisom programu certyfikacyjnego. Obowiązek wprowadzenia takiej procedury wynika z Aktu o cyberbezpieczeństwie.

#### Nowy art. 59o

#### Art. 59o wskazuje, że jednostka oceniająca zgodność odmawia dokonania tej oceny, o ile dostawca nie dostarcza wszystkich informacji niezbędnych czy dany produkt, usługa pub proces ICT spełnia wymagania określone w odpowiednim programie certyfikacji. Dzięki temu te jednostki będą miały wyraźną podstawę do odmowy działań w przypadku stwierdzenia, że dostawca działa w złej wierze

#### Nowy art. 59p

Art. 59p precyzuje kwestie związane z certyfikatami wskazując na ich role w tym systemie. Ust. 2 określa co musi być wskazane w treści certyfikatu. Szczególnie ważne jest tu wskazanie poziomu uzasadnienia zaufania, oznaczenie podmiotu, który wydał certyfikat i okresu na jaki został wydany. Przy określaniu okresu ważności certyfikatu będzie brana pod uwagę specyfikacja techniczna określonego produktu, usługi lub procesu ICT.

#### Nowy art. 59q

Projektowany art. 59q reguluje sytuację, gdy produkt, usługa lub proces ICT przestają spełniać wymagania już po otrzymaniu certyfikatu. Programy certyfikacyjne będą przewidywać zasady monitorowania produktów, usług i procesów, które uzyskały certyfikaty. W ramach tego monitoringu właściciele certyfikowanych produktów będą musieli wykazać, że ich towar wciąż spełnia wymagania określone w programie. W przypadku gdy przestanie je spełniać jednostka oceniająca zgodność obowiązana jest do cofnięcia certyfikatu. Musi również o tym poinformować ministra właściwego do spraw informatyzacji. Otrzymywanie takich informacji jest niezbędne by minister mógł wykonywać swoje obowiązki związane z nadzorem nad rynkiem certyfikacji.

#### Nowy art. 59r

Projektowany art. 59r wprowadza obowiązek jednostek oceniających zgodność w zakresie monitorowania zgodności produktów, które otrzymały certyfikaty, z wymogami wskazanymi w programie certyfikacji przez cały okres na jaki został wydany certyfikat. Aby zapewnić im możliwość realizacji tego obowiązku przyznano im uprawnienie do żądania niezbędnych informacji od dostawców produktów.

#### Nowy art. 59s

Reguluje sytuację, gdy produkt przestaje spełniać wymagania już po uzyskaniu certyfikatu. W takim przypadku, jeśli dostawca sam poinformuje jednostkę oceniającą zgodność o tej sytuacji, będzie miał 2 miesiące na przywrócenie zgodności z wymaganiami. Jeśli zaś taka niezgodność zostanie wykryta w ramach kontroli to certyfikat od razu zostaje cofnięty. Taka regulacja ma promować współpracę między jednostkami oceniającymi zgodność a dostawcami produktów i zachęcać ich do informowania o kwestiach problematycznych. Pozwoli to im utrzymać certyfikat i nie ponosić kosztów ponownej certyfikacji.

We wskazanym wyżej okresie dostawca nie może powoływać się na posiadany certyfikat.

#### Nowy art. 59t

Projektowany art. 59t reguluje kwestie związane z deklaracjami zgodności. Możliwość ich wydawania dotyczy tylko najniższego poziomu uzasadnienie zaufania i daje szansę skorzystania z programów certyfikacyjnych przy minimalnych kosztach. Producenci będą mogli sami wskazać, że ich produkty spełniają wymagania bez potrzeby przechodzenia przez proces certyfikacji co pozwoli im znacząco ograniczyć posiadane koszty. Przepis ten precyzuje również elementy jakie deklaracja zgodności musi zawierać. Te zasady gwarantują transparentność przy wystawianiu deklaracji zgodności.

#### Nowy art. 59u

Projektowany art. 59u nakłada na podmioty krajowego systemu certyfikacji cyberbezpieczeństwa obowiązek przesyłania kopii wystawionych deklaracji zgodności do ministra właściwego do spraw informatyzacji. Przepis ten gwarantuje, że minister będzie zdolny do wykonywania nadzoru nad tym rynkiem. Reguluje, kiedy jednostka oceniająca zgodność odmawia dokonania certyfikacji.

#### Nowy art. 59v

Projektowany art. 59v ustanawia domniemanie zgodności z wymogami produktów, dla których wystawione zostały deklaracje zgodności.

#### Nowy art. 59w

Zgodnie z projektowanym art. 59w podmiot, którego produkt, usługa czy proces ICT został certyfikowany jest obowiązany zapewnić by spełniał on wymogi określone w programie certyfikacji przez cały cykl życia danego produktu. Musi on również udostępniać użytkownikom wszelkie informacje niezbędne do bezpiecznego z nich korzystania. Postanowienia te są niezbędne do właściwego funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa. Produkty wymagają bowiem odpowiednio wyszkolonego personelu wsparcia by pełnić przypisaną im funkcję. Ponadto, w przypadku wielu produktów, usług i procesów ICT ciągłe aktualizacje są niezbędnym elementem zapewnienia bezpieczeństwa. Wiele z najbardziej skutecznych cyberprzestępstw dotykało urządzeń, które nie przeszły niezbędnych aktualizacji oprogramowania jak np. w czasie rozprzestrzeniania się wirusa WannaCry. Dlatego zagwarantowanie bezpieczeństwa systemów informacyjnych wymaga nałożenia takich obowiązków na ich dostawców.

#### Nowy art. 59x

Projektowany art. 59x określa obowiązki udostępniania informacji nałożone na dostawców certyfikowanych produktów. Regulacje te są niezbędne dla zapewnienia skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa.

#### Nowy art. 59y

Projektowany art. 59y dodaje kolejną metodę sprawowania nadzoru przez ministra właściwego do spraw informatyzacji. Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa będą musiały przekazywać ministrowi wyjaśnienia w kwestiach związanych z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa. Daje to ministrowi możliwość sprawdzania otrzymywanych informacji bez konieczności stosowania długotrwałej i uciążliwej dla przedsiębiorcy procedury kontrolnej. Umożliwi to również ministrowi zbieranie informacji o zjawiskach zachodzących na rynku certyfikacji.

#### Nowy art. 59z

Omawiany art. 59z daje podstawę prawną dla prowadzenia kontroli u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji. Do kontroli będą stosowane dotychczasowe przepisy ustawy o krajowym systemie cyberbezpieczeństwa. Dzięki temu organ będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli. Pozwoli to na najszybsze wdrożenie się organu do nowych obowiązków. W przypadku kontroli u podmiotów administracyjnych będzie stosowana ustawa o kontroli w administracji rządowej, a w przypadku przedsiębiorców stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2023 r. poz. 221, z późn. zm.). W związku z tym wszelkie gwarancje dla przedsiębiorców będą zachowane w tej procedurze. Ponadto będą stosowane przepisy art. 55–59 ustawy. W art. 55 w punktach od 1 do 6 wskazano zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zauważyć, że w celu uniknięcia sytuacji, w której podmiot kontrolowany zwleka z wydaniem przepustki osobie przeprowadzającej kontrolę, przesądzono, że osoba prowadząca czynności kontrolne, legitymująca się odpowiednimi dokumentami upoważniającymi do kontroli, ma prawo do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki. Warto zaznaczyć, że uprawnienia wynikające z art. 55 dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że uprawnienia te nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli.

Art. 57 wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58). W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, iż protokół podpisują osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany, osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole.

W art. 59 wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie, poinformować organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń. Wskazana powyżej regulacja jest istotna z punktu widzenia regulacji zawartych w rozdziale 14 dotyczących nakładania administracyjnych kar pieniężnych. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej. Zgodnie z obowiązującymi regulacjami w podobnych dziedzinach, od zaleceń pokontrolnych nie przysługują środki odwoławcze, natomiast wymierzanie kar pieniężnych będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych (z możliwością zaskarżenia w toku administracyjnym i sądowym).

#### Nowy art. 59za

Ponadto, dla zapewnienia realnej kontroli, nad jakością produktów, które otrzymały certyfikaty, minister właściwy do spraw informatyzacji został wyposażony w uprawnienia do przeprowadzania badań produktów (art. 59z). W zakresie analizy technicznej produktów będzie mógł zwrócić się do nadzorowanych przez siebie instytutów badawczych o wykonanie określonych czynności. Tego typu uprawnienie jest niezbędne dla zapewnienia realnego nadzoru nad jakością produktów na rynku.

#### Nowy art. 59zb

Art. 59zb określa procedurę przeprowadzania badań produktów, o których mowa w art. 59z oraz konsekwencje wykrycia, że produkt nie spełnia wymagań określonych w odpowiednim programie certyfikacji. Przepisy te precyzują kwestie takie jak protokół z pobrania próbki oraz określają kto ponosi koszt przeprowadzanych badań.

#### Nowy art. 59zc

Art. 59zc określa uprawnienia ministra właściwego do spraw informatyzacji w przypadku, gdy okaże się, że określony produkt ICT, usługa ICT lub proces ICT nie spełnia wymogów. W szczególności może on cofnąć certyfikat, jeśli tak przewiduje właściwy europejski program certyfikacyjny.

#### Nowy art. 59zd

Projektowany art. 59zd wskazuje, że minister właściwy do spraw informatyzacji jest też organem właściwym do rozpatrywania skarg na unijne i krajowe deklaracje zgodności dotyczące cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt, dla którego wystawiono deklarację zgodności nie spełnia wymagań określonych w programie certyfikacji. To uprawnienie dla ministra wynika wprost z przepisów Aktu o cyberbezpieczeństwie.

Należy zauważyć, że przepisy dotyczące skarg tworzą tylko ogólne ramy dla rozpatrywania skarg. Szczegółowo kwestie te będą regulowane w aktach implementujących wydawanych przez Komisję dla poszczególnych programów certyfikacyjnych. Należy podkreślić, że będą one odrębnie określane dla każdego kolejnego programu co sprawia, że konieczne jest pozostawienie wielu kwestii nieuregulowanych w przepisach krajowych.

Skargi składane do ministra właściwego do spraw informatyzacji rozpatrywane będą zgodnie z przepisami Kodeksu postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra wskazano, że przepisy te będą stosowane odpowiednio.

### Rekomendacje Pełnomocnika. Nowi członkowie oraz zadania Kolegium

#### Nowy art. 62a

Nowy artykuł 62a umożliwi wydawanie przez Pełnomocnika rekomendacji określających środki techniczne i organizacyjne stosowane w celu zwiększenia bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Ten dokument będzie publikowany na stronie podmiotowej Pełnomocnika w Biuletynie Informacji Publicznej. W takiej formie będą mogły być wydawane Narodowe Standardy Cyberbezpieczeństwa, o których mowa w Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej, a także inne zbiory dobrych praktyk. Podkreślić należy, że rekomendacje będą formalnie niewiążące, jednak podmioty krajowego systemu cyberbezpieczeństwa będą musiały uwzględnić je w ramach procesu zarządzania ryzykiem. Decyzja o uwzględnieniu tych środków będzie należała wyłącznie do podmiotów krajowego systemu cyberbezpieczeństwa. Dzięki rekomendacjom uzyskają one fachową wiedzę, dzięki czemu będą mogły wprowadzić adekwatne do oszacowanego ryzyka zabezpieczenia.

#### Zmiana w art. 64

Zmiana w art. 64 wskazuje, że Kolegium do Spraw Cyberbezpieczeństwa jest organem opiniodawczo-doradczym również w sprawach dotyczących działalności zespołu CSIRT INT.

#### Zmiany w art. 64a

W nowym art. 64a określone zostały nowe rodzaje analiz jakie będą mogły być zlecane CSIRT GOV CSIRT MON lub CSIRT NASK. Będą to analizy dotyczące wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 66a ust. 1 oraz analizy dotyczące trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT. Analizy te będą wykonywane na wniosek Przewodniczącego Kolegium do Spraw Cyberbezpieczeństwa i będą mogły posłużyć jako dowód w ramach postępowania o uznaniu dostawcy za dostawcę wysokiego ryzyka.

#### Zmiany w art. 65

W projektowych zmianach art. 65 rozszerzono katalog zadań Kolegium do Spraw Cyberbezpieczeństwa m. in. o wyrażanie opinii o decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie także wyrażało opinię w sprawie wyznaczenia Operatora strategicznej sieci bezpieczeństwa.

#### Zmiany w art. 66

W art. 66 proponuje się rozszerzenie składu Kolegium. Nowym członkiem Kolegium będzie minister właściwy do spraw energii, z uwagi na to, że sektor energii jest jednym z największych sektorów.

W posiedzeniach Kolegium będą mogli także uczestniczyć:

* Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca,
* Przewodniczący Komisji Nadzoru Finansowego,
* Prokurator Generalny albo jego zastępca,
* Szef Agencji Wywiadu albo jego zastępca,
* Szef Centralnego Biura Antykorupcyjnego albo jego zastępca,
* Szef Służby Wywiadu Wojskowego albo jego zastępca.

Ponadto, umożliwiono, aby pozostali szefowie służb (wymienieni w ust. 4) mogli także desygnować na posiedzenia Kolegium swoich zastępców.

W ślad za odpowiednimi zmianami w innych przepisach, uzupełniono katalog kompetencji przewodniczącego Kolegium o możliwość:

* wnioskowania o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;
* zlecenia zespołom CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;
* zlecenia CSIRT GOV CSIRT MON lub CSIRT NASK, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;
* wnioskowania o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1.

Przewodniczący Kolegium otrzyma także kompetencję do powołania zespołu opiniującego, o którym mowa w art. 66a ust. 10 pkt 1, oraz będzie mógł wskazać przedstawicieli członków Kolegium wchodzących w jego skład. Będzie mógł również rozstrzygnąć spór, o którym mowa w art. 66a ust. 10 pkt 2, wskazując właściwego członka zespołu opiniującego.

Ustawa o krajowym systemie cyberbezpieczeństwa nie przewiduje sytuacji nieobecności Sekretarza Kolegium do Spraw Cyberbezpieczeństwa na przykład spowodowanej czasowymi problemami zdrowotnymi. Aby zapewnić ciągłość obsługi Kolegium proponuje się wprowadzenie instytucji zastępcy Sekretarza Kolegium. Sekretarz Kolegium jest powoływany przez Przewodniczącego Kolegium - czyli Prezesa Rady Ministrów. Aby nie nakładać nadmiernych obowiązków na Prezesa Rady Ministrów zastosowano zasadę pomocniczości - zastępcę Sekretarza Kolegium będzie powoływał jak również odwoływał Sekretarz Kolegium. Będzie to też oznaczało, że Sekretarz Kolegium odpowiada przed Przewodniczącym Kolegium za wybór danej osoby na zastępcę. Kryteria wyboru zastępcy Sekretarza będą takie same, jak dla Sekretarza - zastępca będzie musiał spełniać wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”.

W przepisie wskazano jasno, że zastępca Sekretarza Kolegium wykonuje obowiązki Sekretarza w razie nieobecności tego ostatniego, w szczególności zastępuje go na posiedzeniu Kolegium.

### Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka

#### Nowy art. 66a

Zawarty w rozdziale I Konstytucji[[47]](#footnote-48)) art. 20 stanowi o ustroju gospodarczym Rzeczypospolitej Polskiej. Opiera się on między innymi na wolności prowadzenia działalności gospodarczej, która polega na możliwości: podejmowania działalności gospodarczej w wybranej formie, swobodnego podejmowania decyzji gospodarczych oraz decyzji w sprawie zakończenia działalności. Z kolei art. 22 Konstytucji dopuszcza ograniczenie wolności działalności gospodarczej w drodze ustawy ze względu na ważny interes publiczny. W ślad za tym artykułem Trybunał Konstytucyjny podkreślał w swoim orzecznictwie, że wolność działalności gospodarczej nie ma charakteru absolutnego. W jednym z wyroków Trybunał zaznaczył, że działalność gospodarcza może podlegać różnego rodzaju ograniczeniom w stopniu większym niż prawa i wolności o charakterze osobistym bądź politycznym[[48]](#footnote-49)). Państwo może więc wprowadzić takie przepisy ustawowe, które pozwolą zminimalizować niekorzystne skutki mechanizmów wolnorynkowych, jeżeli skutki te ujawniają się w sferze, która nie może pozostać obojętna dla państwa ze względu na ochronę powszechnie uznawanych wartości[[49]](#footnote-50)). Z kolei w innym orzeczeniu Trybunał zaznaczył, że rezygnacja z niezbędnych środków kontroli przez państwo niektórych dziedzin gospodarki mogłaby doprowadzić do zagrożenia bezpieczeństwa państwa, porządku publicznego a także prawno-międzynarodowym zobowiązaniom państwa[[50]](#footnote-51)). W tym kontekście należy wskazać, że bezpieczeństwo państwa zostało uznane przez Trybunał Konstytucyjny za element dobra wspólnego, a każdy obywatel jest zobowiązany do troski o dobro wspólne. Obowiązkiem Rady Ministrów jest zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa (art. 146 ust. 4 pkt 7 i 8 Konstytucji).

Opierając się na powyższych przesłankach, projektodawca proponuje wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych, za dostawcę wysokiego ryzyka. Wskazane w decyzji zakresy produktów ICT, rodzaje usług ICT lub konkretne procesy ICT pochodzące od dostawcy wysokiego ryzyka, będą musiały być wycofane z tych podmiotów. Rozwiązanie to ma na celu zapewnienie ochrony ważnego interesu państwowego w postaci bezpieczeństwa państwa.

