Druk nr 2505 cz. I

Warszawa, 30 kwietnia 2018 r.

SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-10-64-18

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o krajowym systemie cyberbezpieczeństwa z projektami aktów wykonawczych.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Jednocześnie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem

(-) Mateusz Morawiecki

Projekt

U S T A W A

z dnia

o krajowym systemie cyberbezpieczeństwa[1), 2)]

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

2. Ustawy nie stosuje się do:

1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650) w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;
2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);
3) podmiotów wykonujących działalność leczniczą tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Agencji Wywiadu.

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Ministra Obrony Narodowej;

---

1) Niniejsza ustawa w zakresie swojej regulacji wdraża dyrektywę 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 194 z 19.07.2016, str. 1).

2) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 4 września 1997 r. o działach administracji rządowej, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne oraz ustawę z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

2) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
3) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
4) cyberbezpieczeństwo – odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
5) incydent – każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
6) incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;
8) incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;
9) incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15;
10) obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych, ograniczenie skutków incydentu;

11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;
12) ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
13) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
14) system informacyjny – system teleinformatyczny, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
15) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę incydentu;
16) zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowanie wniosków z obsługi incydentu;
17) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Art. 3. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Art. 4. Krajowy system cyberbezpieczeństwa obejmuje:
1) operatorów usług kluczowych;
2) dostawców usług cyfrowych;
3) CSIRT MON;
4) CSIRT NASK;
5) CSIRT GOV;
6) sektorowe zespoły cyberbezpieczeństwa;
7) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 9 oraz 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62);
8) instytuty badawcze;
9) Narodowy Bank Polski;

10) Bank Gospodarstwa Krajowego;
11) Urząd Dozoru Technicznego;
12) Polską Agencję Żeglugi Powietrznej;
13) Polskie Centrum Akredytacji;
14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;
15) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827);
16) podmioty świadczące usługi z zakresu cyberbezpieczeństwa;
17) organy właściwe do spraw cyberbezpieczeństwa;
18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym”;
19) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, zwanego dalej „Pełnomocnikiem”;
20) Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”.

Rozdział 2

Identyfikacja i rejestracja operatorów usług kluczowych

Art. 5. 1. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy wydał decyzję o uznaniu za operatora usługi kluczowej. Załącznik nr 1 do ustawy określa sektor, podsektor oraz rodzaj podmiotu.

2. Organ właściwy wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli:

1) podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, zwaną dalej „usługą kluczową”, wymienioną w wykazie usług kluczowych;
2) świadczenie tej usługi kluczowej zależy od systemów informacyjnych;
3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora.

3. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 2 pkt 3, określana jest na podstawie progów istotności skutku zakłócającego.

4. W przypadku gdy podmiot świadczy usługę kluczową w innych państwach członkowskich Unii Europejskiej, organ właściwy w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy podmiot został w tych państwach uznany za operatora usługi kluczowej.

5. Okresu na przeprowadzenie konsultacji, o których mowa w ust. 4, nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650).

6. W stosunku do podmiotu, który przestał spełniać warunki, o których mowa w ust. 1 i 2, organ właściwy wydaje decyzję stwierdzającą wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej.

7. Decyzje, o których mowa w ust. 2 i 6, podlegają natychmiastowemu wykonaniu.

Art. 6. Rada Ministrów określi, w drodze rozporządzenia:

1) wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1, kierując się przyporządkowaniem usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu wymienionych w załączniku nr 1 do ustawy oraz znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej;
2) progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie usług kluczowych, uwzględniając:
   a) liczbę użytkowników zależnych od usługi kluczowej świadczonej przez dany podmiot,
   b) zależność innych sektorów, o których mowa w załączniku nr 1 do ustawy, od usługi świadczonej przez ten podmiot,
   c) wpływ, jaki incydent, jeżeli chodzi o skalę i czas trwania, mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne,
   d) udział podmiotu świadczącego usługę kluczową w rynku,
   e) zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent,
   f) zdolność podmiotu dla utrzymywania wystarczającego poziomu świadczenia usługi kluczowej przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia,

g) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują

– kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia i zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi kluczowej.

Art. 7. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz operatorów usług kluczowych.

2. Wykaz operatorów usług kluczowych zawiera:

1) nazwę (firmę) operatora usługi kluczowej;
2) sektor, podsektor i rodzaj podmiotu;
3) siedzibę i adres;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) nazwę usługi kluczowej, zgodną z wykazem usług kluczowych;
7) datę rozpoczęcia świadczenia usługi kluczowej;
8) informację, w których państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej*;*
9) datę zakończenia świadczenia usługi kluczowej;
10) datę wykreślenia z wykazu operatorów usług kluczowych.

3. Wpisanie do wykazu operatorów usług kluczowych i wykreślenie z tego wykazu następuje na wniosek organu właściwego, złożony niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej. Wniosek zawiera informacje, o których mowa w ust. 2 pkt 1–9.

4. Zmiana danych w wykazie operatorów usług kluczowych następuje na wniosek organu właściwego, złożony nie później niż w terminie 6 miesięcy od zmiany tych danych.

5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

6. Wpisanie do wykazu operatorów usług kluczowych i wykreślenie z tego wykazu oraz zmiana danych w wykazie operatorów usług kluczowych jest czynnością materialno-techniczną.

7. Dane z wykazu operatorów usług kluczowych minister właściwy do spraw informatyzacji udostępnia CSIRT MON, CSIRT NASK i CSIRT GOV oraz sektorowemu zespołowi cyberbezpieczeństwa w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym.

8. Dane z wykazu operatorów usług kluczowych, w zakresie niezbędnym do realizacji ich ustawowych zadań, minister właściwy do spraw informatyzacji udostępnia na wniosek następującym podmiotom:

1) organom właściwym;
2) Policji;
3) Żandarmerii Wojskowej;
4) Straży Granicznej;
5) Centralnemu Biuru Antykorupcyjnemu;
6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
8) sądom;
9) prokuraturze;
10) organom Krajowej Administracji Skarbowej;
11) dyrektorowi Rządowego Centrum Bezpieczeństwa.

Rozdział 3

Obowiązki operatorów usług kluczowych

Art. 8. Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie ryzykiem wystąpienia incydentu;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,

d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz poufność, integralność, dostępność i autentyczność informacji,

e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;

4) zarządzanie incydentami;

5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:

a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,

b) dbałość o aktualizację oprogramowania,

c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,

d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;

6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Art. 9. 1. Operator usługi kluczowej:

1) wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

2) zapewnia użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;

3) przekazuje organowi właściwemu informacje, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy od zmiany tych danych.

2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa dane osoby, o której mowa w ust. 1 pkt 1, zawierające imię i nazwisko, numer telefonu, adres poczty elektronicznej, w terminie 14 dni od dnia jej

wyznaczenia, a także informacje o zmianie tych danych, w terminie 14 dni od dnia ich zmiany.

Art. 10. 1. Operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

2. Operator usługi kluczowej jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego:

1) dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami;
2) ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności;
3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w dokumentach.

3. Operator usługi kluczowej przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217, 357, 398 i 650).

4. Operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), który posiada zatwierdzony plan ochrony infrastruktury krytycznej, uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania dokumentacji, o której mowa w ust. 1.

5. Rada Ministrów określi, w drodze rozporządzenia, rodzaje dokumentacji, o której mowa w ust. 1, uwzględniając Polskie Normy oraz potrzebę zapewnienia cyberbezpieczeństwa podczas świadczenia usług kluczowych i ciągłości świadczenia tych usług.

Art. 11. 1. Operator usługi kluczowej:

1) zapewnia obsługę incydentu;

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań;
3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;
4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

3. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej, niezależnie od zadań określonych w ust. 1:

1) przekazuje jednocześnie w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4, temu zespołowi;
2) współdziała na poziomie sektora lub podsektora z tym zespołem podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe;
3) zapewnia temu zespołowi dostęp do informacji o rejestrowanych incydentach, w zakresie niezbędnym do realizacji jego zadań.

4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 do ustawy, określając:

1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej,
2) czas trwania oddziaływania incydentu na świadczoną usługę kluczową,
3) zasięg geograficzny związany z obszarem, którego dotyczy incydent,
4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują

– kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia i zdrowia ludzi, znacznymi stratami majątkowymi oraz obniżeniem jakości świadczonej usługi kluczowej.

Art. 12. 1. Zgłoszenie incydentu poważnego, o którym mowa w art. 11 ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie;
3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu poważnego na usługę kluczową, w tym:
   a) usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ,
   b) liczbę użytkowników usługi kluczowej, na których incydent poważny miał wpływ,
   c) moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania,
   d) zasięg geograficzny, którego dotyczy incydent poważny,
   e) wpływ incydentu poważnego na usługi kluczowe świadczone przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
   f) przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe;
5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;
6) w przypadku incydentu, który mógł mieć wpływ na usługi kluczowe, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;
7) informacje o przyczynie i źródle incydentu poważnego;
8) informacje o podjętych działaniach zapobiegawczych;
9) informacje o podjętych działaniach naprawczych;
10) inne istotne informacje.

2. Operator usługi kluczowej przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego.

3. Operator usługi kluczowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, bądź sektorowego zespołu cyberbezpieczeństwa.

4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV, bądź sektorowy zespół cyberbezpieczeństwa może zwrócić się do operatora usługi kluczowej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

5. W zgłoszeniu operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 13. 1. Operator usługi kluczowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje:

1) o innych incydentach;
2) o zagrożeniach cyberbezpieczeństwa;
3) dotyczące szacowania ryzyka;
4) o podatnościach;
5) o wykorzystywanych technologiach.

2. Informacje, o których mowa w ust. 1, są przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

3. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa, operator usługi kluczowej może przekazywać jednocześnie w postaci elektronicznej informacje, o których mowa w ust. 1, temu zespołowi.

4. Operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 14. 1. Operator usługi kluczowej, w celu realizacji zadań, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 oraz w art. 13, powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.

2. 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.

3. Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowy zespół cyberbezpieczeństwa o podmiocie, z którym została zawarta umowa na świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz o rozwiązaniu umowy, w terminie 14 dni od zawarcia lub rozwiązania umowy.

4. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, uwzględniając Polskie Normy oraz konieczność zapewnienia bezpieczeństwa dla wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo i podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych, a także konieczność zapewnienia bezpieczeństwa informacji przetwarzanych w tych strukturach albo podmiotach.

Art. 15. 1. Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie co najmniej raz na dwa lata audytu bezpieczeństwa systemu informacyjnego, wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej „audytem”.

2. Audyt, o którym nowa w ust. 1, może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650) w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2) co najmniej dwóch audytorów posiadających:
   a) certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub
   b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
   c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była

uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

3) sektorowy zespół cyberbezpieczeństwa, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2.

3. Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa w ust. 2 pkt 2 lit. b i c, uważa się udokumentowane wykonanie 3 audytów w ciągu ostatnich 3 lat w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania, w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z:

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
3) przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;
4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092);
5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524).

4. Audytor jest obowiązany do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych.

5. Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu.

6. Operator usługi kluczowej, u którego w danym roku, w stosunku do systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2 audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, nie ma obowiązku przeprowadzania przez 2 lata audytu, o którym mowa w ust. 1.

7. Operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek:

1) organu właściwego do spraw cyberbezpieczeństwa;
2) dyrektora Rządowego Centrum Bezpieczeństwa, w przypadku gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

8. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, wykaz certyfikatów uprawniających do przeprowadzenia audytu, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób legitymujących się poszczególnymi certyfikatami.

Art. 16. Operator usługi kluczowej realizuje obowiązki określone w:

1) art. 8 pkt 1 i 4, art. 9, art. 11 ust. 1–3, art. 12 i art. 14 ust. 1 – w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;
2) art. 8 pkt 2 i 3 oraz pkt 5 i 6 i art. 10 ust. 1–3 – w terminie sześciu miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;
3) art. 15 ust. 1 – w terminie roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej.

Rozdział 4

Obowiązki dostawców usług cyfrowych

Art. 17. 1. Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy, z wyjątkiem przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646). Załącznik nr 2 do ustawy określa rodzaje usług cyfrowych.

2. Dostawca usługi cyfrowej podejmuje odpowiednie 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 cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają:

1) bezpieczeństwo systemów informacyjnych i obiektów;
2) postępowanie w przypadku obsługi incydentu;
3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej;
4) monitorowanie, audyt i testowanie;
5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151.

3. Dostawca usługi cyfrowej podejmuje środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi.

4. Dostawca usługi cyfrowej, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje usługi cyfrowe w Rzeczypospolitej Polskiej, wyznacza przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej.

5. Przedstawicielem może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona w Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu dostawcy usługi cyfrowej, który nie posiada jednostki organizacyjnej w Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK lub CSIRT GOV może się zwrócić w związku z obowiązkami dostawcy usługi cyfrowej wynikającymi z ustawy.

Art. 18. 1. Dostawca usługi cyfrowej:

1) przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów;
2) zapewnia w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV o incydentach zakwalifikowanych jako krytyczne przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) klasyfikuje incydent jako istotny;
4) zgłasza incydent istotny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;

5) zapewnia obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
6) usuwa podatności, o których mowa w art. 32 ust. 2;
7) przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora.

2. Dostawca usługi cyfrowej, w celu sklasyfikowania incydentu jako istotnego, uwzględnia w szczególności:

1) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług;
2) czas trwania incydentu;
3) zasięg geograficzny, którego dotyczy incydent;
4) zasięg zakłócenia funkcjonowania usługi;
5) zasięg wpływu incydentu na działalność gospodarczą i społeczną.

3. Dostawca usługi cyfrowej, klasyfikując incydent jako istotny, ocenia istotność wpływu incydentu na świadczenie usługi cyfrowej, na podstawie parametrów, o których mowa w ust. 2, oraz progów określonych w rozporządzeniu wykonawczym 2018/151.

4. Dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, o którym mowa w ust. 1 pkt 4, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej.

5. Zgłoszenie, o którym mowa w ust. 1 pkt 4, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 19. 1. Zgłoszenie incydentu istotnego, o którym mowa w art. 18 ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie;
3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu istotnego na świadczenie usługi cyfrowej, w tym:
   a) liczbę użytkowników, na których incydent miał wpływ,
   b) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania,
   c) zasięg geograficzny, którego dotyczy incydent istotny,
   d) zakres zakłócenia funkcjonowania usługi cyfrowej,
   e) zakres wpływu incydentu na działalność gospodarczą i społeczną;
5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;
6) informacje o przyczynie i źródle incydentu istotnego;
7) informacje o podjętych działaniach zapobiegawczych;
8) informacje o podjętych działaniach naprawczych;
9) inne istotne informacje.

2. Dostawca usługi cyfrowej przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu istotnego.

3. Dostawca usługi cyfrowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do dostawcy usługi cyfrowej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

5. W zgłoszeniu dostawcy usług cyfrowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 20. Dostawca usługi cyfrowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje, o których mowa w art. 13 ust. 1. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Rozdział 5

Obowiązki podmiotów publicznych

Art. 21. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

2. Organ administracji publicznej może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane.

3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne.

Art. 22. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego:

1) zapewnia zarządzanie incydentem w podmiocie publicznym;
2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) zapewnia obsługę incydentu w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;
4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej;
5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, zawierające imię i nazwisko, numer telefonu, adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 23. 1. Zgłoszenie incydentu w podmiocie publicznym, o którym mowa w art. 22 ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres;
2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie;
3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym:
   a) wskazanie zadania publicznego, na które incydent miał wpływ,
   b) liczbę osób, na które incydent miał wpływ,
   c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
   d) zasięg geograficzny, którego dotyczy incydent,
   e) przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne podmiotu publicznego;
5) informacje o przyczynie i źródle incydentu;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych działaniach naprawczych;
8) inne istotne informacje.

2. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu w podmiocie publicznym.

3. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, o uzupełnienie zgłoszenia

o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

5. W zgłoszeniu podmiot publiczny, o którym mowa w art. 4 pkt 7–15, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 24. Podmiot publiczny, o którym mowa w art. 4 pkt 7–15, realizujący zadanie publiczne zależne od systemu informacyjnego może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje, o których mowa w art. 13 ust. 1. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji.

Art. 25. Do podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 3 w zakresie świadczenia usługi kluczowej, w związku ze świadczeniem której został uznany za operatora usługi kluczowej.

Rozdział 6

Zadania CSIRT MON, CSIRT NASK i CSIRT GOV

Art. 26. 1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów.

2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7–15, sektorowych zespołów cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.

3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV, zgodnie z właściwością wskazaną w ust. 5–7, należy:

1) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;

2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
3) przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
4) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
5) reagowanie na zgłoszone incydenty;
6) klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
7) zmiana klasyfikacji incydentów poważnych i incydentów istotnych;
8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;
9) przeprowadzanie, w uzasadnionych przypadkach, badania lub oceny bezpieczeństwa stosowania sprzętu lub oprogramowania oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania sprzętu lub oprogramowania, w szczególności w zakresie wpływu stosowania sprzętu lub oprogramowania na bezpieczeństwo publiczne lub istotne interesy bezpieczeństwa państwa, zwanych dalej „rekomendacjami dotyczącymi sprzętu lub oprogramowania”;
10) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;
11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw, informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;
12) przekazywanie, w terminie do dnia 30 maja każdego roku, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość

świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;

13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącego cyberbezpieczeństwa;

14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:
   a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności,
   b) monitoruje wskaźniki zagrożeń cyberbezpieczeństwa,
   c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa,
   d) prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa,
   e) wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,
   f) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,
   g) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

15) zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1 oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń;

16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA).

4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga

współpracy CSIRT, oraz określą, we współpracy z sektorowymi zespołami cyberbezpieczeństwa, sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu.

5. Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez:

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, 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;
2) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571) jest Minister Obrony Narodowej.

6. Do zadań CSIRT NASK należy:

1) koordynacja obsługi incydentów zgłaszanych przez:
   a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2,
   c) instytuty badawcze,
   d) Urząd Dozoru Technicznego,
   e) Polską Agencję Żeglugi Powietrznej,
   f) Polskie Centrum Akredytacji,
   g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,
   h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,
   i) dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 5,
   j) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i 7,
   k) inne podmioty niż wymienione w lit. a–j oraz ust. 5 i 7,

l) osoby fizyczne;

2) tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;

3) zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzącego działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. UE L 335 z 13.12.2011, str. 1).

7. Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6;

2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;

3) Narodowy Bank Polski;

4) Bank Gospodarstwa Krajowego;

5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, 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;

6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

8. CSIRT MON, CSIRT NASK lub CSIRT GOV, który otrzymał zgłoszenie incydentu, a nie jest właściwy do koordynacji jego obsługi, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

9. Działalność CSIRT NASK jest finansowana w formie dotacji podmiotowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.

10. CSIRT MON, CSIRT NASK i CSIRT GOV mogą, w drodze porozumienia, powierzyć sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów, o których mowa w ust. 5–7. O zawarciu porozumienia CSIRT, który powierzył wykonywanie zadań, informuje podmioty, w stosunku do których nastąpiła zmiana CSIRT.

11. Komunikat o zawarciu porozumienia, o którym mowa w ust. 10, ogłasza się odpowiednio w dzienniku urzędowym Ministra Obrony Narodowej, Ministra Cyfryzacji, Agencji Bezpieczeństwa Wewnętrznego. W komunikacie wskazuje się informacje o:

1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;
2) terminie, od którego porozumienie będzie obowiązywało.

Art. 27. 1. CSIRT GOV jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730).

2. CSIRT MON jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 5 ust. 1 pkt 2a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978 i 2405 oraz z 2018 r. poz. 650).

3. W przypadku stwierdzenia, że incydent, którego obsługa jest koordynowana przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV, jest związany ze zdarzeniami, o których mowa w ust. 1 i 2, koordynację obsługi incydentu przejmuje właściwy CSIRT MON lub CSIRT GOV.

Art. 28. 1. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV informuje, na podstawie zgłoszenia incydentu poważnego dokonanego przez operatora usługi kluczowej, inne państwa członkowskie Unii Europejskiej, których dotyczy ten incydent, za pośrednictwem Pojedynczego Punktu Kontaktowego.

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje, jeżeli pozwalają na to okoliczności, operatorowi usługi kluczowej zgłaszającemu incydent poważny, informacje dotyczące działań podjętych po zgłoszeniu tego incydentu, które mogłyby pomóc w jego obsłudze.

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić z wnioskiem do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego,

o którym mowa w ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich Unii Europejskiej, których dotyczy ten incydent.

Art. 29. CSIRT MON, CSIRT NASK lub CSIRT GOV informuje inne państwa członkowskie Unii Europejskiej w przypadku, gdy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej, za pośrednictwem Pojedynczego Punktu Kontaktowego.

Art. 30. 1. Podmioty inne, niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK. W zgłoszeniu należy podać:

1) nazwę podmiotu lub systemu informacyjnego, w którym wystąpił incydent;
2) opis incydentu;
3) inne istotne informacje.

2. Zgłoszenia incydentów od operatorów usług kluczowych oraz dostawców usług cyfrowych są traktowane priorytetowo względem zgłoszeń, o których mowa w ust. 1.

3. Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK.

4. Podmiot, o którym mowa w ust. 1, oznacza w zgłoszeniu informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 31. 1. CSIRT MON, CSIRT NASK i CSIRT GOV określa sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, a także określa sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji, w przypadku braku możliwości zgłoszenia albo przekazania ich w postaci elektronicznej.

2. Komunikat, zawierający informacje, o których mowa w ust. 1, CSIRT MON, CSIRT NASK i CSIRT GOV publikuje na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego.

Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego.

2. W trakcie koordynacji obsługi incydentu poważnego, incydentu istotnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, istotnego lub krytycznego.

3. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do operatora usługi kluczowej o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowe zespoły cyberbezpieczeństwa na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od operatora usługi kluczowej, dostawcy usługi cyfrowej lub podmiotu publicznego, o którym mowa w art. 4 pkt 7–15, może przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.

Art. 33. 1. CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie lub ocenę bezpieczeństwa stosowania sprzętu lub oprogramowania, na podstawie którego składa wniosek do Pełnomocnika w sprawie wydania, zmiany lub odwołania rekomendacji dotyczących sprzętu lub oprogramowania.

2. Pełnomocnik, po uzyskaniu opinii Kolegium, decyduje o wydaniu, zmianie lub odwołaniu rekomendacji dotyczących sprzętu lub oprogramowania.

3. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do zakresu stosowania rekomendacji dotyczących sprzętu lub oprogramowania z uwagi na ich negatywny wpływ na świadczone usługi lub realizowane zadanie publiczne, niezwłocznie, jednak nie później niż w terminie 7 dni od dnia ich otrzymania.

4. Pełnomocnik odnosi się do zastrzeżeń otrzymanych w trybie ust. 3 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania.

5. Podmioty krajowego systemu cyberbezpieczeństwa informują Pełnomocnika, na jego wniosek, o sposobie i zakresie stosowania rekomendacji dotyczących sprzętu lub oprogramowania lub ich niestosowaniu.

6. Pełnomocnik może przekazać do organu sprawującego nadzór nad podmiotem krajowego systemu cyberbezpieczeństwa informację o sposobie i zakresie stosowania

rekomendacji dotyczących sprzętu lub oprogramowania albo ich niestosowaniu przez ten podmiot.