Obecnie nie ma żadnych środków prawnych umożliwiających nakazanie wycofywania z eksploatacji produktów ICT, usług ICT i procesów ICT zagrażających bezpieczeństwu kluczowych podmiotów w Polsce, a przez to funkcjonowaniu państwa. W szczególności dotyczy to kluczowych przedsiębiorców telekomunikacyjnych, którzy będą świadczyć usługi w oparciu o mobilne sieci 5G[[51]](#footnote-52)). Sieć 5G będzie oferowała możliwość przetwarzania znacznie większej liczby danych oraz wyższe prędkości przekazywania danych w porównaniu do dotychczasowej sieci 3G oraz 4G. Dzięki sieci 5G możliwe będzie podłączenie znacznie większej liczby urządzeń Internetu Rzeczy niż do tej pory. Umożliwi to znacznie większe możliwości przekazywania danych pomiędzy obywatelami oraz wpłynie pozytywnie na rozwój gospodarki.

Wdrożenie sieci 5G wiąże się z ryzykami, szczególnie tymi związanymi z bezpieczeństwem. Dzięki tym sieciom będzie możliwe świadczenie wielu usług niezbędnych do funkcjonowania rynku wewnętrznego oraz utrzymania i realizacji podstawowych funkcji społecznych i gospodarczych – takich jak energetyka, transport, bankowość i opieka zdrowotna oraz systemy sterowania produkcją. Potencjalny cyberatak mógłby doprowadzić do naruszenia dostępności danej usługi na niespotykaną dotąd skalę. Możliwy byłby atak na sieć 5G, który doprowadziłby do przejęcia kontroli nad infrastrukturą krytyczną jak np. sieci energetyczne. Przejęcie kontroli nad siecią 5G mogłoby doprowadzić do naruszenia poufności ogromnej liczby przesyłanych danych. Skutki takich incydentów byłyby bardzo poważne.

Kwestia bezpieczeństwa sieci 5G została podjęta na poziomie unijnym. W motywie 3 i 4 zaleceń Komisji (UE) 2019/534 wskazano, że:

*(3) Z powodu uzależnienia wielu usług o krytycznym znaczeniu od sieci 5G konsekwencje systemowych i rozległych zakłóceń byłyby szczególnie poważne. W rezultacie zapewnienie cyberbezpieczeństwa sieci 5G jest kwestią o strategicznym znaczeniu dla Unii w czasie, gdy cyberataki przybierają na sile i są coraz bardziej wyrafinowane.*

*(4) Ponadnarodowy charakter infrastruktury stanowiącej podstawę ekosystemu cyfrowego, która charakteryzuje się siecią wzajemnych powiązań, jak również transgraniczny charakter zagrożeń oznaczają, że wszelkie istotne luki bezpieczeństwa lub cyberincydenty dotyczące sieci 5G występujące w jednym państwie członkowskim miałyby wpływ na całą Unię. Dlatego też należy przewidzieć środki w celu zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa sieci 5G.*

Komisja zaleciła, aby państwa członkowskie przeprowadziły krajową ocenę ryzyka bezpieczeństwa sieci 5G je Komisji oraz ENISA. Ponadto Komisja zaleciła, aby w oparciu o krajową ocenę ryzyka państwa członkowskie powinny:

1. zaktualizować wymogi w zakresie bezpieczeństwa oraz metody zarządzania ryzykiem stosowane w odniesieniu do sieci 5G,
2. zaktualizować odpowiednie obowiązki nakładane na przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej zgodnie z art. 13a i 13b dyrektywy 2002/21/WE,
3. obwarować ogólne zezwolenia warunkami dotyczącymi zabezpieczenia sieci publicznych przed nieuprawnionym dostępem oraz uzyskać od przedsiębiorstw uczestniczących w przyszłych postępowaniach o udzielenie praw użytkowania częstotliwości radiowych w pasmach 5G zobowiązanie do przestrzegania wymogów w zakresie bezpieczeństwa sieci na podstawie dyrektywy 2002/20/WE,
4. stosować inne środki zapobiegawcze mające na celu ograniczenie potencjalnych zagrożeń dla cyberbezpieczeństwa.

Środki te powinny obejmować obowiązki nakładane na dostawców oraz operatorów celem zapewnienia bezpieczeństwa sieci 5G.

W wyniku powyższych zaleceń powstała unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci 5G[[52]](#footnote-53)) oraz Unijny zestaw środków dla cyberbezpieczeństwa sieci 5G – tzw. Toolbox 5G[[53]](#footnote-54)). W dokumentach tych wskazano na ryzyka związane z sieciami 5G w tym także tymi związanymi z dostawcami sprzętu i oprogramowania dla tej sieci.

Jedno ze wskazanych ryzyk dotyczy dostawców, którzy znajdują się pod wpływem państw prowadzących agresywne działania w cyberprzestrzeni. Takie państwo może wpływać na dostawcę, aby wykorzystał ukryte podatności w sprzęcie lub oprogramowaniu dostarczonemu innemu państwu, aby uzyskać dostęp do wrażliwych danych przesyłanych przez ten sprzęt czy też wpływać na dostępność usług świadczonych poprzez ten sprzęt. Dostawca taki będzie działał na rzecz interesów państwa, pod którego wpływem znajduje się. Prawdopodobieństwo zaistnienia tej sytuacji zależy od stopnia, w jakim dostawca ma dostęp do sieci, w szczególności jej krytycznych funkcji[[54]](#footnote-55)).

Natomiast ryzyka dotyczą również aspektów technicznych - np. tego czy dostawca jest w stanie zapewnić bezpieczeństwo swoich produktów, jak reaguje na incydenty związane z tymi produktami, jak zarządza podatnościami własnych produktów. Niska jakość sprzętu i oprogramowania dostarczanego przez dostawcę, w tym ukryte podatności, może umożliwić cyberatak na sieć dokonywany przez agresywne państwa w cyberprzestrzeni, grupy *Advanced Persistent Threat* czy grupy przestępcze[[55]](#footnote-56)).

Z wyżej wskazanych dokumentów wynika więc, że mogą istnieć dostawcy sprzętu lub oprogramowania, którzy poprzez dostarczany sprzęt lub oprogramowanie mogą zagrażać państwom członkowskim UE, w tym także Polsce. Przyjęło się określać takich dostawców jako „dostawców wysokiego ryzyka” (*high risk vendors).*

Toolbox 5G wskazuje środki strategiczne, które będą w stanie zmitygować ryzyka wskazane w Unijnej ocenie cyberbezpieczeństwa sieci 5G. Przede wszystkim Toolbox 5G zaleca środki strategiczne:

* SM01 – wzmocnienie roli władz krajowych – środek ten polega m. in. na wyposażenie władz krajowych w kompetencje do zakazu, ograniczenia lub wprowadzenia wymagań odnośnie produktów dla sieci 5G, biorąc pod uwagę m. in. bezpieczeństwo krytycznych (*critical and sensitive)* części sieci 5G, ryzyka związane z wpływ państw trzecich na łańcuchy dostaw 5G czy ryzyka dla bezpieczeństwa narodowego,
* SM03 – ocena ryzyka dostawców – przeprowadzenie rygorystycznej oceny ryzyka dostawców a następnie wprowadzenie niezbędnych wyłączeń w krytycznych zasobach.

W swoim komunikacie z 29 stycznia 2020 Komisja Europejska potwierdziła, że *państwa członkowskie zgodziły się co do konieczności oceny profilu ryzyka poszczególnych dostawców i w konsekwencji stosowania odpowiednich ograniczeń wobec dostawców uznanych za stwarzających wysokie ryzyko, w tym niezbędnych wyłączeń, aby skutecznie łagodzić ryzyko w odniesieniu do kluczowych aktywów, jak wskazano w zestawie narzędzi[[56]](#footnote-57)).*

Biorąc pod uwagę powyższe stanowisko unijne zasadne jest wprowadzenie procedury umożliwiającej zbadanie ryzyk związanych z danym dostawcą sprzętu lub oprogramowania. W przypadku, gdyby ryzyka dla bezpieczeństwa państwa okazały się zbyt wysokie, taki dostawca powinien być uznany za stwarzający wysokie ryzyko.

W art. 66a została dodana kompetencja ministra właściwego do spraw informatyzacji do przeprowadzenia postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Postępowanie to będzie prowadzone w celu ochrony ważnych interesów państwowych w postaci bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego. Tak jak wyżej wspomniano kwestia cyberbezpieczeństwa sieci 5G jest kwestią strategiczną dla Unii Europejskiej z uwagi na współzależności pomiędzy sieciami telekomunikacyjnymi państw członkowskich UE. Ze względu na potencjalne szkody, które może przynieść zakłócenie funkcjonowania tych sieci jest to również materia dotycząca bezpieczeństwa państwa. Jednakże przepis nie zamyka się wyłącznie do sieci 5G. Postępowaniu będzie mógł być poddany dostawca produktów, usług i procesów ICT nie tylko dla sieci 5G, ale również dla innych systemów informacyjnych – jeżeli będzie spełniona przesłanka zapewnienia ochrony bezpieczeństwa państwa.

W rozumieniu artykułu 66a dostawcą sprzętu lub oprogramowania jest dostawca produktów ICT, usług ICT lub procesów ICT[[57]](#footnote-58)). Zgodnie z definicją dostawcy może to być producent, importer, dystrybutor. Dzięki temu postępowaniem będą mogły być objęte wszystkie podmioty kluczowe w łańcuchu dostaw. Postępowanie nie będzie dotyczyło wszystkich produktów, usług i procesów ICT pochodzących od konkretnego dostawcy sprzętu lub oprogramowania, lecz tylko tych, które są wykorzystywane przez:

1. podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorów usług kluczowych, dostawców usług cyfrowych, czy podmiotów publicznych:
   1. operatorzy usług kluczowych świadczą usługi kluczowe, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej,
   2. dostawcy usług cyfrowych świadczą usługi cyfrowe (internetowa platforma handlowa, usługa przetwarzania w chmurze, wyszukiwarka internetowa), które są niezbędne dla zapewnienia funkcjonowania współczesnego społeczeństwa informacyjnego,
   3. podmioty publiczne realizują, za pomocą systemów informacyjnych, zadania publiczne na rzecz obywateli;
2. przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacji szczególnego zagrożenia (obecnie, na gruncie Prawa telekomunikacyjnego jest to 69 podmiotów):
   1. przedsiębiorcy ci mają za zadanie m. in. współpracę z podmiotami i służbami wykonującymi zadania w zakresie
      * ratownictwa, niesienia pomocy ludności,
      * obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;
3. właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej w uzasadnieniu zwani operatorami infrastruktury krytycznej (100-200 podmiotów)). Operatorzy infrastruktury krytycznej zarządzają infrastrukturą krytyczną, którą stanowią systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców.

Podmioty te są szczególnie ważne dla zapewnienia bezpieczeństwa państwa, dlatego konieczne jest, żeby korzystały z bezpiecznego sprzętu lub oprogramowania w trakcie świadczenia usług na rzecz państwa i obywateli. Podkreślić należy, że choć niniejszą nowelizacją dodaje się do podmiotów krajowego systemu cyberbezpieczeństwa przedsiębiorców komunikacji elektronicznej, to niniejsze postępowanie ma dotyczyć sprzętu lub oprogramowania wykorzystywanego przez przedsiębiorców komunikacji elektronicznej sporządzających plany działań w sytuacjach szczególnych zagrożeń.

Do postępowania w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będą miały zastosowanie przepisy Kodeksu postępowania administracyjnego (Kpa). Dzięki temu dostawca sprzętu lub oprogramowania będzie brał udział w postępowaniu na prawach strony, z odmiennościami wynikających ze szczególnych regulacji wynikających z przepisów nowelizacji. W postępowaniu nie będą stosowane przepisy następujących artykułów Kpa:

* Art. 28 – projekt wprowadza wyjątek, że w tym szczególnym postępowaniu stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka.
* Art. 31 – wyłącza się udział organizacji społecznej w postępowaniu;
* Art. 51 – wyłącza się przepis, który zawęża osobiste stawiennictwo do obrębu gminy lub miasta, w którym zamieszkuje albo przebywa osoba, jak również sąsiedniej gminy albo miasta;
* Art. 66a – wyłącza się przepis dotyczący prowadzenia metryki sprawy;
* Art. 79 – wyłącza się przepis o udziale strony w przeprowadzeniu dowodu;

Wyłączenia tych przepisów Kpa są niezbędne ze względu na szczególny charakter tego postępowania, które ma na celu zapewnienie bezpieczeństwa narodowego.

W celu usprawnienia przebiegu postępowania i wzmocnienia trwałości rozstrzygnięć konieczne jest zawężenie przymiotu strony oraz udziału organizacji społecznej, mając na względzie, że do każdego takiego postępowania, według zasad ogólnych mogłoby przystąpić na prawach strony nawet setki podmiotów korzystających z konkretnych produktów pochodzących od konkretnego dostawcy sprzętu lub oprogramowania.

Wyłączenie art. 28 Kpa jest konieczne, ponieważ postępowanie jest wszczynane z urzędu przez ministra albo na wniosek przewodniczącego Kolegium – co za tym idzie stroną jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka. Podobne rozwiązanie znajduje się w art. 88 ust. 1 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów.

Z kolei wyłączenie art. 31 Kpa wynika ze szczególnego związku tego postępowania z kwestiami bezpieczeństwa narodowego.

Ze względu na ogólnopolski zasięg decyzji jaka ma zostać wydana w tym postępowaniu został wyłączony art. 51 Kpa.

Kwestia metryki sprawy przy tego typu postępowaniu jest złożona. Obowiązkowo w ramach postepowania o uznaniu dostawcy za dostawcę wysokiego ryzyka będą przeprowadzane szerokie analizy podmiotu, którego dotyczy postępowanie oraz jego produktów. Ujawnienie nazwisk osób, które przeprowadzały te analizy mogłoby narazić ich na działania ze strony podmiotów zainteresowanych konkretnym wynikiem sprawy. Ponadto wiele z tych osób to funkcjonariusze, których tożsamość, ze względu na wykonywane zadania, musi być chroniona. Z powyższych względów wyłączony został art. 66a Kodeksu postępowania administracyjnego.

W związku z wrażliwym charakterem informacji, jakie będą wykorzystywane w ramach tego postępowania, konieczne jest wyłączenie udziału strony z przeprowadzanych dowodów.

Jednocześnie umożliwiono przystąpienie do postępowania na prawach strony kilkunastu największych przedsiębiorców komunikacji elektronicznej. Będą to tacy przedsiębiorcy komunikacji elektronicznej, którzy w poprzednim roku obrotowym uzyskali przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych. Aby przystąpić do postępowania taki przedsiębiorca będzie obowiązany złożyć stosowny wniosek. Zmiana odpowiada na postulaty strony społecznej, jednocześnie zapewniając sprawny przebieg postępowania.

Decyzja ministra właściwego do spraw informatyzacji będzie miała formę decyzji administracyjnej, co pozwoli dostawcy na złożenie skargi do wojewódzkiego sądu administracyjnego.

W przypadku, gdy dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) zawiadomienie o wszczęciu postępowania publikowane jest na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Publikacja ma skutek doręczenia po upływie 14 dni od dnia jej dokonania. Przepis ten stanowi szczególną regulację w stosunku do zasad doręczeń określonych w Kpa.

Zawiadomienie o wszczęciu postępowania wobec dostawcy, który ma siedzibę na terytorium Unii Europejskiej, Konfederacji Szwajcarskiej czy państwa członkowskiego EFTA będzie doręczane na zasadach ogólnych wynikających z Kpa. Natomiast po otrzymaniu potwierdzenia doręczenia informacja o tym będzie publikowana na stronie Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, aby uprawnieni przedsiębiorcy telekomunikacyjni mogli złożyć wniosek o dopuszczenie do postępowania na prawach strony.

Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka będzie wszczynane z urzędu przez ministra właściwego ds. informatyzacji lub na wniosek przewodniczącego Kolegium. Minister właściwy do spraw informatyzacji jest odpowiedzialny za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym, stąd też zasadne jest, aby to on prowadził tego rodzaju postępowanie. Przed wydaniem decyzji minister właściwy ds. informatyzacji będzie obowiązany zwrócić się do Kolegium o wydanie opinii w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka. Kolegium będzie miało 3 miesiące, od dnia wystąpienia o opinię, na przekazanie jej do ministra. Termin od dnia wystąpienia o opinię do dnia otrzymania opinii nie będzie wliczał się do terminu załatwienia sprawy.

Art. 66a ust. 10 zawiera wskazanie elementów analizy, która ma być zawarta w opinii Kolegium. W większości nawiązują one do pkt. 2.37 raportu Unii Europejskiej dotyczącego unijnej oceny ryzyka cyberbezpieczeństwa sieci 5G[[58]](#footnote-59)).

Celem opinii Kolegium jest kompleksowa analiza działalności dostawcy sprzętu lub oprogramowania. W skład Kolegium wchodzą ministrowie kluczowi dla bezpieczeństwa państwa a także szefowie służb specjalnych. Będą więc w stanie pozyskać niezbędne informacje do oceny dostawcy od swoich jednostek podległych lub nadzorowanych.

Zasadne jest, aby opinia podejmowała kwestie zagrożeń, które stwarza dostawca. Nie są to jednak zwykłe zagrożenia, lecz takie, które wpływają na bezpieczeństwo narodowe. Przepis dalej precyzuje, że chodzi o zagrożenia w wymiarze ekonomicznym, wywiadowczym oraz terrorystycznym[[59]](#footnote-60)). Ponadto konieczna będzie analiza zagrożeń, które stwarza dostawca dla zobowiązań sojuszniczych (np. w ramach NATO czy innych umów międzynarodowych) a także europejskich. Niewątpliwie zobowiązaniem europejskim jest zapewnienie na poziomie unijnym wysokiego poziomu bezpieczeństwa systemów informacyjnych (co wynika z dyrektywy NIS/NIS2) oraz bezpieczeństwa sieci i usług komunikacji elektronicznej (co wynika z EKŁE).

Kolejnym aspektem opinii powinna być analiza prawdopodobieństwa, z jakim dostawca znajduje się pod wpływem państwa. Ta część opinii skupia się na powiązaniach dostawcy sprzętu lub oprogramowania z państwem spoza Unii Europejskiej oraz NATO. Wpływ ten może obejmować prawodawstwo danego państwa, które reguluje stosunki między państwem a dostawcą (np. w zakresie swobody działalności gospodarczej czy bezpieczeństwa przetwarzanych danych). Co istotne Kolegium powinno pochylić się także nad praktyką stosowania tych przepisów, aby sprawdzić, jak one funkcjonują - np. czy gwarancje zawarte w tych przepisach rzeczywiście są respektowane przez dane państwo.

Z uwagi na to, że współcześnie coraz więcej danych osobowych jest przesyłanych poza Unię Europejską ważna jest także kwestia ochrony danych osobowych w danym państwie - i kwestia faktycznego stosowania tych przepisów.

Opinia będzie także zawierała analizę struktury własnościowej dostawcy sprzętu lub oprogramowania - chodzi tutaj o ustalenie kto faktycznie sprawuje kontrolę własnościową nad dostawcą. Finalnie powinny być sprawdzone możliwości wpływu danego państwa na dostawcę.

Opinia będzie więc dotyczyła otoczenia regulacyjnego dostawcy, faktycznego stosowania prawa, struktury własnościowej aż po faktyczny wpływ państwa na dostawcę. Po dokonaniu analiz uzyskany zostanie całościowy obraz relacji między dostawcą a państwem.

Rozporządzeniem wykonawczym Rady (UE) 2020/1125 z dnia 30 lipca 2020 r. wykonującym rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim Unia Europejska wskazała podmioty, które dokonują cyberataków na Unię lub jej państwa członkowskie. Wskazane jest, aby opinia Kolegium dotyczyła również jakie są relacje pomiędzy tymi podmiotami a dostawcą sprzętu lub oprogramowania.

Jak już wyżej wspomniano ryzyka dotyczą również aspektów technicznych produktów, usług i procesów ICT dostarczanych przez dostawcę. Dlatego do technicznych aspektów opinii należy analiza:

1. liczby i rodzajów wykrytych podatności i incydentów dotyczących zakresu typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;
2. tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt. 1–4 oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
3. treść wydanych wcześniej rekomendacji, o których mowa w art. 33, dotyczących sprzętu lub oprogramowania danego dostawcy.

Jest to związane z potencjalnymi ryzykami, które wiążą się z niską jakością sprzętu lub oprogramowania. Jak wyżej wspomniano podatności mogą być wykorzystane do cyberataków przez państwa, grupy APT czy grupy przestępcze – dlatego warto zbadać jakość produktów dostarczanych przez dostawcę.

Realizując postulaty strony społecznej dodano wymóg, aby prowadząc opinię Kolegium uwzględniło także certyfikaty produktów, usług i procesów ICT dostarczanych przez dostawcę oraz wyniki analiz łańcuchów dostaw, które przeprowadziły zespoły CSIRT poziomu krajowego oraz CSIRT INT.

Procedura sporządzania opinii Kolegium została określona w art. 66a ust. 12. Opinia zostanie przygotowana przez zespół opiniujący w skład, którego wchodzą przedstawiciele członków Kolegium. Każdy członek zespołu opiniującego przygotowuje stanowisko w zakresie swojej właściwości. Przewodniczący Kolegium będzie miał kompetencję do rozstrzygnięcia ewentualnego negatywnego sporu co do zakresu tej właściwości poprzez wskazanie właściwego członka zespołu opiniującego. Wprowadzono obowiązek przeprowadzenia analiz łańcuchów dostaw, o których mowa w art. 64a, zanim zostanie sporządzona opinia Kolegium w sprawie dostawcy.

Po przeprowadzeniu postępowania minister właściwy do spraw informatyzacji wyda decyzję uznającą dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli z przeprowadzonego postępowania wynika, że dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. Nie chodzi więc o zwykłe zagrożenie, tylko o jego kwalifikowaną postać. Decyzja będzie zawierać wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka – ponieważ one też stwarzają zagrożenie.

Dzięki prawnemu zidentyfikowaniu dostawcy wysokiego ryzyka będzie możliwe wprowadzenie dodatkowych środków mitygujących zagrożenie, jakie stwarza sprzęt lub oprogramowanie dostarczane przez dostawcę wysokiego ryzyka. Ze względu na charakter sprawy – stwierdzenie poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi – decyzja ta będzie podlegała natychmiastowej wykonalności. Wskazać należy, że zastosowane w przepisie przesłanki w żaden sposób nie odnoszą się do pochodzenia dostawcy. Za dostawcę wysokiego ryzyka może być uznany zarówno podmiot zagraniczny jak również podmiot działający w kraju. Wszyscy przedsiębiorcy są obowiązani do działania w sposób nie zagrażający bezpieczeństwu państwa polskiego.

Jeżeli w trakcie postępowania zostanie stwierdzone, że dostawca nie stanowi poważnego zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, to zgodnie z zasadami ogólnymi Kpa zostanie wydana decyzja o umorzeniu postępowania.

Aby podmioty obowiązane do wycofania sprzętu mogły zastosować się do obowiązków wynikających z wydania tej decyzji administracyjnej, minister właściwy do spraw informatyzacji opublikuje ją w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, na stronie podmiotowej ministra w Biuletynie Informacji Publicznej, a także na stronie internetowej urzędu obsługującego ministra.

Od decyzji w sprawie uznania za dostawcę wysokiego ryzyka nie będzie przysługiwał wniosek o ponowne rozpatrzenie sprawy. Prawa strony postępowania będą zagwarantowane poprzez możliwość złożenia skargi do sądu administracyjnego.

#### Nowy art. 66b

Następstwem prawnego zidentyfikowania dostawcy wysokiego ryzyka powinno być zmitygowanie ryzyka, które on stwarza. Art. 66b wprowadza więc niezbędne wymogi bezpieczeństwa dla podmiotów krajowego systemu cyberbezpieczeństwa, operatorów infrastruktury krytycznej czy 69 przedsiębiorców komunikacji elektronicznej w związku z wykorzystywaniem sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka.

Podmioty krajowego systemu cyberbezpieczeństwa, operatorzy infrastruktury krytycznej, przedsiębiorcy komunikacji elektronicznej sporządzający plany działań w sytuacji szczególnego zagrożenia, nie będą mogły wprowadzać do użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka. Dotyczyć to będzie zarówno nowych produktów, usług i procesów, jak i używanych. W tym przypadku chodzi o sytuację, w której w chwili wydania decyzji dany podmiot nie ma danego produktu, usługi lub procesu ICT – nie będzie mógł więc ich używać lub z nich korzystać. Celem jest, aby nie wprowadzać kolejnych produktów, usług, procesów ICT, żeby nie zwiększać już i tak wysokiego ryzyka związanego z nimi.

Innym obowiązkiem będzie wycofanie z użytkowania zakresów typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, jednak nie później niż 7 lat od dnia opublikowania informacji o decyzji. Chodzi tutaj o sytuację, w której w chwili wydania decyzji o uznaniu za dostawcę wysokiego ryzyka dany podmiot już używa lub korzysta z produktów, usług i procesów ICT uwzględnionych w decyzji o uznaniu za dostawcę wysokiego ryzyka. Będzie więc musiał wycofać go w terminie 7 lat. Jest to związane z tym, że natychmiastowe wycofanie produktów, usług i procesów ICT mogłoby być niemożliwe w praktyce, gdyż mogłoby spowodować zaprzestanie świadczenia usług.

Natomiast przedsiębiorcy komunikacji elektronicznej, posiadający lub korzystający z typów produktów ICT, rodzajów usług ICT, konkretnych procesy ICT wskazanych w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy będą musieli wycofać je w ciągu 5 lat od ogłoszenia decyzji. 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.

Jednocześnie wprowadzono przepis umożliwiający użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją w sprawie uznania za dostawcę wysokiego ryzyka, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji. Będzie to możliwe wyłącznie, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń. Te same przepisy zostały zastosowane do podmiotów publicznych, które już zakupiły określony sprzęt w drodze zamówienia publicznego. Jest to niezbędne rozwiązanie zarówno dla zapewnienia ciągłości świadczenia usług jak również ochrony dyscypliny finansów publicznych.

Wyżej zaproponowana interwencja prawodawcy jest konieczna ze względu na istotność dla bezpieczeństwa państwa usług świadczonych przez podmioty obowiązane do wycofania sprzętu lub oprogramowania. Podmioty te mogą być związane wieloletnimi umowami z dostawcą wysokiego ryzyka na dostarczanie sprzętu lub oprogramowania czy świadczenie usług serwisowych. Bez prawnego obowiązku stopniowego wycofania sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka podmioty te nie wycofają sprzętu lub oprogramowanie m. in. z uwagi na ryzyko odpowiedzialności kontraktowej wobec dostawcy. W konsekwencji ryzyko związane ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka nie zostanie skutecznie zmitygowane.

Podkreślić należy, że jest to wyjątek od podstawowej reguły zakazu wprowadzania do użytkowania i obowiązku wycofania ww. sprzętu lub oprogramowania w ciągu 5-7 lat. Wyjątek ten nie może być interpretowany rozszerzająco.

Wyjaśnienia wymaga termin *użytkowania* użyty w tym przepisie. Nie należy go utożsamiać z użytkowaniem z Kodeksu cywilnego, które jest ograniczonym prawem rzeczowym. Użytkowanie w rozumieniu art. 66b oznacza każdy przypadek używania czy korzystania z produktu, usługi, procesu ICT do świadczenia usług przez dany podmiot.

Należy podkreślić, że w zaproponowanych przepisach prawa nie ma mechanizmu nakazującego natychmiastowe wycofanie sprzętu lub oprogramowania wskazanego w ocenie ryzyka dostawców. Podmioty krajowego systemu cyberbezpieczeństwa, w tym operatorzy usług kluczowych, czy przedsiębiorcy telekomunikacyjni, zostaną zobowiązani do wycofania danego sprzętu lub oprogramowania w określonym czasie. 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.

Proponowane rozwiązania mają wpływ na swobodę działalności gospodarczej podmiotów zobowiązanych do wycofania sprzętu – wpływają bowiem na wolność podejmowania decyzji gospodarczych. Mają także wpływ na wykonywanie niektórych atrybutów prawa własności tj. prawa do używania produktów. Wskazać należy, że przepisy te mają na celu mitygację ryzyk związanych ze sprzętem lub oprogramowaniem pochodzącym od dostawcy wysokiego ryzyka. Tak jak wyżej wspomniano korzystanie z takiego sprzętu mogłoby doprowadzić do poważnych ryzyk naruszenia poufności danych oraz naruszenia dostępności usługi. Co za tym idzie doprowadziłoby to do poważnego utrudnienia funkcjonowania obywateli - współczesnego społeczeństwa informacyjnego - a także do ryzyka przejęcia kontroli nad infrastrukturą krytyczną państwa. Wycofanie sprzętu lub oprogramowania pochodzących od dostawcy wysokiego ryzyka jest zatem konieczne do zapewnienia funkcjonowania demokratycznego państwa prawnego.

Proponowane rozwiązania nie naruszają istoty swobody prowadzenia działalności gospodarczej. Ogranicza się wykorzystywanie przez przedsiębiorców konkretnego sprzętu lub oprogramowania do świadczenia usług - w pozostałym zakresie przedsiębiorcy będą mogli swobodnie podejmować decyzje biznesowe. Przepisy te nie naruszają również istoty prawa własności. Tak jak wyżej wspomniano nie ma mechanizmu natychmiastowego wycofania sprzętu lub oprogramowania - przez czas wycofywania z użytkowania podmioty te będą mogły w pełni wykonywać prawo własności. Ponadto w czasie wycofywania będzie można wprowadzić dotychczas posiadany sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka, aby dokonać niezbędnych napraw usterek czy awarii, aby zapewnić ciągłość świadczenia usługi – pokazuje to, że istota prawa własności nie została naruszona. Co ważne sprzęt lub oprogramowanie pochodzący od dostawcy wysokiego ryzyka i tak podlegałby stopniowej wymianie ze względu na zużycie czy postęp technologiczny. Proponowane rozwiązanie wpisuje się więc w mechanizm stopniowej wymiany sprzętu.

Proponowane rozwiązanie wpłynie na swobodę prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka. Należy jednak podkreślić, że będzie to związane z poważnym zagrożeniem dla państwa, które stwarza ten dostawca. Jednakże istota prowadzenia działalności gospodarczej przez dostawcę wysokiego ryzyka nie zostanie naruszona. Taki dostawca nadal będzie mógł prowadzić działalność gospodarczą.

Podkreślić należy, że wartością konstytucyjną, która w tej sytuacji powinna być bardziej chroniona od swobody prowadzenia działalności gospodarczej czy prawa własności jest bezpieczeństwo państwa. Państwo powinno odpowiednio zaadresować problem dostawcy wysokiego ryzyka, który może, dzięki podatnościom w sprzęcie lub oprogramowaniu które dostarczył, doprowadzić do ataku na infrastrukturę krytyczną państwa (np. inteligentne sieci energetyczne, sieci telekomunikacyjne), zakłócać funkcjonowanie organów państwa (np. poprzez ataki *man in the middle*, kradzież danych) czy zakłócić działanie kluczowych dla społeczeństwa usług (np. poprzez atak na systemy i urządzenia szpitalne, bez których znacznie utrudnione jest wykonywanie operacji ratujących życie). Może to się odbyć poprzez celowo zaprojektowane ukryte podatności lub również ukryte podatności powstałe w wyniku aktualizacji oprogramowania dostarczonego przez dostawcę wysokiego ryzyka. Wykorzystanie podatności w infrastrukturze telekomunikacyjnej, której elementy dostarczył taki dostawca, mogłoby utrudnić lub uniemożliwić funkcjonowanie usług komunikacji elektronicznej na danym obszarze.

Demokratyczne państwo prawne nie może być bezbronne i musi zawczasu identyfikować poważne zagrożenia dla jego funkcjonowania oraz skutecznie je mitygować. Ryzyka stwarzanego przez dostawcę wysokiego ryzyka (który działa pod wpływem obcych służb wywiadowczych lub grup przestępczych) oraz jego sprzęt lub oprogramowanie nie da się inaczej zmitygować, jak tylko poprzez stopniowe wycofanie takiego sprzętu. Podmioty korzystające z tych produktów, usług, procesów nie będą w stanie zidentyfikować ukrytych podatności, poprzez które dostawca wysokiego ryzyka będzie mógł dokonywać ataków. W związku z tym nie jest możliwe zmitygowanie ryzyka stwarzanego przez dostawcę wysokiego ryzyka poprzez wprowadzenie dodatkowych środków bezpieczeństwa, innych niż wycofanie sprzętu lub oprogramowania, ponieważ będą one nieskuteczne wobec ukrytych podatności pozwalających np. nagle wyłączyć sprzęt czy zakłócić telekomunikację między podmiotami.

Zmitygowanie ryzyka sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nie jest także możliwe poprzez obowiązkową certyfikację sprzętu lub oprogramowania. Standardy certyfikacyjne nie zawsze będą w stanie pomóc przy wykryciu ukrytych podatności, zwłaszcza jeśli sam producent chce je ukryć. Ponadto standardy te są znane samemu producentowi, który może to wykorzystać.

Warto raz jeszcze podkreślić, że postępowanie w sprawie uznania za dostawcę wysokiego ryzyka będzie postępowaniem administracyjnym. Dostawca będzie mógł przedstawić swoje racje w postępowaniu zanim zostanie uznany za dostawcę wysokiego ryzyka. Decyzja będzie mogła być zaskarżona do sądu administracyjnego, co zapewnia dostawcy możliwość obrony swoich praw. Dostawca będzie mógł być uznany za dostawcę wysokiego ryzyka, jeżeli będzie spełniał szczególnego rodzaju przesłanki - będzie stwarzał poważne zagrożenie dla obronności, bezpieczeństwa państwa.

Podsumowując - zanim dostawca zostanie uznany za dostawcę wysokiego ryzyka jego sprawa zostanie wszechstronnie wyjaśniona - nastąpi to poprzez opinię Kolegium oraz czynności przeprowadzone przez ministra właściwego do spraw informatyzacji. Dostawca będzie mógł przedstawić swoje stanowisko a w przypadku uznania za dostawcę wysokiego ryzyka - kwestionować to przed sądem administracyjnym.

#### Nowy art. 66c

Organy właściwe do spraw cyberbezpieczeństwa będą mogły zwracać się do podmiotów krajowego systemu cyberbezpieczeństwa o udzielenie informacji w sprawie wycofywanych produktów ICT, usług ICT i procesów ICT. Podobne kompetencje będzie miał w stosunku do przedsiębiorców telekomunikacyjnych Prezes UKE. Przepis wzmocni kompetencje organów i zapewni im możliwość monitorowania procesu wycofywania produktów ICT, usług ICT i procesów ICT.