Art. 34. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.

2. CSIRT MON, CSIRT NASK i CSIRT GOV, koordynując obsługę incydentu, który doprowadził do naruszenia danych osobowych, współpracują z organem właściwym do spraw ochrony danych osobowych.

Art. 35. 1. CSIRT MON, CSIRT NASK i CSIRT GOV informują się wzajemnie oraz informują Rządowe Centrum Bezpieczeństwa o incydencie krytycznym.

2. Informacja, o której mowa w ust. 1, zawiera:

1) wstępną analizę potencjalnych skutków incydentu z uwzględnieniem w szczególności:
   a) liczby użytkowników, których dotyczy incydent, w szczególności jeśli zakłóca świadczenie usługi kluczowej,
   b) momentu wystąpienia i wykrycia incydentu oraz czasu jego trwania,
   c) zasięgu geograficznego, którego dotyczy incydent;
2) rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

3. Informacja, o której mowa w ust. 1, może zawierać wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 36 ust. 1.

4. W przypadku uzyskania informacji o zagrożeniach cyberbezpieczeństwa CSIRT MON, CSIRT NASK i CSIRT GOV mogą informować się wzajemnie oraz informować Rządowe Centrum Bezpieczeństwa. Przepisy ust. 2 i 3 stosuje się odpowiednio.

5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą publikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje, w niezbędnym zakresie, o podatnościach i incydentach, o których mowa w ust. 1, oraz o zagrożeniach cyberbezpieczeństwa, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia

bezpiecznego korzystania z tych systemów. Publikowane informacje nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.

Art. 36. 1. Tworzy się Zespół do spraw Incydentów Krytycznych, zwany dalej „Zespołem”, jako organ pomocniczy w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynujący działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa.

2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizujący zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa.

3. Dyrektor Rządowego Centrum Bezpieczeństwa przewodniczy pracom Zespołu.

4. Obsługę prac Zespołu zapewnia Rządowe Centrum Bezpieczeństwa.

5. Do udziału w pracach Zespołu, z głosem doradczym, członkowie Zespołu mogą zapraszać przedstawicieli organów właściwych lub jednostek im podległych lub przez nie nadzorowanych, organów ścigania, wymiaru sprawiedliwości lub służb specjalnych.

6. W przypadku, o którym mowa w art. 35 ust. 3, albo na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 2, dyrektor Rządowego Centrum Bezpieczeństwa zawiadamia niezwłocznie członków Zespołu o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej.

7. Zespół na posiedzeniu:

1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 2;
2) określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 2;
3) określa sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV;
4) podejmuje decyzję o wystąpieniu przez dyrektora Rządowego Centrum Bezpieczeństwa z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego;

5) w przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego.

Rozdział 7

Zasady udostępniania informacji i przetwarzania danych osobowych

Art. 37. 1. Do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 933).

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym operatorem usługi kluczowej, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej lub Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach istotnych lub wystąpić do organu właściwego dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.

4. Opublikowanie informacji, o której mowa w ust. 2 i 3, nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.

Art. 38. Nie udostępnia się informacji przetwarzanych na podstawie ustawy, jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania.

Art. 39. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i w celu niezbędnym do realizacji tych zadań.

2. CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa, przetwarzając dane osobowe określone w art. 9 ust. 1 rozporządzenia 2016/679, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowują procedury bezpiecznej wymiany informacji.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:

1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych;
2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
3) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług;
4) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

4. W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik oraz organy właściwe do spraw cyberbezpieczeństwa przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa:

1) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług;
2) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych;
3) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne dla realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3.

6. Dane, o których mowa w ust. 3 i 4, niezbędne dla realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa w terminie 5 lat od zakończenia obsługi incydentu, którego dotyczą.

7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa mogą wzajemnie przekazywać dane osobowe, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych.

8. Przetwarzanie przez CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa danych osobowych, o których mowa w ust. 3, nie wymaga realizacji obowiązków, o których mowa w art. 15, art. 16 i art. 18 ust. 1 lit. a i d i art. 19 zdanie drugie rozporządzenia 2016/679, jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK, CSIRT MON i sektorowych zespołów cyberbezpieczeństwa, o których mowa w art. 26 ust. 3 pkt 1–11 oraz 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3, i jest możliwe, gdy CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji.

9. CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa publikują na swojej stronie internetowej:

1) dane kontaktowe administratora danych oraz gdy ma to zastosowanie, dane kontaktowe inspektora ochrony danych;

2) cele przetwarzania i podstawę prawną przetwarzania;
3) kategorie przetwarzanych danych osobowych;
4) informacje o odbiorcach danych osobowych;
5) okres, przez który dane osobowe będą przechowywane;
6) informacje o ograniczeniach obowiązków i praw osób, których dane dotyczą;
7) informacje o prawie wniesienia skargi do organu właściwego do spraw ochrony danych osobowych;
8) źródło pochodzenia danych osobowych.

Art. 40. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i minister właściwy do spraw informatyzacji przetwarzają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, o których mowa w ustawie.

2. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przekazują dane, o których mowa w ust. 1, organom ścigania w związku z incydentem wyczerpującym znamiona przestępstwa.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa zobowiązane są do zachowania w tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań, o których mowa w ustawie.

Rozdział 8

Organy właściwe do spraw cyberbezpieczeństwa

Art. 41. Organami właściwymi do spraw cyberbezpieczeństwa są:
1) dla sektora energii – minister właściwy do spraw energii;
2) dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu;
3) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej;
4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
5) dla sektora ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw zdrowia;

6) dla sektora ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej;
8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji;
9) dla sektora infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej;
10) dla dostawców usług cyfrowych z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – minister właściwy do spraw informatyzacji;
11) dla dostawców usług cyfrowych obejmujących podmioty, o których mowa w art. 26 ust. 5 – Minister Obrony Narodowej.

Art. 42. 1. Organ właściwy do spraw cyberbezpieczeństwa:

1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
2) wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
3) niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu;
4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;
5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON oraz sektorowymi zespołami cyberbezpieczeństwa rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
6) monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych;
7) wzywa na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie

podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;

8) prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych;

9) może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;

10) przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;

11) uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej.

2. W przypadku gdy osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, świadcząca usługi cyfrowe, nie posiada siedziby lub zarządu na terytorium Rzeczypospolitej Polskiej albo nie wyznaczyła przedstawiciela na terytorium Rzeczypospolitej Polskiej, ale jej systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej, i nie spełnia wymagań określonych w rozporządzeniu wykonawczym 2018/151, organ właściwy dla dostawców usług cyfrowych może przekazywać informacje oraz zwracać się o podejmowanie działań, o których mowa w art. 53 ust. 2, do organu właściwego w innym państwie członkowskim Unii Europejskiej, na terytorium którego posiada ona siedzibę lub zarząd albo został wyznaczony jej przedstawiciel.

3. Organ właściwy może powierzyć realizację, w jego imieniu, niektórych zadań, o których mowa w ust. 1, jednostkom podległym lub nadzorowanym przez ten organ.

4. Powierzenie następuje na podstawie porozumienia organu właściwego z podmiotami, o których mowa w ust. 3.

5. W porozumieniu, o którym mowa w ust. 4, określa się zasady sprawowania przez organ właściwy kontroli nad prawidłowym wykonywaniem powierzonych zadań.

6. Komunikat o zawarciu porozumienia ogłasza się w dzienniku urzędowym właściwego organu. W komunikacie wskazuje się informacje o:

1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami;

2) terminie, od którego porozumienie będzie obowiązywało.

7. Organy właściwe i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych.

8. Rekomendacje działań mające na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów, o których mowa w ust. 1 pkt 5, przygotowuje się z uwzględnieniem w szczególności Polskich Norm przenoszących normy europejskie, wspólne specyfikacje techniczne, rozumianych jako specyfikacje techniczne w dziedzinie produktów teleinformatycznych określone zgodnie z art. 13 i art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12), wytyczne Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) w tym zakresie.