#### Nowy art. 66d

W artykule 66d wprowadzono przepisy dotyczące procedury przed sądem administracyjnym, jest to więc przepis o charakterze *lex specialis* do ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz. U. 2023 r. poz. 259 i 803) (dalej – PPSA). Jest on wzorowany na art. 38 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756), która dotyczy rozpoznania skargi na decyzję o odmowie wydania poświadczenia bezpieczeństwa. Przepis ma za zadanie pogodzić dwie wartości prawne – prawo do złożenia skargi na decyzję administracyjną oraz ochronę informacji niejawnych, których ujawnienie mogłoby narazić państwo na niepowetowane szkody. Sąd administracyjny będzie rozpoznawał skargę na decyzję o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka na posiedzeniu niejawnym. Z kolei sentencja wyroku z uzasadnieniem zostanie doręczona tylko ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie wymaga utajnienia ze względu na ochronę informacji niejawnych. Takie sformułowanie przepisu będzie zgodne z wyrokiem Trybunału Konstytucyjnego, który za niekonstytucyjne uznał brak doręczenia jawnych elementów wyroku sądu administracyjnego[[60]](#footnote-61)). Przepis stanowi niezbędne odstąpienie od zasady ustności i jawności, jednakże strona będzie miała możliwość składania pism procesowych, jak w każdym innym postępowaniu przed sądem administracyjnym.

Rozwiązanie to jest konieczne dla zapewnienia bezpieczeństwa demokratycznego państwa prawnego – ujawnienie informacji niejawnych wykorzystanych w postępowaniu o uznaniu za dostawcę wysokiego ryzyka mogłoby narazić Rzeczpospolitą na niepowetowane szkody. Nie została naruszona istota prawa do sądu, ponieważ w zakresie w jakim uzasadnienie nie zawiera informacji niejawnych (uzasadnienie prawne, kwestia wykładni, ustalenia organu niepodlegające utajnieniu) zostanie doręczone skarżącemu, dzięki czemu będzie mógł złożyć skargę kasacyjną. Rozwiązanie jest też proporcjonalne sensu stricto, bowiem sędziowie mają z urzędu dostęp do wszystkich materiałów niejawnych, które będą zgromadzone w sprawie. Będą więc mogli skrupulatnie zbadać legalność postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Na poparcie tego rozwiązania warto tutaj odwołać się do wyroku Naczelnego Sądu Administracyjnego z 8 marca 2017 r. sygn. akt I OSK 1312/15: *strona skarżąca – z istoty sprawy mająca ograniczony dostęp do szeregu informacji z nią związanych – powinna móc działać w zaufaniu, że zasadniczo pełny dostęp do informacji posiada sąd, do którego zwraca się ona o kontrolę działania organu administracji publicznej, i że tę kontrolę sąd ten dokona w sposób niezależny i niezawisły w oparciu o pełną wiedzę wynikającą z ustaleń organu, w tym także niejawnych*.

#### Nowy art. 66e

Projektowany art. 66e określa, że minister właściwy do spraw informatyzacji będzie prowadził wykaz decyzji o uznaniu za dostawcę wysokiego ryzyka w podziale na produkty, usługi i procesy w nich wskazane. Ułatwi to dostęp do informacji o niebezpiecznych produktach, usługach i procesach ICT.

### Ostrzeżenie

#### Nowy art. 67a

Przepisy nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa zawierają dodanie szczególnego środka – ostrzeżenia (art. 67a). Jego stosowanie będzie ograniczone do niektórych grup podmiotów gospodarki i społeczeństwa. Będzie mogły być stosowane w przypadku ryzyka wystąpienia (ostrzeżenie) incydentu krytycznego. Incydent krytyczny jest najbardziej dotkliwym w skutkach typem incydentu cyberbezpieczeństwa, skutkującym znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi. Incydent krytyczny jest klasyfikowany przez zespoły CSIRT poziomu krajowego, a więc najpierw operator usługi kluczowej, dostawca usługi cyfrowej lub podmiot publiczny zgłaszają właściwy incydent, który następnie – po przeprowadzeniu należytej oceny – może być uznany przez CSIRT poziomu krajowego za incydent krytyczny.

Obecnie państwo nie dysponuje środkami prawnymi, które umożliwiałyby skuteczną reakcję na incydent krytyczny. Oczywiście za obsługę incydentu krytycznego odpowiada jeden z zespołów CSIRT poziomu krajowego, który będzie współpracował z podmiotem, u którego wystąpił incydent krytyczny. Podkreślić jednak należy, że cyberataki mogą nie dotyczyć jednego podmiotu, a skutki takich ataków mogą się rozszerzać na inne podmioty w bardzo szybkim czasie. Zespoły CSIRT mogą nie nadążyć w obsłudze takiego incydentu krytycznego, który dotyczy wielu podmiotów. Jako przykład można podać sytuację, gdy cały świat zmagał się z podatnością Log4Shell. Była to krytyczna podatność, która mogła być wykorzystywana przez grupy *advanced persistent threat*[[61]](#footnote-62)). Innym przykładem są ataki na wiele podmiotów administracji rządowej na Ukrainie.

Przed wydaniem ostrzeżenia niezbędne będzie przeprowadzenie analizy uzasadniającej wydanie tych środków nadzwyczajnych. Analiza będzie przeprowadzana wspólnie z Zespołem do spraw incydentów krytycznych. Zespół ten jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz ministra właściwego do spraw informatyzacji. Jest to zespół ekspercki mający ułatwić reakcję na incydent krytyczny.

Pełnomocnik będzie mógł wydać ostrzeżenie, które będzie miękkim, niewiążącym środkiem wskazującym na ryzyko związane z możliwością wystąpienia incydentu krytycznego oraz zalecającym określone działania zmniejszające ryzyko wystąpienia tego incydentu. Instrument ten jest wzorowany na ostrzeżeniach wydawanych przez czeską Narodową Agencję Bezpieczeństwa Cybernetycznego i Informacji. Ostrzeżenie jako miękki środek będzie zawierało zalecenie określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu. Katalog możliwych zaleceń został wskazany w art. 67a ust. 9. Może to być m.in. zalecenie zastosowania określonej poprawki bezpieczeństwa, szczególnej konfiguracji sprzętu lub oprogramowania lub zalecenie zaprzestania korzystania z określonego sprzętu lub oprogramowania. Decyzja o zastosowaniu się do ostrzeżenia będzie należała do adresatów ostrzeżenia.

#### Nowy art. 67b

Z uwagi na konstytucyjną niezależność Narodowego Banku Polskiego nie będą do niego stosowały się przepisy dotyczące wycofania produktów ICT, usług ICT, procesów ICT pochodzących od dostawcy wysokiego ryzyka. Minister właściwy do spraw informatyzacji będzie informował Prezesa Narodowego Banku Polskiego o wydaniu decyzji o uznaniu danego dostawcy za dostawcę wysokiego ryzyka. Prezes Narodowego Banku Polskiego zdecyduje zatem czy wycofa produkty ICT, usługi ICT oraz procesy ICT wskazane w decyzji o uznaniu dostawcy za dostawcę wysokiego ryzyka.

#### Nowy art. 67c

W art. 67c dodano opcjonalną możliwość przekazania zadań zespołów CSIRT, określonych w art. 26, Ministrowi Obrony Narodowej. Decyzję w tej sprawie podejmie Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium do Spraw Cyberbezpieczeństwa oraz w uzgodnieniu z Ministrem Obrony Narodowej. W decyzji zostaną określone m.in. zakres, czas powierzenia zadań a także fakultatywnie szczegóły współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV. Zadania te będą realizowane przez Ministra Obrony Narodowej za pomocą jego jednostek podległych lub przez niego nadzorowanych. Decyzja będzie ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Ponadto celem poinformowania podmiotów krajowego systemu cyberbezpieczeństwa informacja o ogłoszeniu decyzji będzie publikowana na stronach internetowych CSIRT GOV, CSIRT MON, CSIRT NASK lub jest udostępniania w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

### Zmiany w przepisach o administracyjnych karach pieniężnych

W związku ze zmianami w przepisach materialnych należało odpowiednio zmodyfikować przepisy o karach administracyjnych. Kary administracyjne pełnią w systemie prawa przede wszystkim funkcję prewencyjną oraz represyjną[[62]](#footnote-63)), dlatego niezbędne jest ich prawidłowe ustanowienie oraz zapewnienie skutecznego stosowania. W art. 73 ustawy, będącym przedmiotowo-podmiotowym katalogiem kar pieniężnych, wprowadzono zmiany zarówno techniczne, ujednolicające jak i dodano przesłanki ponoszenia odpowiedzialności przez operatora usługi kluczowej. Nadto wprowadza się w ustawie o Krajowym Systemie Cyberbezpieczeństwa karę na operatora usługi kluczowej, który z własnej winy nie korzysta z systemu S46 w celu realizacji obowiązków z art. 11, czyli przekazywania zgłoszeń incydentów poważnych. Kara nie będzie więc nakładana np. w sytuacjach siły wyższej, gdy z powodów technicznych nie było możliwości przekazania zgłoszenia. Ponadto wprowadza się karę za brak współdziałania operatora usługi kluczowej z CSIRT sektorowym podczas obsługi incydentu poważnego, a także za niezapewnienie temu zespołowi dostępu do informacji o rejestrowanych incydentach.

Co więcej nowelizacja przewiduje poszerzenie katalogu podmiotów, które będą podlegały obligatoryjnej odpowiedzialności karnoadministracyjnej. W szczególności przewidziane zostały kary za posługiwanie się certyfikatem lub deklaracją zgodności w przypadku niespełniania przez dany produkt warunków określonych w programie certyfikacji. Zapewnia to, że próby nadużycia systemu będą spotykały się ze zdecydowaną reakcją. Odpowiedzialności podlegać będą też m.in. osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, które utrudniają lub uniemożliwiają właściwym organom prowadzenie czynności kontrolnych. Wysokość kar administracyjnych została odpowiednio zróżnicowana tak by były one skuteczne, proporcjonalne do czynu oraz odstraszające (art. 73 ust.1a–1c).

Przewidziano także kary dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka. Kara dla podmiotów zobowiązanych do wycofania sprzętu dostawcy uznanego za dostawcę wysokiego ryzyka będzie nakładana w sytuacji naruszenia przez te podmioty obowiązków określonych w art. 66b, a zatem w sytuacji wprowadzania do użytkowania typów produktów, rodzajów usług i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka lub w sytuacji niewycofania z użytkowania przedmiotowych produktów, usług bądź procesów ICT dostarczanych przez dostawcę wysokiego ryzyka w terminie do 7 lat od ogłoszenia lub udostępnienia informacji o decyzji. Obydwie kary będą wynosiły do 3% całkowitego rocznego światowego obrotu danego podmiotu z poprzedniego roku obrotowego. W przypadku podmiotów publicznych kara będzie wynosić do 100 000 zł.

Ponadto, niezależnie od kary pieniężnej w przypadku podmiotu publicznego, który nie wyznaczył osób, o których mowa w art. 21 ustawy, minister właściwy do spraw informatyzacji zyskuje uprawnienie do nałożenia w drodze decyzji na kierującego podmiotem publicznym, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek. Podobne rozwiązanie przyjęto przy niewypełnianiu przez podmiot obowiązków informacyjnych o których mowa w art. 66c, przy czym w tym wypadku kara pieniężna nałożona na kierującego podmiotem może wynosić do 300% jego miesięcznego wynagrodzenia. Sankcję tą może w drodze decyzji nałożyć organ uprawniony do żądania informacji zgodnie z właściwością, która została określona w art. 66c ust. 2. Jak zostało powyżej podniesione, jest to uprawnienie ministra do spraw informatyzacji bądź innego właściwego organu (art. 66 ust. 2), a zatem odpowiedzialność karnoadministracyjna w tym przypadku jest fakultatywna.

Odnosząc się do fakultatywnej odpowiedzialności karnoadministracyjnej, należy wskazać, że art. 73 ust. 2d wprowadza możliwość nałożenia kary pieniężnej wyłącznie, gdy przemawia za tym charakter lub zakres naruszenia. Takie określenie jest niezbędne, aby zapewnić proporcjonalność w rozumieniu konieczności i adekwatności nakładanej kary do zakresu naruszenia. Może się również okazać, że działanie bądź zaniechanie podmiotu przejawia znikomą szkodliwość społeczną wobec czego niecelowe byłoby obligatoryjne karanie kierującego podmiotem. Wyjaśnienia wymagają jednak pojęcia „zakres naruszenia” oraz „charakter naruszenia”.

Zakres naruszenia można zdefiniować jako rozmiar naruszenia oraz częstotliwość naruszeń. Zakres naruszenia jest niezbędny do określenia stopnia szkodliwości społecznej czynu sprawcy, a więc pozwala na określenie rzeczywistych oraz potencjalnych skutków naruszenia prawa. Ze względu na to, że jest to pojęcie o charakterze stopniowalnym, dokonując oceny organ nakładający karę administracyjną powinien brać pod uwagę w szczególności podstawowe cele ustawy oraz szkodliwość naruszenia tj. rodzaj naruszonych obowiązków i dóbr, intensywność naruszenia, następstwa oraz wysokość wyrządzonej szkody[[63]](#footnote-64)).

Charakter naruszenia należy rozumieć jako stopień zawinienia osoby podlegającej odpowiedzialności karnoadministracyjnej, tj. czy czyn został przez nią popełniony z winy umyślnej lub nieumyślnej[[64]](#footnote-65). Określając zatem charakter naruszenia organ obowiązany jest do ustalenia czy osoba podlegająca odpowiedzialności karnoadministracyjnej w tym przypadku popełniła ten czyn w zamiarze bezpośrednim, ewentualnym, poprzez lekkomyślność albo niedbalstwo. Od tego ustalenia zależeć będzie właśnie decyzja o odstąpieniu od nałożenia kary bądź o jej nałożeniu oraz wysokości.

W art. 74 wskazano organy właściwe do wymierzania administracyjnych kar pieniężnych, o których mowa w artykule poprzedzającym. Wprowadzono ogólną zasadę, że karę na przedsiębiorców komunikacji elektronicznej za niewycofanie sprzętu lub oprogramowania pochodzącego od dostawcy wysokiego ryzyka nakłada Prezes UKE. Z kolei kary na operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej będą nakładać organy właściwe do spraw cyberbezpieczeństwa. W pozostałych przypadkach kary będzie nakładał minister właściwy do spraw informatyzacji.

W celu zagwarantowania prawidłowego przebiegu postępowania, a tym samym wymierzenia adekwatnej do popełnionego czynu kary pieniężnej, w stosunku do podmiotów obowiązanych do wycofania sprzętu bądź oprogramowania dostarczanego przez dostawcę wysokiego ryzyka (art. 66a ust. 1 pkt 1–4 wprowadzony zostaje art. 74a, który nakłada na te podmioty obowiązek dostarczenia danych organowi uprawnionemu do nakładania kary na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania. Jeżeli jednak dane nie zostały organowi doręczone bądź uniemożliwiają one ustalenie podstawy wymiaru kary pieniężnej, organ uprawniony do jej nałożenia ustala podstawę wymiaru kary w sposób szacunkowy biorąc pod uwagę wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu. Przyjęcie takiego rozwiązania ma przyczynić się do zapewnienia realizacji zasady szybkości postępowania oraz zasady proporcjonalności.

Mając na uwadze konieczność zapewnienia sprawnego przekazywania zgłoszeń incydentów z CSIRT sektorowego czy CSIRT INT do właściwego CSIRT poziomu krajowego wprowadza się karę za nie wykonanie tego obowiązku. Kara będzie nakładana na kierownika CSIRT sektorowego i CSIRT INT w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku.

W związku z nałożeniem na przedsiębiorców komunikacji elektronicznej zadań i obowiązków, wprowadza się sankcje za niewykonywanie obowiązków wyszczególnionych w art. 76a–76c. Zgodnie z tymi przepisami, karze pieniężnej podlegać będzie przedsiębiorca komunikacji elektronicznej, który:

1. nie wypełnia obowiązku systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia, o którym mowa w art. 20 ust. 2;
2. nie podejmuje środków, o których mowa w art. 20a ust. 2 pkt 2;
3. nie dokumentuje czynności, o których mowa w art. 20a ust. 2 pkt 1 i 2;
4. nie przekazuje informacji, o których mowa w art. 20b ust. 2, w terminie wskazanym w żądaniu Prezesa UKE;
5. nie wykonuje obowiązku, o którym mowa w art. 20b ust. 4, w terminie wskazanym w decyzji Prezesa UKE;
6. nie obsługuje incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;
7. nie zgłasza poważnego incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;
8. nie współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco lub z właściwym CSIRT GOV, CSIRT MON, CSIRT NASK i tym samym nie wykonuje obowiązku, o którym mowa w art. 20d ust. 1 pkt 3 i 4;
9. nie usuwa, w wyznaczonym przez Prezesa UKE terminie, podatności, która doprowadziła lub mogła doprowadzić do incydentu telekomunikacyjnego lub krytycznego, o której mowa w art. 54a;
10. nie wykonuje zaleceń pokontrolnych Prezesa UKE, o których mowa w art. 59.

Ponadto, zgodnie z art. 76 ust. 2 sankcje przewiduje się za:

1. niewyznaczenie przez przedsiębiorcę komunikacji elektronicznej dwóch osób, o których mowa w art. 20a ust. 4;
2. niezapewnienie dostępu do informacji o rejestrowanych przez przedsiębiorcę komunikacji elektronicznej incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań;
3. niewykonywanie obowiązku, o którym mowa w art. 20f ust. 1 i 2;
4. niewykonywanie obowiązku, o którym mowa w art. 20h ust. 5.

Kary w powyżej przytoczonych sytuacjach będzie nakładał Prezes UKE. Należy jednak zwrócić uwagę na to, że art. 76a ust. 1 i ust. 2 dotyczy dwóch różnych odpowiedzialności karnoadministracyjnych. Pierwsza sytuacja to odpowiedzialność o charakterze obligatoryjnym, a zatem Prezes UKE będzie miał obowiązek nałożenia kary pieniężnej na przedsiębiorcę komunikacji elektronicznej, gdy zajdą przesłanki enumeratywnie wymienione w art. 76a ust. 1. W ust. 2 przewiduje się odpowiedzialność fakultatywną, wobec czego nadaje się uprawnienie Prezesowi UKE do nałożenia kary pieniężnej na przedsiębiorcę komunikacji elektronicznej, jeżeli przemawia za tym charakter lub zakres naruszenia. Przesłanki dotyczące charakteru i zakresu naruszenia należy rozumieć analogicznie względem uzasadnienia art. 73 ust. 2d. Wprowadza się również dopuszczalność nałożenia kary pieniężnej nawet w sytuacji zaprzestania naruszania prawa przez podmiot bądź naprawienia wyrządzonej przez niego szkody. Uprawniony będzie do tego Prezes UKE po uznaniu, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

Powyższe kary będą nakładane przez Prezesa UKE w drodze decyzji, której nie nadaje się rygoru natychmiastowej wykonalności. Górna granica nałożonej kary została ustalona na poziomie 3% przychodu ukaranego podmiotu osiągniętego w poprzednim roku kalendarzowym. Przepisy przewidują również sposób ustalania wysokości wymiaru kary, w przypadku, gdy podmiot nie osiągnął przychodu bądź nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary.

Wymierzanie kar pieniężnych co do zasady będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych tj. przy zastosowaniu przepisów działu 4A Kodeksu Postępowania Administracyjnego (z możliwością odwołania i drogi sądowej).

### Strategiczna sieć bezpieczeństwa

#### Nowy art. 76c.

Celem tworzonej strategicznej sieci bezpieczeństwa jest zapewnienie realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego w aspekcie telekomunikacyjnym, czyli związanym z nadawaniem, odbiorem lub transmisją informacji, niezależnie od ich rodzaju, za pomocą przewodów, fal radiowych bądź optycznych lub innych środków wykorzystujących energię elektromagnetyczną. Podmiotem zobowiązanym do jej uruchomienie oraz zarządzania będzie operator strategicznej sieci bezpieczeństwa (OSSB). Przepis ten precyzuje również, że strategiczna sieć bezpieczeństwa jest siecią telekomunikacyjną w rozumieniu Prawa komunikacji elektronicznej.

Stworzenie strategicznej sieci bezpieczeństwa jest niezbędne i konieczne, ponieważ usługi telekomunikacyjne związane z obronnością i bezpieczeństwem państwa powinien świadczyć podmiot kontrolowany w całości przez państwo, wolny od wpływów podmiotów trzecich. w szczególności infrastruktura telekomunikacyjna służąca tego rodzaju usługom powinna być pod kontrolą państwa.

Istotne jest zapewnienie, aby dane na temat osób realizujących zadania z zakresu obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego podczas wypełniania obowiązków służbowych były w jak najmniejszym stopniu przetwarzane przez podmioty niepubliczne. Utworzenie strategicznej sieci bezpieczeństwa jest przydatne do osiągnięcia tego celu bowiem sieć ta będzie odrębna od innych sieci telekomunikacyjnych i będzie zarządzana przez podmiot znajdujący się pod kontrolą państwa.

Utworzenie strategicznej sieci bezpieczeństwa jest konieczne do osiągnięcia ww. celu. Obecnie organy administracji korzystają, przy realizacji zadań z zakresu obronności czy bezpieczeństwa państwa z usług operatorów znajdujących się, ze względu na strukturę, pod wpływem podmiotów trzecich. Sytuacja ta może zagrażać bezpieczeństwu przekazywanych informacji, a co za tym idzie zagraża bezpieczeństwu państwa.

Utworzenie strategicznej sieci bezpieczeństwa oraz jej operatora jest zdaniem projektodawcy najmniej uciążliwym rozwiązaniem. Podkreślić należy, że nie chodzi tutaj o utworzenie operatora, który świadczyłby usługi telekomunikacyjne do wykonywania wszystkich zadań administracji. Operator ten będzie świadczył jedynie usługi telekomunikacyjne związane ze szczególnymi zadaniami – tymi związanymi z bezpieczeństwem państwa. W pozostałym zakresie organy administracji będą mogły w swobodnym zakresie korzystać z usług różnych przedsiębiorców telekomunikacyjnych. Strategiczna sieć bezpieczeństwa będzie zapewniała poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych niezbędny do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Operatora strategicznej sieci cyberbezpieczeństwa będzie wyznaczał Prezes Rady Ministrów. Wpierw będzie zasięgał opinii Kolegium do Spraw Cyberbezpieczeństwa w tej sprawie. Wskazanie, jako organu wyznaczającego Operatora strategicznej sieci bezpieczeństwa, Prezesa Rady Ministrów wynika ze szczególnej pozycji ustrojowej tego organu, który na mocy art. 148 Konstytucji Rzeczypospolitej Polskiej nie tylko reprezentuje Radę Ministrów i kieruje jej pracami, ale także zapewnia wykonywanie polityki Rady Ministrów. Polski system prawa sytuuje władzę wykonawczą jako odpowiedzialną za zapewnienie obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, przypisując zadania w tych obszarach poszczególnym organom administracji rządowej, w szczególności ministrom kierującym działami administracji rządowej. Tworzona strategiczna sieć bezpieczeństwa ma zapewnić bezpieczną komunikację na potrzeby realizacji tych zadań, jej Operator ma świadczyć usługi w ramach tej sieci podmiotom realizującym zadania z zakresu bezpieczeństwa państwa. Ponadto, Prezes Rady Ministrów jest przewodniczącym zarówno Kolegium do Spraw Służb Specjalnych, Rządowego Zespołu Zarządzania Kryzysowego, jak i Kolegium do Spraw Cyberbezpieczeństwa. A zatem wskazanie Prezesa Rady Ministrów jako organu wyznaczającego operatora strategicznej sieci bezpieczeństwa jest w pełni uzasadnione.

Przez pojęcie zarządzania siecią, użyte w art. 76c ust. 2, należy rozumieć dokonywanie wszelkich czynności zarządczych związanychzarówno z bieżącym utrzymaniem tej sieci, zapewnieniem bezpieczeństwa, w tym bezpieczeństwa świadczonych w sieci usług, jak i modernizacją i rozwojem sieci, które są nierozerwalnie związane z podnoszeniem poziomu bezpieczeństwa oraz jakości świadczonych usług.

Wprowadza się fakultatywne upoważnienie ustawowe do wydania rozporządzenia przez Prezesa Rady Ministrów. Organ ten będzie mógł określić w rozporządzeniu minimalne wymagania techniczne jakie musi spełniać strategiczna sieć bezpieczeństwa oraz minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo–technicznej.

#### Nowy art. 76d.

Strategiczna sieć bezpieczeństwa będzie zarządzana przez OSSB wskazanego przez Prezesa Rady Ministrów. Wybór Prezesa Rady Ministrów jest ograniczony do kręgu podmiotów, które spełniają łącznie następujące warunki:

* będących jednoosobową spółką Skarbu Państwa,
* będących przedsiębiorcą telekomunikacyjnym,
* posiadających infrastrukturę telekomunikacyjną niezbędną do zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego,
* posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej,
* posiadających świadectwo bezpieczeństwa przemysłowego pierwszego stopnia,
* dających rękojmię należytego wykonywania zadań operatora strategicznej sieci bezpieczeństwa.

Przyjęcie przez podmiot funkcji OSSB nastąpi po wyrażeniu przez niego zgody.

OSSB będzie przedsiębiorca telekomunikacyjny, który już dostarcza sieć telekomunikacyjną za wynagrodzeniem. Dlatego zasadne jest, aby działalność OSSB polegająca na zarządzaniu strategicznej sieci bezpieczeństwa była wyodrębniona m. in. pod kątem rachunkowości. Operator strategicznej sieci bezpieczeństwa ma świadczyć bezpieczne usługi dla szeregu kluczowych podmiotów administracji publicznej. Są to podmioty należące do różnych działów administracji rządowej. W związku z tym działalność OSSB będzie wpływać na realizację zadań administracji podlegającej różnym ministrom. Z tego względu jego wyznaczenie nie może zostać powierzone jednemu z ministrów, ale organowi, który posiada ogólne kierownictwo w kwestiach działań administracji publicznej.

#### Nowy art. 76e.

OSSB świadczy usługi telekomunikacyjne, a także może świadczyć inne usługi (np. w zakresie bezpieczeństwa, czy usługi związane z telekomunikacyjnym procesem inwestycyjnym) w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

OSSB oprócz możliwości korzystania, tak jak wszystkie inne podmioty cywilne, z częstotliwości przeznaczonych dla użytkowania cywilnego, będzie mógł także świadczyć swoje usługi telekomunikacyjne w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym. Zgodnie z obowiązującymi regulacjami częstotliwości rządowe lub użytkowane jako rządowe w użytkowaniu cywilno-rządowym, mogą być wykorzystywane wyłącznie przez określonych ustawą użytkowników, będących użytkownikami rządowymi.

Wykorzystanie częstotliwości rządowych przez OSSB będzie koordynowane przez Ministra Obrony Narodowej, jednakże koordynacja częstotliwości rządowych w zakresie 703–713 MHz oraz 758–768 MHz w drodze pewnego wyjątku zostaje powierzona Prezesowi Urzędu Komunikacji Elektronicznej (dalej jako „Prezes UKE”). Takie rozwiązanie jest konieczne ze względu na przewidzianą w niniejszej ustawie możliwość współużytkowania, w ramach jednej sieci telekomunikacyjnej, tych częstotliwości z częstotliwościami cywilnymi z zakresu 713–733 MHz oraz 768–788 MHz. W takim przypadku, organ regulacyjny odpowiedzialny za gospodarowanie widmem w Polsce musi mieć realne narzędzia, które umożliwią właściwe, a przede wszystkim niepowodujące szkodliwych zakłóceń, użytkowanie, współużytkowanych zakresów widma radiowego. Z tego także powodu wykorzystanie częstotliwości rządowych z zakresu 703–713 MHz oraz 758–768 MHz będzie wymagać uzyskania pozwolenia radiowego, które nie jest wymagane dla użytkowników rządowych.

#### Nowy art. 76f

W ust. 1. wskazano, żeOSSB będzie świadczył na wniosek usługi telekomunikacyjne podmiotom najważniejszym z punktu widzenia bezpieczeństwa państwa, tj.: Kancelarii Prezydenta RP, Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezesa Rady Ministrów, Biuru Bezpieczeństwa Narodowego, urzędom obsługującym organy administracji rządowej, organy jednostek samorządu terytorialnego oraz instytucjom podległym tym organom lub przez nie nadzorowanym, wykonującym zadania z zakresu ochrony bezpieczeństwa i porządku publicznego, bezpieczeństwa i obronności państwa, ochrony granicy państwa, ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa, dostaw energii, ochrony interesów Rzeczypospolitej Polskiej za granicą, ochrony zdrowia, weterynaryjnej ochrony zdrowia publicznego, nadzoru sanitarnego, ochrony środowiska, sprawiedliwości, w tym sądownictwa i prokuratury, Siłom Zbrojnym Rzeczypospolitej Polskiej oraz innym jednostkom organizacyjnym podległym lub nadzorowanym przez Ministra Obrony Narodowej.

W zakresie art. 76f ust. 1 pkt 6 należy podkreślić, że usługi OSSB świadczone na rzecz urzędów obsługujących organy administracji rządowej będą wykorzystywane przede wszystkim przy realizacji zadań określonych w przepisach jako zadania organu. W praktyce zadania te wykonywane są przez pracowników urzędów obsługujących dany organ. W związku z tym nie istnieją przeszkody, które uniemożliwiałyby korzystanie z usług operatora przy wykonywaniu ustawowych zadań organów.

Jednocześnie OSSB będzie świadczył usługi telekomunikacyjne także instytucjom wykonującym na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa, również na wniosek tych podmiotów.

Projekt zakłada nałożenie na ww. podmioty obowiązku korzystania z usług telekomunikacyjnych świadczonych przez OSSB w ruchomej publicznej sieci telekomunikacyjnej w zakresie niezbędnym do zapewnienia w tych podmiotach realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Przyjęcie takiego rozwiązania ma zapewnić bezpieczeństwo informacji przekazywanych przy wykorzystaniu świadczonych przez OSSB usług. Jednocześnie, z uwagi na charakter działalności, obowiązek ten nie dotyczy służb specjalnych a także Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek podległych lub nadzorowanych przez Ministra Obrony Narodowej (projektowany art. 76f ust. 3). Jeżeli jednak służby specjalne albo Siły Zbrojne Rzeczypospolitej Polskiej podejmą decyzję o korzystaniu z usług telekomunikacyjnych świadczonych przez OSSB to na podstawie projektowanego art. 76f ust. 1 będą mogły wystąpić do OSSB o świadczenie takich usług.

Art. 76f ust. 4–6.

Przepis art. 76f ust. 4 przewiduje, że Prezes Rady Ministrów będzie mógł zobowiązać OSSB do świadczenia usług właścicielom i posiadaczom obiektów, instalacji lub urządzeń infrastruktury krytycznej, a także przedsiębiorcom realizującym zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny. Wprowadzenie takiego uprawnienia dla Prezesa Rady Ministrów zwiększy elastyczność w reagowaniu na aktualne potrzeby w zakresie zapewnienia bezpiecznej wymiany informacji pomiędzy kluczowymi podmiotami odpowiedzialnymi za realizację zadań z zakresu obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Prezes Rady Ministrów będzie mógł podejmować takie działania na wniosek odpowiednio ministra, we właściwości którego znajduje się określony system infrastruktury krytycznej lub Ministra Obrony Narodowej.

Z kolei przepis art. 76f ust. 5 ustawy wprowadza możliwość zlecenia OSSB świadczenia usługi wsparcia technicznego przy realizacji zadań Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Państwowej Straży Pożarnej, Służby Ochrony Państwa oraz Policji. Usługi te są ściśle powiązane ze świadczonymi przez OSSB usługami telekomunikacyjnymi w związku z czym świadczenie ich przez inny podmiot byłoby co najmniej nieefektywne, a w wielu przypadkach niemożliwe.

Usługi wsparcia technicznego mogą polegać w szczególności na utrzymaniu, rozbudowie i modyfikacji sieci teleinformatycznych w zakresie sieci rozległych oraz zestawienia i utrzymania łączy dostępowych do takich sieci.

Świadczenie usług telekomunikacyjnych, usług wsparcia technicznego oraz innych usług, o których mowa w art. 76e ust. 1 i art. 76f ust. 1 i 2 wymaga zawarcia umowy pomiędzy stronami (art. 76f ust. 6), a umowa to musi odnosić się do jakości usług, co najmniej w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego (art. 76f ust. 7). Wskazano, że umowa określa również zasady odpłatności za świadczone usługi.

Rozwiązania zawarte w art. 76e oraz 76f zawierają rozwiązania niezbędna dla zapewnienia efektywności świadczenia usług przez OSSB. W szczególności usługi wsparcia technicznego oraz usługi badawczo-rozwojowe muszą być zapewniane w ramach bezpiecznej sieci telekomunikacyjnej. Rozdzielenie tych usług od usług telekomunikacyjnych byłyby nieefektywne, gdyż w efekcie dwa podmioty miałyby dostęp do sieci telekomunikacyjnej stosowanej przez OSSB. Prowadziłoby to potencjalnie do dodatkowych kosztów związanych z wpuszczeniem nowego podmiotu do tego systemu oraz wymagałoby to wprowadzenia dodatkowych środków bezpieczeństwa związanych z dostępem do informacji podmiotu zajmującego się świadczeniem usług wsparcia. Taka sytuacja jest nieakceptowalna z punktu widzenia wrażliwego charakteru danych jakie będą przesyłane za pośrednictwem strategicznej sieci bezpieczeństwa. Dopuszczenie dodatkowych osób do takich informacji zawsze zwiększa ryzyko wycieku danych w związku z czym inne środki nie są w stanie zapewnić realizację celów jakie służą utworzeniu strategicznej sieci bezpieczeństwa.

#### Nowy art. 76g.

Przepis przesądza, że przy zawieraniu umów dotyczących realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, z późn. zm.), gdyż umowy te są ściśle związane z ochroną istotnych interesów bezpieczeństwa państwa. Aby wyłączenie doszło do skutku muszą być więc spełnione dwie przesłanki – umowy muszą dotyczyć zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji oraz zachodzić konieczność ochrony istotnych interesów bezpieczeństwa państwa. Jest to rozwiązanie zgodne z art. 13 lit. a dyrektywy 2009/81/WE, zgodnie z którym nie stosuje się postanowień tejże dyrektywy do zamówień, w przypadku których stosowanie dyrektywy zobowiązałoby państwo członkowskie do dostarczenia informacji, których ujawnienie uznaje się za sprzeczne z jego podstawowymi interesami w zakresie bezpieczeństwa.