Art. 43. 1. Organ właściwy może, bez wszczynania postępowania w sprawie uznania podmiotu za operatora usługi kluczowej, wystąpić do podmiotu, o którym mowa w załączniku nr 1 do ustawy, o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot spełnia warunki do uznania go za operatora usługi kluczowej.

2. Organ właściwy może, bez wszczynania kontroli, wystąpić do operatora usługi kluczowej o udzielenie informacji, które pozwolą na ustalenie potrzeby przeprowadzania kontroli, a także może, bez wszczynania postępowania, wystąpić do operatora usługi kluczowej o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot przestał spełniać warunki do uznania go za operatora usługi kluczowej.

3. Organ, występując do podmiotu lub operatora usługi kluczowej, o których mowa w ust. 1 i 2, wskazuje termin udzielenia informacji. Wyznaczony termin nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot lub operatora usługi kluczowej.

4. Podmiot i operator usługi kluczowej, o których mowa odpowiednio w ust. 1 i 2, do którego organ skierował wystąpienie, może przekazać informacje w sprawie, której dotyczy wystąpienie, lub poinformować o odmowie udzielenia informacji.

5. Wystąpienie o udzielenie informacji oraz brak udzielenia informacji przez podmiot lub operatora usługi kluczowej, o których mowa odpowiednio w ust. 1 i 2, nie wpływa na możliwości wszczęcia postępowania administracyjnego lub kontroli.

6. Informacje udzielone przez podmiot lub operatora usługi kluczowej, o których mowa w ust. 1 i 2, mogą stanowić materiał dowodowy we wszczętym postępowaniu administracyjnym lub kontroli. Brak udzielenia informacji nie wpływa na sytuację procesową strony albo kontrolowanego oraz na wszczęte postępowanie administracyjne lub kontrolę.

Art. 44. 1. Organ właściwy do spraw cyberbezpieczeństwa może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, odpowiedzialny w szczególności za:

1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów;
2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13;
3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowanie wniosków z obsługi incydentu;
4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych.

2. Sektorowy zespół cyberbezpieczeństwa może przekazywać do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmować z tych państw informacje o incydentach poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej.

3. Sektorowy zespół cyberbezpieczeństwa może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego Unii Europejskiej dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. Sektorowy zespół cyberbezpieczeństwa przekazuje te zgłoszenia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz Pojedynczego Punktu Kontaktowego.

4. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa, organ właściwy do spraw cyberbezpieczeństwa informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu tego zespołu i zakresie realizowanych zadań.

Rozdział 9

Zadania ministra właściwego do spraw informatyzacji

Art. 45. 1. Minister właściwy do spraw informatyzacji jest odpowiedzialny za:

1) monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizację planów działań na rzecz jej wdrożenia;
2) rekomendowanie obszarów współpracy z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa Rzeczypospolitej Polskiej;
3) opracowywanie rocznych sprawozdań dotyczących:
   a) incydentów poważnych zgłaszanych przez operatorów usług kluczowych mających wpływ na ciągłość świadczonych przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej,
   b) incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, w tym incydentów dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;
4) prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników;
5) gromadzenie informacji o incydentach poważnych, które dotyczą lub zostały przekazane przez inne państwo członkowskie Unii Europejskiej;
6) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych, uzyskanych z Grupy Współpracy, w tym:
   a) procedur postępowania w zakresie zarządzania incydentem,
   b) procedur postępowania przy zarządzaniu ryzykiem,
   c) klasyfikacji informacji, ryzyka i incydentów.

2. Przez Grupę Współpracy rozumie się grupę, o której mowa w decyzji wykonawczej Komisji UE 2017/179 z dnia 1 lutego 2017 r. ustanawiającej procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego

poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 28 z 02.02.2017, str. 73).

Art. 46. 1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) zgłaszanie i obsługę incydentów;
4) szacowanie ryzyka na poziomie krajowym;
5) ostrzeganie o zagrożeniach cyberbezpieczeństwa.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej, mogą korzystać z systemu teleinformatycznego na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.

3. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego.

Art. 47. 1. Minister właściwy do spraw informatyzacji może realizować zadania, o których mowa w art. 45 i 46 ust. 1, na zasadach określonych w przepisach odrębnych, za pomocą właściwych w tym zakresie jednostek podległych lub nadzorowanych przez ministra właściwego do spraw informatyzacji.

2. Zadania powierzone do realizacji podmiotowi, o którym mowa w ust. 1, są finansowane w formie dotacji celowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.

Art. 48. Minister właściwy do spraw informatyzacji prowadzi Pojedynczy Punkt Kontaktowy, do którego zadań należy:

1) odbieranie zgłoszeń incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowych zespołów cyberbezpieczeństwa;
2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub

większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;

3) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy;
4) zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa;
5) koordynacja współpracy między organami właściwymi i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
6) zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT.

Art. 49. 1. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy:

1) informacje, o których mowa w art. 45 pkt 3;
2) dobre praktyki związane ze zgłaszaniem incydentów, o których mowa w art. 45 pkt 4;
3) propozycje do programu prac Grupy Współpracy;
4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju z zakresu cyberbezpieczeństwa;
5) dobre praktyki w odniesieniu do identyfikowania operatorów usług kluczowych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.

2. Informacje, o których mowa w ust. 1, nie obejmują informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego.

3. Pojedynczy Punkt Kontaktowy przekazuje organom właściwym, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowym zespołom cyberbezpieczeństwa oraz innym organom władzy publicznej informacje pochodzące z Grupy Współpracy dotyczące:

1) ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa oraz skuteczności CSIRT, a także dobrych praktyk w zakresie cyberbezpieczeństwa;
2) działań podjętych w odniesieniu do ćwiczeń dotyczących cyberbezpieczeństwa, europejskich programów edukacyjnych i szkoleń, w tym działań Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA);
3) wytycznych o charakterze strategicznym dotyczących działalności Sieci CSIRT;
4) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych;

5) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących podnoszenia świadomości, szkolenia, zakresu badań i rozwoju w zakresie cyberbezpieczeństwa;
6) dobrych praktyk w zakresie identyfikowania operatorów usług kluczowych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.

Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

1) niezwłocznie informacje:
   a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa;
2) co 2 lata informacje umożliwiające ocenę wdrażania dyrektywy, obejmujące w szczególności:
   a) środki umożliwiające identyfikację operatorów usług kluczowych,
   b) wykaz usług kluczowych,
   c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku nr 1 do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora,
   d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych;
3) informacje o zadaniach CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu.

Rozdział 10

Zadania Ministra Obrony Narodowej

Art. 51. Minister Obrony Narodowej jest odpowiedzialny za:

1) współpracę Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa;
2) zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa, powodującego konieczność działań obronnych;

3) rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;
4) pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP;
5) kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego, o którym mowa w ustawie 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 2017 r. poz. 1932);
6) ocenę wpływu incydentów na system obrony państwa;
7) ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;
8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego, dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa.

Art. 52. Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego, do którego zadań należy:
1) zapewnienie współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa;
2) koordynacja działań w zakresie wzmacniania zdolności obronnych w przypadku zagrożenia cyberbezpieczeństwa;
3) zapewnienie współpracy między narodowymi i sojuszniczymi siłami zbrojnymi w zakresie zapewnienia cyberbezpieczeństwa;
4) rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej;
5) udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.

Rozdział 11

Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa

Art. 53. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują:

1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 15 ust. 2;
2) organy właściwe w zakresie:
   a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych,
   b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych.

2. W ramach nadzoru, o którym mowa w ust. 1:

1) organ właściwy lub minister właściwy do spraw informatyzacji prowadzi kontrole w zakresie, o którym mowa w ust. 1;
2) organ właściwy nakłada kary pieniężne na operatorów usług kluczowych i dostawców usług cyfrowych.

3. W stosunku do dostawcy usług cyfrowych, podjęcie czynności, o których mowa w ust. 2, następuje po uzyskaniu dowodu, że dostawca usług cyfrowych nie spełnia wymogów określonych w rozporządzeniu wykonawczym 2018/151 lub nie wykonuje wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych.

Art. 54. 1. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

2. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 2, realizowanej wobec podmiotów:

1) będących przedsiębiorcami, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców;
2) niebędących przedsiębiorcami, stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, określające zasady i tryb przeprowadzania kontroli.

Art. 55. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki;
2) wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;
3) sporządzania, a w razie potrzeby żądania sporządzenia niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń;
4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
5) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli;
6) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych.

Art. 56. 1. Kontrolowane podmioty będące przedsiębiorcami zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

2. Podmiot kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 1. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je osoba prowadząca czynności kontrolne, o czym czyni wzmiankę w protokole kontroli.

Art. 57. 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.

Art. 58. 1. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli.

2. Protokół kontroli zawiera:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu podmiotu kontrolowanego;

2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko, stanowisko oraz numer upoważnienia osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7) wyszczególnienie załączników.

3. Protokół kontroli podpisują osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany.

4. Przed podpisaniem protokołu podmiot kontrolowany może, w terminie 7 dni od przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu.

5. W razie zgłoszenia zastrzeżeń osoba prowadząca czynności kontrolne dokonuje ich analizy i w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu.

6. W razie nieuwzględnienia zastrzeżeń w całości lub w części osoba prowadząca czynności kontrolne informuje podmiot kontrolowany na piśmie.

7. O odmowie podpisania protokołu osoba prowadząca czynności kontrolne czyni wzmiankę w protokole, zawierającą datę jej dokonania.

8. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go podmiotowi kontrolowanemu.

Art. 59. 1. 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 nieprawidłowości.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń.

Rozdział 12

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa

Art. 60. Koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej powierza się Pełnomocnikowi.

Art. 61. 1. Pełnomocnika powołuje i odwołuje Prezes Rady Ministrów.

2. Pełnomocnik podlega Radzie Ministrów.

3. Pełnomocnikiem jest sekretarz stanu albo podsekretarz stanu.

4. Obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową Pełnomocnika zapewnia ministerstwo lub inny urząd administracji rządowej, w którym powołano Pełnomocnika.

Art. 62. 1. W ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa do zadań Pełnomocnika należy:

1) analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji publicznej, organów właściwych, CSIRT MON, CSIRT NASK i CSIRT GOV;
2) nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych, CSIRT MON, CSIRT NASK i CSIRT GOV;
3) opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;
4) upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;
5) inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa;
6) wydawanie rekomendacji dotyczących sprzętu lub oprogramowania na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV.

2. Do zadań Pełnomocnika wykonywanych w porozumieniu z właściwymi ministrami należy również:

1) współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;

2) podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa;
3) podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu.

Art. 63. 1. Pełnomocnik opracowuje i przedkłada Radzie Ministrów, w terminie do dnia 31 marca każdego roku, sprawozdanie za poprzedni rok kalendarzowy, zawierające informację o prowadzonej działalności w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym.

2. Pełnomocnik może 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. 64. Przy Radzie Ministrów działa Kolegium, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych.

Art. 65. 1. Do zadań Kolegium należy wyrażanie opinii w sprawach:
1) kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa;
2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa oraz organy właściwe powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa;
3) współdziałania organów prowadzących lub nadzorujących CSIRT MON, CSIRT GOV i CSIRT NASK;
4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego oraz ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, sektorowych zespołów cyberbezpieczeństwa i organów właściwych;
5) organizacji wymiany informacji istotnych dla cyberbezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej między organami administracji rządowej;
6) wniosków CSIRT MON, CSIRT NASK lub CSIRT GOV w sprawie rekomendacji dotyczących sprzętu lub oprogramowania.

2. Do zadań Kolegium należy opracowywanie rekomendacji dla Rady Ministrów, dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym, o których mowa w art. 67.

Art. 66. 1. W skład Kolegium wchodzą:

1) przewodniczący Kolegium – Prezes Rady Ministrów;
2) Pełnomocnik;
3) sekretarz Kolegium;
4) członkowie Kolegium:
   a) minister właściwy do spraw wewnętrznych,
   b) minister właściwy do spraw informatyzacji,
   c) Minister Obrony Narodowej,
   d) minister właściwy do spraw zagranicznych,
   e) Szef Kancelarii Prezesa Rady Ministrów,
   f) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,
   g) minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego.

2. Prezes Rady Ministrów może upoważnić Pełnomocnika do pełnienia funkcji przewodniczącego Kolegium.

3. Członkowie Kolegium, o których mowa w ust. 1 pkt 4 lit. a–e, mogą być zastępowani przez upoważnionych przedstawicieli w randze sekretarza stanu albo podsekretarza stanu.

4. W posiedzeniach Kolegium uczestniczą również:

1) Dyrektor Rządowego Centrum Bezpieczeństwa;
2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;
3) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;
4) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

5. Przewodniczący Kolegium:

1) zwołuje posiedzenia Kolegium;

2) może zapraszać do udziału w posiedzeniach Kolegium przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych, przedstawicieli organów właściwych oraz inne osoby, których uczestnictwo jest niezbędne ze względu na tematykę obrad.

6. Sekretarza Kolegium powołuje Prezes Rady Ministrów spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”. Sekretarza Kolegium odwołuje Prezes Rady Ministrów.

7. Sekretarz Kolegium organizuje pracę Kolegium i w tym zakresie może występować do CSIRT MON, CSIRT GOV i CSIRT NASK, sektorowych zespołów cyberbezpieczeństwa, organów właściwych oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium.

8. Obsługę Kolegium zapewnia ministerstwo lub inny urząd administracji rządowej, które obsługuje Pełnomocnika.

9. Rada Ministrów określi, w drodze rozporządzenia, zakres działania oraz tryb pracy Kolegium, mając na uwadze charakter zadań Kolegium oraz konieczność zapewnienia jego sprawnej pracy.

Art. 67. 1. Prezes Rady Ministrów w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa może, na podstawie rekomendacji Kolegium, wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa, a także żądać informacji i opinii w tym zakresie od:

1) ministra właściwego do spraw wewnętrznych – w odniesieniu do działalności Policji i Straży Granicznej;
2) Ministra Obrony Narodowej – w odniesieniu do działalności CSIRT MON;
3) Szefa Agencji Bezpieczeństwa Wewnętrznego – w odniesieniu do działalności CSIRT GOV;
4) Dyrektora Rządowego Centrum Bezpieczeństwa – w odniesieniu do zadań realizowanych zgodnie z ustawą;
5) Dyrektora Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego – w odniesieniu do działalności CSIRT NASK;
6) ministra właściwego do spraw informatyzacji – w odniesieniu do zadań realizowanych zgodnie z ustawą.

2. Prezes Rady Ministrów wydaje wiążące wytyczne dla CSIRT MON, CSIRT GOV i CSIRT NASK w zakresie obsługi incydentów krytycznych, w tym wskazuje CSIRT odpowiedzialny za obsługę incydentu krytycznego.

Rozdział 13

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Art. 68. Rada Ministrów przyjmuje, w drodze uchwały, Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zwaną dalej „Strategią”.

Art. 69. 1. Strategia określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Strategia obejmuje sektory, o których mowa w załączniku nr 1 do ustawy, usługi cyfrowe oraz podmioty publiczne, o których mowa w art. 4 pkt 7–15.

2. Strategia uwzględnia w szczególności:

1) cele i priorytety w zakresie cyberbezpieczeństwa;
2) podmioty zaangażowane we wdrażanie i realizację Strategii;
3) środki służące realizacji celów Strategii;
4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
5) podejście do oceny ryzyka;
6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

3. Strategia ustalana jest na okres pięcioletni z możliwością wprowadzenia zmian w okresie jej obowiązywania.

Art. 70. 1. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, ministrami i właściwymi kierownikami urzędów centralnych.