Wprowadzone wyłączenie jest niezbędne dla realizacji celu jaki stawia sobie niniejsza ustawa. Aby strategiczna sieć bezpieczeństwa realnie przyczyniła się do wzrostu poziomu bezpieczeństwa komunikacji kluczowych podmiotów niezbędne jest zapewnienie, aby wszystkie relewantne podmioty korzystały z tej sieci. Jeśli chociaż część z nich nie będzie z niej korzystała to przesyłanie do nich informacji wrażliwych będzie obarczone dodatkowym ryzykiem. Mamy tu do czynienia ze specyficznym efektem sieciowym, w którym korzyści z danego rozwiązania są tym większe im większa jest skala danego przedsięwzięcia. W związku z powyższym wszystkie podmioty, na rzecz których obowiązki powinien świadczyć, muszą mieć możliwość uzyskania jego usług tak szybko jak to możliwe. Z tego względu konieczne jest umożliwienie im jak najszybszego zawarcia umowy z OSSB.

Ponadto wyłączenie, o którym mowa w art. 76g ust. 1, mieści się w zakresie art. 12 ust. 1 lit. b ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych. Operatorem strategicznej sieci bezpieczeństwa będzie jednoosobowa spółka Skarbu Państwa, a więc istnieje zależność między państwem a OSSB. Państwo poprzez nadzór właścicielski (wykonywanie swoich uprawnień) będzie miało wpływ na działalność OSSB. Dzięki temu spełnione zostaną wymagania wskazane w art. 12 ust. 1 lit. a oraz c dyrektywy 2014/24/UE.

Wskazać przy tym należy, że OSSB będzie świadczył usługi w ramach strategicznej sieci bezpieczeństwa dla *stationes fisci* Skarbu Państwa. Dlatego projektodawca uważa wymaganie wskazane w art. 12 ust. 1 lit. b dyrektywy 2014/24/UE za spełnione.

Równocześnie jednak należy zwrócić uwagę, że w praktyce zastosowanie art. 12 PZP wiązałoby się z licznymi problemami praktycznymi, gdyż każdorazowo zamawiający musiałby dokonywać ocenę czy można zastosować to wyłączenie. Mogłoby to rodzić wątpliwości prawne oraz przedłużać proces zawierania umów z OSSB. Aby uniknąć wskazanych problemów i potencjalnych opóźnień zdecydowano się wprowadzić art. 76g ust. 1. Pozwoli to zapewnić sprawny proces zawierania umów z OSSB nie naruszając przy tym przepisów prawa europejskiego.

Należy też zauważyć, że stosowanie ustawy z dnia 11 września 2019 r. -Prawo zamówień publicznych do kluczowych usług telekomunikacyjnych mogłoby prowadzić do ujawnienia przez państwo polskie kluczowych informacji związanych z podstawowym interesem bezpieczeństwa państwa, o których mówi art. 346 Traktatu o funkcjonowaniu Unii Europejskiej. Kluczowe kwestie związane z technicznymi zabezpieczeniami komunikacji między najistotniejszymi organami państwa muszą pozostać tajemnicą tak aby nie ułatwiać w żaden sposób działań państw nieprzyjaznych, które mogłyby próbować przejąć taką komunikację. Każda informacja o stosowanych metodach zabezpieczania komunikacji mogłaby przyczynić się do wzrostu ryzyka tej komunikacji. Wraz z agresją Rosji na Ukrainę znacząco wzrosło zagrożenie działaniami w tym zakresie. Nie możemy ignorować tego faktu przy przygotowywaniu przepisów mających służyć bezpośrednio interesom bezpieczeństwa państwa.

Zgodnie z ust. 2 ceny usług świadczonych przez OSSB będą kształtowane zgodnie z przepisami ustawy, tj. będą obejmowały koszty oraz rozsądną marżę. Rozwiązanie z rozsądną marżą występuje już w przepisach – por. art. 9mk ustawy z 28 marca 2003 r. o transporcie kolejowym. Mechanizm ten równoważy interesy zarówno OSSB jak i podmiotów zobowiązanych do zawarcia z nim umowy.

#### Nowy art. 76h

Prezes UKE będzie mógł przeprowadzić analizę cen usług telekomunikacyjnych stosowanych przez OSSB. Analiza ta będzie mogła być przeprowadzona na wniosek podmiotów korzystających z usług telekomunikacyjnych OSSB. Prezes UKE będzie miał 2 miesiące na przeprowadzenie analizy – od momentu złożenia wniosku. Jeżeli Prezes UKE stwierdzi, że ceny usług telekomunikacyjnych OSSB przekraczają koszty i rozsądną marżę to podmiot zobowiązany do zawarcia umowy z operatorem strategicznej sieci bezpieczeństwa będzie mógł rozpocząć procedurę zawarcia umowy o świadczenie usług telekomunikacyjnych z innym dostawcą usług. Po stronie OSSB powstanie również wtedy obowiązek przedstawienia usługobiorcy nowej oferty, która ponownie, na wniosek usługobiorcy, będzie podlegała analizie przez Prezesa UKE, tym razem w terminie 21 dni. Jeżeli ponownie Prezes UKE stwierdzi, że ceny usług świadczonych przez OSSB przekraczają koszty i rozsądną marżę, to będzie mógł wydać decyzję zmieniającą tą umowę. Operator strategicznej sieci bezpieczeństwa będzie również zobowiązany do udostępniania informacji na żądanie Prezesa UKE, tak aby zagwarantować, że organ będzie dysponował wszystkimi informacjami niezbędnymi do realizacji jego zadań.

Prezes UKE jako organ regulacyjny w dziedzinie rynku usług telekomunikacyjnych, jest jedynym podmiotem, który posiada kompetencję pozwalające mu ocenić czy cena zaproponowana przez OSSB odpowiada ponoszonym kosztom oraz rynkowym cenom podobnych usług. Należy podkreślić, że Prezes UKE w ramach swojej zwykłej działalności otrzymuje informacje o cenach usług oferowanych przez operatorów telekomunikacyjnych oraz jest z nimi w stałym kontakcie. Każdy inny organ musiałby osobno pozyskiwać informacje potrzebne do przeprowadzenia analiz.

#### Nowy art. 76i

Przepis ten reguluje obowiązki informacyjne OSSB wobec Prezesa UKE. OSSB będzie przekazywał Prezesowi UKE informacje o zawartej umowie na świadczenie usług za pośrednictwem strategicznej sieci bezpieczeństwa, w szczególności cenę oraz zakres świadczonych usług, w terminie 14 dni od dnia zawarcia umowy.

#### Nowy art. 76j

W art. 76j zapewniono operatorowi strategicznej sieci bezpieczeństwa możliwość uzyskania dostępu do infrastruktury technicznej, w tym współkorzystanie z niej, w celu realizacji zadań, o których mowa w art. 76c ust. 1. Wprowadzenie regulacji o charakterze szczególnym wobec przepisów art. 17-24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2023 r. poz. 733,) jest uzasadnione z uwagi na szczególny cel, któremu ma służyć wspomniany dostęp, tj. realizację zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji.

Rozwiązania zawarte w art. 76j zostały opracowane na kanwie funkcjonującej obecnie regulacji - art. 17-24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, bądź wprost do nich odsyłają. Jednocześnie, z uwagi na specyfikę zadań realizowanych przez operatora strategicznej sieci bezpieczeństwa i szczególny charakter sytuacji, w jakich uzyskanie przez niego dostępu do infrastruktury technicznej będzie konieczne, zdecydowano się na wprowadzenie pewnych odstępstw od przepisów ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych.

W ust. 3 wprost wskazano, iż opłaty z tytułu dostępu do infrastruktury technicznej określa się w wysokości, która umożliwia zwrot części kosztów, które ponosi operator sieci w związku z utrzymaniem tej infrastruktury oraz z zapewnieniem dostępu.

Zdecydowano również, że podstawową formą zapewnienia Operatorowi strategicznej sieci bezpieczeństwa dostępu do infrastruktury technicznej przez operatora sieci będzie umowa. Decyzja Prezesa UKE może być wydana wyłącznie w przypadku odmowy udzielenia dostępu do infrastruktury technicznej przez operatora sieci lub niezawarcia umowy o dostępie do infrastruktury technicznej w terminie 2 miesięcy od dnia złożenia wniosku o taki dostęp. W związku z powyższym, wobec Operatora strategicznej sieci bezpieczeństwa nie znajdą zastosowania przepisy art. 18 ust. 2–10 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych. W celu przyspieszenia procedury wydania decyzji w sprawie dostępu do infrastruktury technicznej, zrezygnowano także z konieczności dokonywania uzgodnień z Prezesem URE i Prezesem UTK, o których mowa w art. 22 ust. 6 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych.

#### Nowy art. 76k.

W analogiczny sposób jak dostęp do infrastruktury technicznej, uregulowana została w art. 76k możliwość uzyskania przez operatora strategicznej sieci bezpieczeństwa dostępu do nieruchomości – co do zasady przepis ten bazuje na rozwiązaniach zawartych w ustawie z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych. Dostęp do nieruchomości, w tym do budynku, o którym mowa w przepisie, polega na umożliwieniu umieszczenia na tej nieruchomości infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości.

Podmiotami obowiązanymi do zapewnienia operatorowi strategicznej sieci bezpieczeństwa dostępu do nieruchomości są użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa jednostka samorządu terytorialnego oraz właściciel lub zarządca nieruchomości.

Co istotne, w odróżnieniu od dostępu, o którym mowa art. 30 ust. 1 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, dostęp do nieruchomości przez operatora strategicznej sieci bezpieczeństwa nie ma na celu zapewnienia telekomunikacji w tym budynku, a realizację zadań, o których mowa w art. 76c ust. 1, czyli zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Ze względu na ten wyjątkowy charakter strategicznej sieci bezpieczeństwa i fakt, że jej celem jest realizacja zadań publicznych o szczególnym znaczeniu wprowadzono pewne odstępstwo od art. 30 ust. 3a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, zgodnie z którym dostęp do nieruchomości jest nieodpłatny. Zgodnie z ust. 4 pkt 2, jeżeli podmiotem zapewniającym dostęp jest jednostka samorządu terytorialnego, właściciel lub zarządca nieruchomości, operator strategicznej sieci bezpieczeństwa ponosi proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością, proporcjonalną część kosztów, które wystąpiły po stronie udostępniającego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu oraz koszty przywrócenia nieruchomości do stanu poprzedniego.

#### Nowy art. 76l

Od decyzji Prezesa UKE, o której mowa w ust. 76j ust. 5 oraz art. 76k ust. 5 w sprawie dostępu telekomunikacyjnego, jak również od decyzji w sprawie dostępu do nieruchomości użytkownika wieczystego lub zarządcy nieruchomości stanowiącej własność Skarbu Państwa lub jednostki samorządu terytorialnego, będzie przysługiwało odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

#### Nowy art. 76m.

Przepis zastrzega dla OSSB pierwszeństwo kupna sieci telekomunikacyjnych na wypadek, gdyby państwowa osoba prawna lub jednostka samorządu terytorialnego sprzedała je osobie trzeciej. Wprowadzono obowiązek poinformowania przez ww. podmioty OSSSB o zamiarze zbycia sieci telekomunikacyjnych. OSSB będzie miał nie krócej niż 2 tygodnia na skorzystanie z prawa pierwokupu. Do pierwokupu stosuje się przepisy rozdziału IV księgi III ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2022 r. poz. 1360, z późn. zm.).

#### Nowy art. 76n.

W sytuacjach nadzwyczajnych wzrasta potrzeba przekazywania sygnałów pomiędzy podmiotami realizującymi zadania z obszaru bezpieczeństwa państwa, porządku publicznego czy zarządzania kryzysowego. Czasowo może się okazać, że w takich sytuacjach, świadczący usługi tym podmiotom, OSSB nie dysponuje wystarczającymi zasobami częstotliwości, by zapewnić sprawną łączność wszystkim podmiotom zobowiązanym do działania w sytuacjach nadzwyczajnych na określonym obszarze. Dlatego uprawnia się Prezesa UKE do nałożenia w drodze decyzji administracyjnej na podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz udostępnienia zasobów częstotliwości z tego zakresu na rzecz OSSB. Uprawnienie to przysługuje, jeżeli wystąpi sytuacja szczególnego zagrożenia oraz gdy OSSB wykorzysta możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758-768 MHz. Decyzja ta będzie wydawana na uzasadniony wniosek OSSB, który będzie zawierał opis sytuacji szczególnego zagrożenia, wskazanie przyczyn pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758–768 MHz i wskazanie obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia. Decyzja Prezesa UKE będzie wydana na czas określony, nie dłuższy niż czas trwania sytuacji szczególnego zagrożenia i nie dłużej niż 72 godziny. Będzie miała ona rygor natychmiastowej wykonalności.

Podmiot dysponujący tymi częstotliwościami będzie musiał niezwłocznie, nie później niż w ciągu 1 godziny, udostępnić Operatorowi strategicznej sieci bezpieczeństwa zasoby częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz. Wprowadza się tutaj wyjątek – nie będą mogły być w ten sposób udostępnione częstotliwości wcześniej udostępnione Siłom Zbrojnym RP.

OSSB będzie obowiązany udostępnić Siłom Zbrojnym RP udostępnione mu przez podmiot dysponujący rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz zasoby częstotliwości z tego zakresu niezwłocznie, nie później niż w ciągu jednej godziny, na czas na jaki zostały mu udostępnione.

W przypadku udostępnienia częstotliwości operatorowi strategicznej sieci bezpieczeństwa, przedsiębiorca telekomunikacyjny nie uiszcza opłaty za prawo dysponowania częstotliwością, za okres udostępnienia częstotliwości

Wprowadza się także regulację odszkodowawczą - do roszczenia o odszkodowanie z tytułu strat poniesionych przez przedsiębiorcę telekomunikacyjnego wskutek wydania decyzji stosuje się odpowiednio przepisy ustawy z dnia 22 listopada 2002 r. o wyrównywaniu strat majątkowych wynikających z ograniczenia w czasie stanu nadzwyczajnego wolności i praw człowieka i obywatela (Dz. U. poz. 1955).

Proponowane rozwiązanie dotyczy sytuacji nagłych, kryzysowych, niebezpiecznych, gdy OSSB nie ma wystarczających zasobów do realizacji zwiększonego zapotrzebowania na jego usługi. Obwarowane jest szczególnymi przesłankami. Udostępnienie częstotliwości jest ograniczone czasowo do okresu trwania sytuacji szczególnego zagrożenia – po tym czasie OSSB ma obowiązek zwolnić zasoby. Z tych powodów należy uznać to rozwiązanie za proporcjonalne.

#### Nowy art. 76o.

Reguluje obowiązek operatorów telekomunikacyjnych określenia kanału komunikacji z operatorem strategicznej sieci bezpieczeństwa. Gwarantuje to, że w przypadku wystąpienia sytuacji kryzysowej Operator będzie w stanie szybko skontaktować się z operatorami telekomunikacyjnymi i zareagować na kryzys.

#### Nowy art. 76p

Art. 76p określa, że w zakresie nieuregulowanym w niniejszej ustawie do operatora strategicznej sieci bezpieczeństwa stosuje się odpowiednio przepisy ustawy – Prawo komunikacji elektronicznej. Oznacza to, że operator strategicznej sieci bezpieczeństwa posiada takie same prawa i obowiązki jak pozostali operatorzy telekomunikacyjni, z wyjątkiem kwestii uregulowanych w niniejszej ustawie.

#### Nowy art. 76q

Art. 76q zawiera kompetencję dla Prezesa Rady Ministrów, który może, w przypadku utraty przez OSSB co najmniej jednego z przymiotów niezbędnych do jego wyznaczenia, w drodze zarządzenia odwołać OSSB, oraz wyznaczyć nowego operatora strategicznej sieci bezpieczeństwa (art. 76q ust. 1), także z określeniem terminu skuteczności obu czynności (art. 76r ust. 2). Kompetencja ta ma charakter fakultatywny, aby zapewnić odpowiednią elastyczność, np. w sytuacji gdyby żaden podmiot w danym momencie nie spełniałby wymogów ustawowych lub w sytuacji gdy spółka wyznaczona jako OSSB przestałaby być w efekcie przekształceń spółką jednoosobową, a w ocenie Prezesa Rady Ministrów istniałaby nieproporcjonalne ryzyko związane ze zmianą OSSB w kontekście zapewnienia ciągłości świadczenia określonych usług w celu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

#### Nowy art. 76r.

Nowy operator strategicznej sieci bezpieczeństwa, wyznaczony przez Prezesa Rady Ministrów, jest następcą prawnym dotychczasowego operatora strategicznej sieci bezpieczeństwa w zakresie realizacji jego zadań. Poprzez przepis szczególny przesądzony jest skutek niektórych stosunków prawnych – umowy o świadczenie usług, do których odnosi się, poprzez odesłanie, art. 76f ust. 4, 10 i 11 ustawy, wygasają z mocy prawa w terminie 3 miesięcy od dnia wydania zarządzenia.

### Przyznanie częstotliwości z zakresu 703–713 MHz oraz 758–768 MHz

11 marca 2013 r., na podstawie art. 4 ust. 2 Decyzji o spektrum radiowym[[65]](#footnote-66)) Komisja Europejska udzieliła Europejskiej Konferencji Administracji Pocztowych i Telekomunikacyjnych (*European Conference of Postal and Telecommunications Administrations* - CEPT) zlecenia na opracowanie zharmonizowanych warunków technicznych dla pasma 700 MHz na potrzeby bezprzewodowych usług szerokopasmowej łączności elektronicznej w Unii oraz na potrzeby innych zastosowań, wspierających priorytety unijnej polityki widma radiowego. W ramach tego zlecenia, CEPT przedstawił sprawozdania nr 53[[66]](#footnote-67)) (w 2014 r.) i 60[[67]](#footnote-68)) (w 2016 r.), które stanowią podstawę technicznej harmonizacji pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w Europie. Komisja Europejska w komunikacie pt. „Strategia jednolitego rynku cyfrowego dla Europy”[[68]](#footnote-69)) przedstawiła wizję powszechnego dostępu do łączności wysokiej jakości dla przedsiębiorstw i obywateli. Strategia ta zapowiadała konkretne wnioski ustawodawcze Komisji, dotyczące m.in. skoordynowanego zwalniania zakresu 694–790 MHz. Bazując na sprawozdaniach CEPT, oraz biorąc pod uwagę prace legislacyjne nad decyzją zmieniającą przeznaczenia pasma 700 MHz w Unii, 28 kwietnia 2016 r. Komisja Europejska wydała Decyzję harmonizacyjną odnośnie zakresu częstotliwości 694–790 MHz[[69]](#footnote-70)). Tym samym zapewniono ujednolicone warunki techniczne, umożliwiające użytkowanie pasma 700 MHz na potrzeby naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej i innych zastosowań zgodnie z priorytetami polityki widma radiowego na szczeblu unijnym i krajowym. 17 maja 2017 r. Parlament Europejski i Rada wydały Decyzję w sprawie wykorzystania zakresu częstotliwości 470–790 MHz w Unii Europejskiej[[70]](#footnote-71)) (dalej: Decyzja o zmianie przeznaczenia), na mocy której Państwa Członkowskie UE zostały zobowiązane do udostępnienia pasma 700 MHz na potrzeby usług szerokopasmowych do 30 czerwca 2020 r. lub w uzasadnionych przypadkach najpóźniej do 30 czerwca 2022 r.

Zgodnie z Krajowym Planem Działań zmiany przeznaczenia pasma 700 MHz w Polsce, którego przyjęcie wymagane było Decyzją o zmianie przeznaczenia, 28 grudnia 2018 r. na podstawie z art. 1. ust. 1. Decyzji Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii, Polska wystąpiła do Komisji Europejskiej z informacją o konieczności odsunięcia terminu udostępnienia pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej do 30 czerwca 2022 r. Wskazanym przez Polskę uzasadnionym powodem odroczenia dopuszczenia do korzystania z częstotliwości z pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewnienia usług bezprzewodowej szerokopasmowej łączności elektronicznej po dniu 30 czerwca 2020 r. (art. 1 ust. 1) były nierozwiązane problemy dotyczące koordynacji transgranicznej skutkujące szkodliwymi zakłóceniami. Brak informacji ze strony Federacji Rosyjskiej, Republiki Białorusi oraz Ukrainy o wyłączeniu do 30 czerwca 2020 r. naziemnej telewizji, działającej w paśmie 700 MHz na terenie tych krajów, uniemożliwiłby de facto w sposób niezakłócony uruchomienie pasma 700 MHz na potrzeby naziemnych systemów zdolnych do zapewniania usług bezprzewodowej szerokopasmowej łączności elektronicznej na terenie Polski w wymaganym terminie tj. do 30 czerwca 2020 r.

Ramy krajowych działań wyznaczane są przez decyzje Unii Europejskiej oraz regulacje Międzynarodowego Związku Telekomunikacyjnego (International Telecommunications Union - ITU) stąd Krajowy Plan Działań zmiany przeznaczenia pasma 700 MHz w Polsce, stanowiący podstawę do dalszych decyzji ustawodawczych nie przesądza o kierunkach i sposobie wykorzystania tego zasobu. Z punktu widzenia realizacji Decyzji o zmianie przeznaczenia kluczowa jest więc zgodność podejmowanych działań na szczeblu krajowym z uwarunkowaniami Decyzji harmonizacyjnej. Zgodnie z tą Decyzją użytkowanie pasma 700 MHz do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej będzie opierało się o zharmonizowaną w skali europejskiej „podstawową aranżację” kanałów 2x30 MHz w zakresach 703- 733 MHz (FDD - Frequency Division Duplex łącze „w górę”) oraz 758–788 MHz (FDD - Frequency Division Duplex łącze „w dół”). W myśl Decyzji harmonizacyjnej ww. zakresy pasma 700 MHz powinny być użytkowane do świadczenia naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej w oparciu o zharmonizowaną aranżację kanałów (jako tzw. „aranżacja podstawowa”) oraz powiązane wspólne najmniej restrykcyjne warunki techniczne, jeżeli państwa członkowskie wyznaczą je do użytkowania w zastosowaniach innych niż przez sieci radiodyfuzyjne o dużej mocy.

Niemniej jednak państwa członkowskie UE mają swobodę decyzji w zakresie użytkowania części pasma częstotliwości 700 MHz w celu zaspokojenia szczególnych potrzeb krajowych. Oprócz naziemnych bezprzewodowych usług szerokopasmowej łączności elektronicznej powyższe obejmuje również użytkowanie zgodnie z priorytetami sektorowymi unijnej polityki widma radiowego, w szczególności na potrzeby Programme Making and Special Events (PMSE, bezprzewodowe urządzenia do transmisji sygnałów akustycznych), Public Protection and Disaster Relief (PPDR, łączność radiowa na potrzeby ochrony publicznej i pomocy w przypadku klęsk żywiołowych) i Internet of Things (IoT, Internet Rzeczy)) i  w celu zapewnienia efektywnego użytkowania widma.

#### Nowy art. 76s

Przepis ustawy zobowiązuje Prezesa UKE do przydzielenia, w drodze decyzji administracyjnej, OSSB określonego zakresu częstotliwości, przeznaczonego do użytkowania rządowego. Do decyzji Prezesa UKE odpowiednio należy stosować przepisy ustawy Prawo komunikacji elektronicznej dotyczące rezerwacji częstotliwości, regulujące między innymi okres, na który jest ona wydawana oraz jej treść. Jednocześnie w decyzji tej Prezes UKE obligatoryjnie określi zobowiązania pokryciowe, czyli nałożone na OSSB wymogi w zakresie pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o te częstotliwości.

Decyzja harmonizacyjna w tym kontekście wyraźnie wskazuje, że nie naruszając prawa państw członkowskich do organizowania i użytkowania swojego widma radiowego do celów bezpieczeństwa publicznego oraz obronności, jeżeli została wdrożona łączność radiowa PPDR, należy stosować warunki techniczne dla bezprzewodowych usług szerokopasmowej łączności elektronicznej określonych dla aranżacji podstawowej. Państwa członkowskie mogą więc dokonać przeznaczenia określonego zasobu z pasma 700 MHz zgodnie z wytycznymi wskazanymi w Decyzji harmonizacyjnej.

#### Nowy art. 76t

Przepis reguluje kwestię zmiany podmiotu, któremu przydzielono częstotliwości rządowe z zakresu 703–713 MHz oraz 758–768 MHz w przypadku odwołania lub zmiany podmiotu będącego OSSB. W takim przypadku nowy OSSB wstępuje w prawa i obowiązki związane z przydziałem tego zakresu częstotliwości określone w ustawie oraz decyzji Prezesa UKE. Takie rozwiązanie zapewni dalsze niezakłócone funkcjonowanie sieci i prawidłową realizację usług strategicznych.

### Finansowanie strategicznej sieci bezpieczeństwa

#### Nowy art. 76u.

Utworzenie, utrzymanie, rozwój i modernizacja infrastruktury strategicznej sieci bezpieczeństwa będą finansowane w formie dotacji celowej udzielanej operatorowi strategicznej sieci bezpieczeństwa przez ministra właściwego do spraw aktywów państwowych z części budżetu państwa, której jest dysponentem. Podstawą określenia wysokości dotacji będzie koszt realizacji poszczególnych zadań ustalony przez ministra właściwego do spraw aktywów państwowych. Łączna kwota dotacji zostanie oszacowana na podstawie przedstawionych przez operatora strategicznej sieci bezpieczeństwa danych dotyczących kosztu realizacji poszczególnych zadań z uwzględnieniem liczby zrealizowanych zadań. Szczegółowe warunki wypłaty środków, wysokość kwot przeznaczonych na realizację poszczególnych zadań, a także sposób i zasady rozliczeń będzie określała umowa zawarta pomiędzy tym ministrem a OSSB.

Jednocześnie ze środków tej dotacji Operator strategicznej sieci bezpieczeństwa nie będzie mógł finansować swojej działalności gospodarczej. Przepis ten zapewnia, że środki z dotacji zostaną wyłącznie spożytkowane na cele publiczne.

### Zmiany w art. 93

Artykuł 93 ustawy o KSC zawiera maksymalny limit wydatków z budżetu państwa dla poszczególnych części budżetowych, będących skutkiem finansowym wejścia w życie ustawy o KSC. Przepis ust. 8 oraz ust. 23 zawierają limity dla części budżetowej dla Komisji Nadzoru Finansowego. Część ta już nie istnieje – Urząd Komisji Nadzoru Finansowego jest obecnie państwową osobą prawną, a zasady jego finansowania określa rozdział 3 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym[[71]](#footnote-72)). Z tego powodu uchyla się przepisy art. 93 ust. 8 i 23 jako zbędne.

### Zmiany w załącznikach do ustawy

W sektorze ochrona zdrowia obecnie za operatora usługi kluczowej może zostać uznana jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia. Zmiana załącznika polegałaby na zastąpieniu wyrażenia „Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia” na „Jednostka podległa ministrowi właściwemu do spraw zdrowia lub przez niego nadzorowana”. Za operatora usługi kluczowej mogłaby być uznana każda jednostka podległa lub nadzorowana przez ministra właściwego do spraw zdrowia, która np. zarządza danymi epidemiologicznymi.

Ponadto w załączniku numer 1 w kolumnie „Rodzaj podmiotów” dotyczącej sektora „Ochrona zdrowia” usunięto:

* „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301 oraz z 2023 r. poz. 605 i 650).”
* „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”

Podmioty lecznicze, w przedsiębiorstwie których funkcjonują dział farmacji szpitalnej lub apteka szpitalna są faktycznie tożsame z podmiotami leczniczymi, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej. Brak jest jakiegokolwiek uzasadnienia dla istnienia wyodrębnienia takich podmiotów, ponieważ podmioty posiadające dział farmacji lub aptekę szpitalną są podmiotami leczniczymi, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.

W tym samym załączniku nr 1 w kolumnie „Rodzaj podmiotów” odnoszącej się do sektora Infrastruktury cyfrowej dodano nowy podmiot, jakim jest operator strategicznej sieci bezpieczeństwa.

## Zmiany w innych ustawach

Zgodnie z art. 10 w ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzaniu mieniem państwowym w art. 13 ust. 1 dodaje się pkt 31 w brzmieniu: „podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa”. Ta zmiana jest konsekwencją wprowadzenia do polskiego porządku prawnego operatora strategicznej sieci bezpieczeństwa, który nie powinien zbywać akcji lub praw z akcji należących do Skarbu Państwa.

Wprowadza się również zmianę w art. 226 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych. Artykuł ten reguluje sytuacje, w którym zamawiający odrzuca ofertę złożoną w ramach postępowania o zamówienie publiczne. Kolejną przesłanką odrzucenia oferty będzie sytuacja, gdy oferta obejmuje produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i poz. …) oraz usługę ICT lub proces ICT, określone w tej decyzji.

## Pozostałe przepisy przejściowe i dostosowujące

#### Art. 4

Celem art. 4 jest uregulowanie kwestii rozstrzygnięcia postępowań wszczętych o udzielenie zamówienia publicznego. Przepis przejściowy wprost rozstrzyga o stosowaniu do tych postępowań ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych w brzmieniu nadanym niniejszą ustawą, jeżeli zostały one wszczęte przed dniem wejścia w życie niniejszej ustawy, a jednocześnie nie zakończyły się wyborem wykonawcy albo unieważnieniem postępowania przed dniem opublikowania informacji o wydaniu decyzji o uznaniu dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, przy czym relewantną datą jest data publikacji w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

#### Art. 5

Artykuł ten reguluje funkcjonowanie niektórych umów w związku ze zmianami jakie zostały wprowadzone do art. 33 ustawy o krajowym systemie cyberbezpieczeństwa. Ponadto wskazuje, że dotychczasowe porozumienia dot. korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ustawy o ksc zachowują ważność.

#### Art. 6

Art. 6 reguluje kwestię utrzymania w mocy aktów wykonawczych do ustawy o krajowym systemie cyberbezpieczeństwa. Jest to niezbędne dla zapewnienia ciągłości działania w ramach krajowego systemu cyberbezpieczeństwa.

Utrzymane w mocy zostaną następujące rozporządzenia:

* Rozporządzenie Rady Ministrów z dnia 16 października 2018 r. w *sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej*[[72]](#footnote-73)*)* - do czasu wydania rozporządzenia z art. 10 ust. 5 znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy;
* Rozporządzenie Rady Ministrów z dnia 2 października 2018 r. w *sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa*[[73]](#footnote-74)*)* - do czasu wydania rozporządzenia z art. 66 ust. 9 znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa, jednak nie dłużej niż 36 miesięcy od dnia wejścia w życie niniejszej ustawy.

#### Art. 7

Zgodnie z tym artykułem operator usługi kluczowej wyznaczy 2 osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 14 dni od dnia wejścia w życie ustawy. Ponadto wskazuje się, że do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. Po dniu wydania komunikatu operator usługi kluczowej będzie zgłaszał incydenty do CSIRT sektorowego.

#### Art. 8

Zgodnie z tym przepisem z dniem wejścia w życie ustawy:

1) dotychczas powołane w ramach operatora usługi kluczowej wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo stają się SOC wewnętrznymi;

2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się podmiotami prowadzącymi SOC zewnętrzne.

#### Art. 9

Przepis ten stanowi, że przedsiębiorca komunikacji elektronicznej zgłasza incydenty telekomunikacyjne do CSIRT poziomu krajowego do czasu ogłoszenia komunikatu o osiągnięciu zdolności operacyjnej przez CSIRT Telco.

#### Art. 10

Przepis ten zobowiązuje CSIRT poziomu krajowego do dostosowania porozumień ws. przeniesienia właściwości CSIRT do zmian w art. 26.

#### Art. 11

Podmioty publiczne będą musiały wyznaczyć 2 osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa w terminie 3 miesięcy od dnia wejścia w życie ustawy.

#### Art. 12

Zgodnie z tym przepisem Pełnomocnik Rządu do spraw Cyberbezpieczeństwa oraz Przewodniczący Kolegium będą mogli złożyć zlecić badanie sprzętu lub oprogramowania, o którym mowa w art. 33 nie wcześniej niż 3 miesiące od wejścia w życie ustawy.

#### Art. 13

CSIRT Telco nie będzie brał udziału w uzgodnieniach sposobu zgłaszania incydentów telekomunikacyjnych do czasu wydania komunikatu o zdolności operacyjnej.

#### Art. 14

Art. 14 reguluje moment zgłaszania incydentów przez jednostki podległe MSZ do CSIRT INT.

#### Art. 15

Przewidziano termin 18 miesięcy od dnia wejścia w życie ustawy na powołanie przez organy właściwe do spraw cyberbezpieczeństwa CSIRT sektorowych.

Powyższy przepis przejściowy jest niezbędny na przeprowadzenie organizacji tych zespołów, w tym na zapewnienie środków w nowej ustawie budżetowej, jak również przygotowanie niezbędnych składników materialnych i pozyskanie wysoko kwalifikowanej kadry ekspertów.

Gdy CSIRT sektorowy zostanie utworzony, organ właściwy do spraw cyberbezpieczeństwa ogłosi komunikat o osiągnięciu przez CSIRT zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

#### Art. 16

Artykuł ten reguluje kwestie dot. pierwszego sprawozdania organu właściwego do spraw cyberbezpieczeństwa z działalności CSIRT sektorowego.

#### Art. 17

Zgodnie z tym artykułem dotychczas powołany sektorowy zespół cyberbezpieczeństwa (CSIRT KNF) staje się CSIRT sektorowym.

#### Art. 18-19

Przepisy te zawierają analogiczne regulacje dostosowujące co do utworzenia CSIRT Telco jak przy CSIRT sektorowym

#### Art. 20

Zgodnie z przepisem art. 20 Prezes Rady Ministrów wyznaczy OSSB w terminie do 30 dni od wejścia w życie ustawy. Termin zawarty w tym przepisie ma charakter instrukcyjny. Ponadto wskazuje, że Prezes Rady Ministrów podaje do publicznej wiadomości informacje o osiągnięciu pełnej zdolności operacyjnej do świadczenia usług przez Operatora strategicznej sieci bezpieczeństwa. Pozwoli to precyzyjnie ustalić moment od kiedy podmioty wskazane w art. 76g ust. 2 mają obowiązek zawarcia umowy z OSSB.

#### Art. 21

Przepis określa maksymalne limity wydatków dla poszczególnych części budżetu państwa w związku z wejściem w życie niniejszej ustawy.

#### Art. 22

Ustawa wejdzie w życie w terminie 6 miesięcy od dnia ogłoszenia. Ze względu na związki treściowe niniejsza ustawa powinna wejść w życie w tym samym dniu co ustawa – Prawo komunikacji elektronicznej.