2. W pracach nad projektem może uczestniczyć przedstawiciel Prezydenta Rzeczypospolitej Polskiej.

Art. 71. Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii co dwa lata.

Art. 72. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej Strategię w terminie trzech miesięcy od dnia jej przyjęcia przez Radę Ministrów.

Rozdział 14

Przepisy o karach pieniężnych

Art. 73. 1. Karze pieniężnej podlega operator usługi kluczowej, który:

1) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o których mowa w art. 8 pkt 1;
2) nie wdrożył środków technicznych i organizacyjnych uwzględniających wymagania, o których mowa w art. 8 pkt 2 lit. a–e;
3) nie stosuje środków, o których mowa w art. 8 pkt 5 lit. a–d;
4) nie wyznaczył osoby, o której mowa w art. 9 ust. 1 pkt 1;
5) nie wykonuje obowiązku, o którym mowa w art. 10 ust. 1;
6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1;
7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4;
8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5;
9) nie wykonuje obowiązku o którym mowa w art. 11 ust. 1 pkt 6;
10) nie wykonuje obowiązku, o którym mowa w art. 14 ust. 1;
11) nie przeprowadza audytu, o którym mowa w art. 15 ust. 1;
12) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 53 ust. 2 pkt 1;
13) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1.

2. Karze pieniężnej podlega dostawca usługi cyfrowej, który:

1) nie wykonuje obowiązku wynikającego z art. 18 ust. 1 pkt 4;
2) nie wykonuje obowiązku wynikającego z art. 18 ust. 1 pkt 5;
3) nie wykonuje obowiązku wynikającego z art. 18 ust. 1 pkt 6;

3. Wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1 wynosi do 150 000 złotych;
2) ust. 1 pkt 2 wynosi do 100 000 złotych;
3) ust. 1 pkt 3 wynosi do 50 000 złotych;
4) ust. 1 pkt 4 wynosi do 15 000 złotych;
5) ust. 1 pkt 5 wynosi do 50 000 złotych;

6) ust. 1 pkt 6 wynosi do 15 000 złotych za każdy stwierdzony przypadek zaniechania obsługi incydentu;
7) ust. 1 pkt 7 wynosi do 20 000 złotych za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego;
8) ust. 1 pkt 8 i 9 wynosi do 20 000 złotych;
9) ust. 1 pkt 10 wynosi 100 000 złotych;
10) ust. 1 pkt 11 i 13 wynosi do 200 000 złotych;
11) ust. 1 pkt 12 wynosi do 50 000 złotych;
12) ust. 2 pkt 1 wynosi do 20 000 złotych za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;
13) ust. 2 pkt 2 i 3 wynosi do 20 000 złotych.

4. Jeżeli w wyniku kontroli organ właściwy stwierdzi, że operator usługi kluczowej bądź dostawca usługi cyfrowej uporczywie narusza przepisy ustawy, powodując:

1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi,
2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych

– organ właściwy nakłada karę w wysokości do 1 000 000 złotych.

Art. 74. 1. Karę pieniężną, o której mowa w art. 73, nakłada, w drodze decyzji, organ właściwy.

2. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73, stanowią dochód budżetu państwa.

3. Kara, o której mowa w:

1) art. 73 ust. 1 pkt 4, nie może być niższa niż 1 000 złotych;
2) art. 73 ust. 1 pkt 1–3, 6–9 i 12, nie może być niższa niż 5 000 złotych;
3) art. 73 ust. 1 pkt 5, 10, 11 i 13, nie może być niższa niż 15 000 złotych.

4. Organ właściwy może nałożyć karę pieniężną na kierownika operatora usługi kluczowej, w przypadku gdy nie dochował należytej staranności celem spełnienia obowiązków, o których mowa w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1, z tym że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia.

5. Kara, o której mowa w art. 73, może zostać nałożona również w przypadku gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

Art. 75. W sprawach nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu stosuje się przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Rozdział 15

Zmiany w przepisach obowiązujących, przepisy przejściowe, dostosowujące i końcowe

Art. 76. W ustawie z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2017 r. poz. 2198, 2203 i 2361) w art. 90u:

1) w ust. 1 pkt 6 otrzymuje brzmienie:

„6) rozwijanie kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, w tym wspomaganie organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych;”;

2) w ust. 4 pkt 6 otrzymuje brzmienie:

„6) szczegółowe warunki, formy i tryb realizacji przedsięwzięć w zakresie rozwijania kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, a także warunki i tryb wspomagania organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych, uwzględniając konieczność rozwijania umiejętności ułatwiających przystosowanie się do zmian zachodzących w życiu społecznym i gospodarczym, możliwość udzielenia wsparcia finansowego organów prowadzących szkoły lub placówki oraz wymóg skuteczności i efektywności wydatkowania środków budżetowych;”.

Art. 77. W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2018 r. poz. 762) wprowadza się następujące zmiany:

1) w art. 12a w ust. 1 pkt 10 otrzymuje brzmienie:

„10) bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym;”;

2) w art. 19 w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) bezpieczeństwo cyberprzestrzeni w wymiarze militarnym,”.

Art. 78. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650) wprowadza się następujące zmiany:

1) w art. 175a:

a) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu:

„1a. Prezes UKE przekazuje informacje, o których mowa w ust. 1, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia …. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego, zgodnie z art. 26 ust. 5–7 tej ustawy, z wyłączeniem informacji stanowiących tajemnicę przedsiębiorstwa, zastrzeżonych na podstawie art. 9.

1b. Informacje, o których mowa w ust. 1a, przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.”,

b) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, kryteria uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, biorąc pod uwagę w szczególności wartość procentową użytkowników, na których naruszenie bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych miało wpływ, czas trwania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych powodującego niedostępność lub ograniczenie dostępności sieci lub usług telekomunikacyjnych oraz rekomendacje i wytyczne Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA).”;

2) w art. 176a:

a) w ust. 1 pkt 3 otrzymuje brzmienie:

„3) bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej przedsiębiorcy lub świadczonych przez niego usług”,

b) w ust. 2 pkt 4 otrzymuje brzmienie:

„4) technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa;”;

3) w art. 209 w ust. 1 po pkt 27 dodaje się pkt 27^1 w brzmieniu:

„27^1)nie wypełnia obowiązku, o którym mowa w art. 175a ust. 1,”.

Art. 79. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) wprowadza się następujące zmiany:

1) w art. 5a ust. 2 otrzymuje brzmienie:

„2. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, natomiast w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, a w części dotyczącej zagrożeń cyberbezpieczeństwa, mogących doprowadzić do sytuacji kryzysowej, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.”;

2) w art. 6 po ust. 5a dodaje się ust. 5b w brzmieniu:

„5b. Właściciele, posiadacze samoistni i zależni, o których mowa w ust. 5, będący jednocześnie operatorami usług kluczowych w rozumieniu ustawy z dnia … o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), uwzględniają w planach ochrony infrastruktury krytycznej, dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 11 ust. 3 ustawy z dnia … o krajowym systemie cyberbezpieczeństwa.”;

3) w art. 8 w ust. 3 w pkt 14 kropkę zastępuje się średnikiem i dodaje się pkt 15 w brzmieniu:

„15) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa.”;

4) w art. 11 po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Centrum zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 37 ust. 1 ustawy z dnia … o krajowym systemie cyberbezpieczeństwa.”.

Art. 80. Minister właściwy do spraw informatyzacji, po wejściu w życie ustawy, przekaże Komisji Europejskiej informacje:

1) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym oraz o ich zadaniach;

2) o zakresie zadań CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku incydentu.

Art. 81. Organy właściwe, w terminie do dnia 9 listopada 2018 r., wydadzą decyzje o uznaniu za operatora usługi kluczowej oraz przekażą ministrowi właściwemu do spraw informatyzacji wnioski o wpisanie operatorów usług kluczowych do wykazu, o którym mowa w art. 7.