# Pozostałe informacje

Wpływ projektu na działalność mikroprzedsiębiorców oraz małych i średnich przedsiębiorców został omówiony w ocenie skutków regulacji.

Projekt ustawy jest zgodny z prawem Unii Europejskiej.

Projektowana ustawa nie wymaga przedstawiania organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do art. 4 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa[[74]](#footnote-75)) projekt został zamieszczony w wykazie prac legislacyjnych.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa oraz uchwałą nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów[[75]](#footnote-76)) projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji w serwisie Rządowy Proces Legislacyjny.

Projektowana regulacja nie podlega notyfikacji technicznej w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych[[76]](#footnote-77)), które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie

przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego, zwanej dalej „dyrektywą 2015/1535”. Wiele przepisów zawartych w tym projekcie stanowi implementację prawa Unii Europejskiej. Ponadto wskazać należy, że dyrektywa 2015/1535 w art. 1 ust. 3 wprost wskazuje, że nie ma zastosowania do zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych. Taki charakter mają przepisy rozdziału 4a dotyczące telekomunikacji, które stanowią implementację art. 40 i 41 Europejskiego Kodeksu Łączności Elektronicznej[[77]](#footnote-78). Projektowane przepisy art. 66a i art. 66b ustawy o krajowym systemie cyberbezpieczeństwa mają na celu wdrożenie postanowień Unijnego zestawu narzędzi cyberbezpieczeństwa sieci 5G tzw. Toolbox 5G[[78]](#footnote-79). W swoim komunikacie z dnia 15 czerwca 2023 r. C (2023) 4049[[79]](#footnote-80) dotyczącym wdrożenia Toolbox 5G Komisja Europejska wskazała, że wdrożenie Toolbox 5G mieści się w ramach wdrożenia art. 40 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Zgodnie ze wspomnianym przepisem art. 40 EKŁE państwa członkowskie zapewniają, aby dostawcy udostępniający publiczne sieci łączności elektronicznej lub świadczące publicznie dostępne usługi łączności elektronicznej podejmowali właściwe i proporcjonalne środki techniczne i organizacyjne, które to środki mają zapewniać poziom bezpieczeństwa proporcjonalny do istniejącego ryzyka. Wycofanie sprzętu lub oprogramowania od dostawcy wysokiego ryzyka jest środkiem mitygującym ryzyko związane z wykorzystywaniem tego sprzętu lub oprogramowania przez przedsiębiorców telekomunikacyjnych. W konsekwencji należy uznać, że proponowane art. 66a i art. 66b wdrażają zarówno Toolbox 5G jak i art. 40 dyrektywy 2018/1972. Dzięki temu korzystają ze zwolnienia, o którym mowa w art. 1 ust. 3 dyrektywy 2015/1535.

Z kolei przepisy rozdziału 11a, tworzące krajowy system certyfikacji cyberbezpieczeństwa, służą wykonaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[[80]](#footnote-81). Przepisy te korzystają ze zwolnienia z obowiązku notyfikacji, o którym mowa w art. 7 ust. 1 lit. a dyrektywy 2015/1535.

1. ) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L z 19.07.2016 , str. 1). [↑](#footnote-ref-2)
2. ) https://www.knf.gov.pl/dla\_rynku/CSIRT\_KNF. [↑](#footnote-ref-3)
3. ) Najwyższa Izba Kontroli, *Informacja o wynikach kontroli, Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, Warszawa 2019 r., s. 7. [↑](#footnote-ref-4)
4. ) https://www.ee-isac.eu/. [↑](#footnote-ref-5)
5. ) https://www.fsisac.com/. [↑](#footnote-ref-6)
6. ) Agencja Unii Europejskiej do spraw Cyberbezpieczeństwa, *Information Sharing and Analysis Center (ISACs) – Cooperative models*, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models, str. 7. [↑](#footnote-ref-7)
7. ) Dz. Urz. UE L 151 z 07.06.2019, str. 15. [↑](#footnote-ref-8)
8. ) Motyw 29 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), (Dz. Urz. UE L 151 z 07.06.2019, str. 15). [↑](#footnote-ref-9)
9. ) *Cybersecurity of 5G networks. EU Toolbox of risk mitigating measures,* https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. [↑](#footnote-ref-10)
10. ) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej (wersja przekształcona), Dz. Urz. UE. L 2018 Nr 321, str. 36 [↑](#footnote-ref-11)
11. ) *Synergies in Cybersecurity Incident Reporting*, NIS Cooperation Group Publication 04/20 https://ec.europa.eu/newsroom/dae/document.cfm?doc\_id=72147 [↑](#footnote-ref-12)
12. ) Dz. U. 2021 r. poz. 1933 z późn. zm. [↑](#footnote-ref-13)
13. ) Dz. Urz. UE L 218 z 13.08.2008, str. 30 oraz Dz. Urz. UE L 169 z 25.06.2019, str. 1.. [↑](#footnote-ref-14)
14. ) Ustawa z dnia 9 listopada 2018 r. o zmianie niektórych ustaw w związku ze wzmocnieniem nadzoru nad rynkiem finansowym oraz ochrony inwestorów na tym rynku (Dz. U. poz. 2243 oraz z 2019 r. poz. 875 i 2217). [↑](#footnote-ref-15)
15. ) G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), Ustawa o krajowym systemie cyberbezpieczeństwa: komentarz, Warszawa 2019., str. 113. [↑](#footnote-ref-16)
16. ) Dz. U. 2022 r. poz. 671. [↑](#footnote-ref-17)
17. ) Art. 12d ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych (Dz. U. 2022 r. poz. 671). [↑](#footnote-ref-18)
18. ) Dz. U. z 2019 r. poz. 2479. [↑](#footnote-ref-19)
19. ) https://datatracker.ietf.org/doc/html/rfc2350 .   
    Jako przykłady praktyki można wskazać:

    https://www.knf.gov.pl/knf/pl/komponenty/img/RFC2350.pdf

    https://www.csirt.gov.sk/csirt-sk-description-document-according-to-rfc-2350.html

    https://www.ncsc.gov.ie/pdfs/RFC2350%20NCSC-IE.txt. [↑](#footnote-ref-20)
20. ) Dz. U. z 2019 r. poz. 2479. [↑](#footnote-ref-21)
21. ) Środki wskazano za: E. Vytogianni, M. Dekker, *Security Supervision under the EECC*, str. 15–16 European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/publications/supporting-the-implementation-of-the-european-electronic-commmunications-code-eecc. Należy podkreślić, że nie jest to wyczerpująca lista, lecz jedynie przykładowe wskazanie. [↑](#footnote-ref-22)
22. ) Celowo w tym przepisie użyto funktora „lub”, ponieważ zależnie od konkretnej sytuacji u przedsiębiorcy komunikacji elektronicznej może zaistnieć potrzeba nakazania uzupełnienia tylko środka technicznego, tylko środka organizacyjnego albo i jednego i drugiego. [↑](#footnote-ref-23)
23. ) Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, str. 43 https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures [↑](#footnote-ref-24)
24. ) Jako szczególne zagrożenie należy uznać takie, które nie jest typowym lub generalnie występującym zagrożeniem. Jako znaczne zagrożenie należy uznać takie, które stwarza ryzyka dla użytkownika. Por. European Union Agency for Cybersecurity, *Cyber threats outreach in telecom: guidelines for national authorities and telecom providers on outreach to users about cyber threats.*, 2022, s. 21. https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom. [↑](#footnote-ref-25)
25. ) https://www.enisa.europa.eu/publications/cyber-threats-outreach-in-telecom. [↑](#footnote-ref-26)
26. ) Dane o osobie reprezentującej ISAC wpisanego do wykazu są niezbędne dla ministra właściwego do spraw informatyzacji celem skontaktowania się np. przy okazji kontroli ISAC. [↑](#footnote-ref-27)
27. ) Przewiduje się obowiązkową elektronizację tych wniosków. [↑](#footnote-ref-28)
28. Chodzi o umożliwienie takich działań jak np. ARTEMIS - https://www.nask.pl/pl/aktualnosci/5137,Artemis-CERT-Polska-bada-bezpieczenstwo-polskiego-internetu.html. [↑](#footnote-ref-29)
29. ) Dz. U. 2022 r. poz. 2512. [↑](#footnote-ref-30)
30. ) Dz. U. 2023 r. poz. 1136.

    Syntetyczne podsumowanie ocen bezpieczeństwa wykonywanych przez Agencję Bezpieczeństwa Wewnętrznego znajduje się w *Raporcie o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* str. 43–52 https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/977,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2021-roku.html. [↑](#footnote-ref-31)
31. ) Przestępstwo polegające na sprowadzeniu niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach w ramach którego sprawca zakłóca, uniemożliwia lub w inny sposób wpływaj na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. [↑](#footnote-ref-32)
32. ) Przestępstwo w którym sprawca w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. [↑](#footnote-ref-33)
33. ) Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. [↑](#footnote-ref-34)
34. ) Przestępstwo w którym sprawca niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych. [↑](#footnote-ref-35)
35. ) Przestępstwo, w którym sprawca nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej. [↑](#footnote-ref-36)
36. ) Art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. 2022 r. poz. 2512). [↑](#footnote-ref-37)
37. ) Dz. U. 2021 r. poz. 1641 oraz z 2022 r. poz. 1700. [↑](#footnote-ref-38)
38. ) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego. [↑](#footnote-ref-39)
39. ) Por. Martijn van der Heide, *Establishing a CSIRT*, str. 25. https://www.first.org/resources/guides/Establishing-CSIRT-v1.2.pdf [↑](#footnote-ref-40)
40. ) *Ibidem.* [↑](#footnote-ref-41)
41. ) Sprawozdanie z działalności Urzędu Komisji Nadzoru Finansowego oraz Komisji Nadzoru Finansowego w 2021 roku, str. 151–154, https://www.knf.gov.pl/knf/pl/komponenty/img/Sprawozdanie\_z\_dzialalnosci\_UKNF\_oraz\_KNF\_w\_2021\_roku\_78361.pdf. [↑](#footnote-ref-42)
42. ) Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/35639/table. [↑](#footnote-ref-43)
43. ) Źródło https://dane.gov.pl/pl/dataset/1992,statystyki-zespolu-cert-polska/resource/43252/table. [↑](#footnote-ref-44)
44. ) Należy przy tym podkreślić, że chodzi tutaj o jednostki organizacyjne, o których mowa w art. 33 ust. 1d ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz. U. z 2022 r. poz. 1188). [↑](#footnote-ref-45)
45. ) Zgodnie z rozporządzeniem Ministra Finansów z dnia 15 stycznia 2014 r. w sprawie szczegółowego sposobu wykonywania budżetu państwa (Dz. U. z 2021 r. poz. 259 z późn. zm.) [↑](#footnote-ref-46)
46. ) Dz. U. 2022 r. poz. 2305 oraz z 2023 r. poz. 347 i 641. [↑](#footnote-ref-47)
47. ) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. poz. 483, z 2001 r. poz. 319, z 2006 r. poz. 1471 oraz z 2009 r. poz. 946). [↑](#footnote-ref-48)
48. ) Wyrok Trybunału Konstytucyjnego z dnia 8 kwietnia 1998 r., sygn. K 10/97. [↑](#footnote-ref-49)
49. ) Ibidem. [↑](#footnote-ref-50)
50. ) Wyrok Trybunału Konstytucyjnego z dnia 10 października 2001 r., sygn. K 28/01. [↑](#footnote-ref-51)
51. ) Jako sieci 5G Komisja Europejska zdefiniowała: *zbiór wszystkich istotnych elementów infrastruktury sieciowej z zakresu technologii łączności ruchomej i bezprzewodowej, wykorzystywanej na potrzeby łączności i usług o wartości dodanej, o zaawansowanych parametrach eksploatacyjnych, takich jak bardzo wysoka prędkość przesyłu danych i przepustowość łączy, łączność charakteryzująca się niskim opóźnieniem, ekstremalnie wysoka niezawodność bądź zdolność obsługi dużej liczby podłączonych urządzeń. Mogą one obejmować elementy dotychczasowych sieci wykorzystujących technologię łączności ruchomej i bezprzewodowej poprzednich generacji, takich jak 4G lub 3G. Sieci 5G należy rozumieć jako obejmujące wszystkie istotne części sieci*. Pkt II.2.a Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz. Urz. UE L 88 z 29.3.2019, s. 42.) [↑](#footnote-ref-52)
52. ) Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks https://ec.europa.eu/commission/presscorner/detail/en/IP\_19\_6049 , zwana dalej Unijną oceną cyberbezpieczeństwa sieci 5G”. [↑](#footnote-ref-53)
53. ) Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures. [↑](#footnote-ref-54)
54. ) Unijna ocena cyberbezpieczeństwa sieci 5G str. 22, przypis 14 i 15, str. 27; Toolbox str. 43 i 44. [↑](#footnote-ref-55)
55. ) Unijna ocena cyberbezpieczeństwa sieci 5G pkt 2.51, Toolbox 5G str. 43. [↑](#footnote-ref-56)
56. ) https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2020:0050:FIN&\_sm\_au\_=iVVZRW54FHZ10n2PVkFHNKt0jRsMJ [↑](#footnote-ref-57)
57. ) Dla przypomnienia: produktem ICT jest element lub grupę elementów systemu informacyjnego, usługą ICT jest usługa polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych, procesem ICT jest zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT.

    Zauważyć przy tym należy, że definicja systemu informacyjnego obejmuje także sieć telekomunikacyjną - por. Sejm RP VIII kadencji, druk nr 2505, Rządowy projekt ustawy o krajowym systemie cyberbezpieczeństwa, uzasadnienie str. 18-19. https://sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2505. [↑](#footnote-ref-58)
58. ) *Report on the EU coordinated risk assessment on cybersecurity in Fifth Generation (5G) networks* https://ec.europa.eu/commission/presscorner/detail/en/IP\_19\_6049. [↑](#footnote-ref-59)
59. ) Np. cyberterroryzm w postaci ataków na infrastrukturę krytyczną państwa. [↑](#footnote-ref-60)
60. ) Wyrok Trybunału Konstytucyjnego z dnia 23 maja 2018 r. sygn. akt SK 8/14. [↑](#footnote-ref-61)
61. ) https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/ [↑](#footnote-ref-62)
62. ) H. Kisilowska, G. Zieliński, *Administracyjne kary pieniężne – funkcja prewencyjna i represyjna*, Prawo w działaniu, Sprawy Karne, 43/2020, s. 160. [↑](#footnote-ref-63)
63. ) M. Czyżak, *Fakultatywna odpowiedzialność karnoadministracyjna w świetle nowelizacji prawa telekomunikacyjnego z 10 maja 2018 r,* internetowy Kwartalnik Antymonopolowy i Regulacyjny, nr 3(8), 2019, s. 69-70. [↑](#footnote-ref-64)
64. ) Ibidem, s. 70. [↑](#footnote-ref-65)
65. ) Decyzja Nr 676/2002/WE Parlamentu Europejskiego i Rady Z dnia 7 marca 2002 r. w sprawie ram regulacyjnych dotyczących polityki spektrum radiowego we Wspólnocie Europejskiej. [↑](#footnote-ref-66)
66. ) *Report A from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 28 November 2014 by the ECC*. [↑](#footnote-ref-67)
67. ) *Report B from CEPT to the European Commission in response to the Mandate. To develop harmonised technical conditions for the 694-790 MHz ('700 MHz') frequency band in the EU for the provision of wireless broadband and other uses in support of EU spectrum policy objectives. Report approved on 01 March 2016 by the ECC*. [↑](#footnote-ref-68)
68. ) Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia jednolitego rynku cyfrowego dla Europy z dnia 6 maja 2015 r. (COM(2015) 192 final). [↑](#footnote-ref-69)
69. ) Decyzja Wykonawcza Komisji (UE) 2016/687 z dnia 28 kwietnia 2016 r. w sprawie harmonizacji zakresu częstotliwości 694–790 MHz na potrzeby systemów naziemnych zapewniających bezprzewodowe szerokopasmowe usługi łączności elektronicznej oraz na potrzeby elastycznego użytkowania na poziomie krajowym w Unii (notyfikowana jako dokument nr C(2016) 2268). [↑](#footnote-ref-70)
70. ) Decyzja Parlamentu Europejskiego i Rady (UE) 2017/899 z dnia 17 maja 2017 r. w sprawie wykorzystywania zakresu częstotliwości 470–790 MHz w Unii. [↑](#footnote-ref-71)
71. Dz. U. z 2023 r. poz. 753 i 825 [↑](#footnote-ref-72)
72. ) Dz. U. z 2018 r. poz. 2080. [↑](#footnote-ref-73)
73. ) Dz. U. z 2018 r. poz. 1952. [↑](#footnote-ref-74)
74. ) Dz. U. z 2017 r. poz. 248. [↑](#footnote-ref-75)
75. ) Uchwała Nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów M.P. z 2022 r. poz. 348. [↑](#footnote-ref-76)
76. ) Dz. U. poz. 2039 oraz z 2004 r. poz. 597. [↑](#footnote-ref-77)
77. Dz. Urz. UE L 321/36 z 17.12.2018, str. 1. [↑](#footnote-ref-78)
78. Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures, Cooperation Group on Network and Information Security, https://digital-strategy.ec.europa.eu/en/library/cybersecurity- 5g-networks-eu-toolbox-risk-mitigating-measures. [↑](#footnote-ref-79)
79. https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5gcybersecurity-

    toolbox. [↑](#footnote-ref-80)
80. Dz. Urz. L 151/15 z 7.6.2019, str. 15. [↑](#footnote-ref-81)