Art. 82. Minister właściwy do spraw informatyzacji, w terminie do dnia 9 sierpnia 2018 r., przekaże Grupie Współpracy sprawozdanie podsumowujące o:

1) incydentach poważnych zgłaszanych przez operatorów usług kluczowych, mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług kluczowych w państwach członkowskich Unii Europejskiej;
2) zgłaszanych przez dostawców usług cyfrowych incydentach istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej.

Art. 83. Minister właściwy do spraw informatyzacji, w terminie do dnia 9 listopada 2018 r., przekaże Komisji Europejskiej informacje o:

1) krajowych środkach umożliwiających identyfikację operatorów usług kluczowych;
2) wykazie usług kluczowych;
3) liczbie zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o którym mowa w załączniku nr 1 do ustawy, ze wskazaniem ich znaczenia w odniesieniu do tego sektora;
4) progach istotności skutku zakłócającego dla świadczonej usługi kluczowej branych pod uwagę przy kwalifikowaniu podmiotów, jako operatorów usług kluczowych .

Art. 84. Minister właściwy do spraw informatyzacji uruchomi system teleinformatyczny, o którym mowa w art. 46 ust. 1, do dnia 1 stycznia 2021 r.

Art. 85. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej zostanie przyjęta do dnia 31 października 2019 r.

Art. 86. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 76 zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 76, w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż do dnia 1 grudnia 2019 r., i mogą być zmieniane na podstawie tych przepisów.

Art. 87. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – Gospodarka morska wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 388 tys. zł;
3) w 2020 r. – 404 tys. zł;
4) w 2021 r. – 404 tys. zł;
5) w 2022 r. – 404 tys. zł;
6) w 2023 r. – 404 tys. zł;
7) w 2024 r. – 404 tys. zł;
8) w 2025 r. – 404 tys. zł;
9) w 2026 r. – 404 tys. zł;
10) w 2027 r. – 404 tys. zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – Gospodarka wodna wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 388 tys. zł;
3) w 2020 r. – 404 tys. zł;
4) w 2021 r. – 404 tys. zł;
5) w 2022 r. – 404 tys. zł;
6) w 2023 r. – 404 tys. zł;
7) w 2024 r. – 404 tys. zł;
8) w 2025 r. – 404 tys. zł;
9) w 2026 r. – 404 tys. zł;
10) w 2027 r. – 404 tys. zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – Informatyzacja wynosi:

1) w 2018 r. – 6 450 tys. zł;
2) w 2019 r. – 13 349 tys. zł;
3) w 2020 r. – 17 334 tys. zł;
4) w 2021 r. – 17 314 tys. zł;
5) w 2022 r. – 18 904 tys. zł;
6) w 2023 r. – 18 904 tys. zł;
7) w 2024 r. – 18 904 tys. zł;

8) w 2025 r. – 18 904 tys. zł;

9) w 2026 r. – 18 904 tys. zł;

10) w 2027 r. – 18 904 tys. zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – Transport wynosi:

1) w 2018 r. – 0 zł;

2) w 2019 r. – 388 tys. zł;

3) w 2020 r. – 404 tys. zł;

4) w 2021 r. – 404 tys. zł;

5) w 2022 r. – 404 tys. zł;

6) w 2023 r. – 404 tys. zł;

7) w 2024 r. – 404 tys. zł;

8) w 2025 r. – 404 tys. zł;

9) w 2026 r. – 404 tys. zł;

10) w 2027 r. – 404 tys. zł.

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – Zdrowie wynosi:

1) w 2018 r. – 0 zł;

2) w 2019 r. – 388 tys. zł;

3) w 2020 r. – 404 tys. zł;

4) w 2021 r. – 404 tys. zł;

5) w 2022 r. – 404 tys. zł;

6) w 2023 r. – 404 tys. zł;

7) w 2024 r. – 404 tys. zł;

8) w 2025 r. – 404 tys. zł;

9) w 2026 r. – 404 tys. zł;

10) w 2027 r. – 404 tys. zł.

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – Energia wynosi:

1) w 2018 r. – 0 zł;

2) w 2019 r. – 758 tys. zł;

3) w 2020 r. – 789 tys. zł;

4) w 2021 r. – 789 tys. zł;

5) w 2022 r. – 789 tys. zł;
6) w 2023 r. – 789 tys. zł;
7) w 2024 r. – 789 tys. zł;
8) w 2025 r. – 789 tys. zł;
9) w 2026 r. – 789 tys. zł;
10) w 2027 r. – 789 tys. zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 70 – Komisja Nadzoru Finansowego wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 388 tys. zł;
3) w 2020 r. – 404 tys. zł;
4) w 2021 r. – 404 tys. zł;
5) w 2022 r. – 404 tys. zł;
6) w 2023 r. – 404 tys. zł;
7) w 2024 r. – 404 tys. zł;
8) w 2025 r. – 404 tys. zł;
9) w 2026 r. – 404 tys. zł;
10) w 2027 r. – 404 tys. zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 203 tys. zł;
3) w 2020 r. – 212 tys. zł;
4) w 2021 r. – 212 tys. zł;
5) w 2022 r. – 212 tys. zł;
6) w 2023 r. – 212 tys. zł;
7) w 2024 r. – 212 tys. zł;
8) w 2025 r. – 212 tys. zł;
9) w 2026 r. – 212 tys. zł;
10) w 2027 r. – 212 tys. zł.

9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 42 – Sprawy wewnętrzne wynosi:

1) w 2018 r. – 242 tys. zł;

2) w 2019 r. – 360 tys. zł;
3) w 2020 r. – 0 zł;
4) w 2021 r. – 0 zł;
5) w 2022 r. – 0 zł;
6) w 2023 r. – 0 zł;
7) w 2024 r. – 0 zł;
8) w 2025 r. – 0 zł;
9) w 2026 r. – 0 zł;
10) w 2027 r. – 0 zł.

10. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1–7, zostaną zastosowane mechanizmy korygujące polegające na:

1) ograniczeniu wydatków związanych z realizacją zadań organu właściwego w zakresie identyfikacji operatorów usług kluczowych oraz prowadzenia bieżącej analizy podmiotów w danym sektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
2) zmniejszeniu liczby kontroli u operatorów usług kluczowych i dostawców usług cyfrowych;
3) rezygnacji z organizowania bądź uczestnictwa w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej;
4) ograniczeniu finansowania działalności sektorowego zespołu cyberbezpieczeństwa powołanego przez dany organ właściwy.

11. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 8, zostaną zastosowane mechanizmy korygujące polegające na ograniczeniu wydatków związanych z realizacją zadań ustawowych dotyczących obsługi incydentów.

12. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 9, zostaną zastosowane mechanizmy korygujące polegające na ograniczeniu wydatków związanych z zapewnieniem wyposażenia niezbędnego do obsługi Zespołu do spraw Incydentów Krytycznych.

13. W przypadku gdy wielkość wydatków w poszczególnych miesiącach zgodna jest z planem finansowym, przepisu ust. 10–12 nie stosuje się.

14. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw gospodarki morskiej.

15. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw gospodarki wodnej.

16. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw informatyzacji.

17. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw transportu.

18. Minister właściwy do spraw ochrony zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw ochrony zdrowia.

19. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10, dokonuje minister właściwy do spraw energii.

20. Komisja Nadzoru Finansowego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia

mechanizmów korygujących, o których mowa w ust. 10, dokonuje Komisja Nadzoru Finansowego.

21. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 12, dokonuje Prezes Urzędu Komunikacji Elektronicznej.

22. Minister właściwy do spraw wewnętrznych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny jego wykorzystania. Wdrożenia mechanizmów korygujących, o których mowa w ust. 13, dokonuje minister właściwy do spraw wewnętrznych.

Art. 88. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Załączniki
do ustawy
z dnia
(poz. …)

Załącznik nr 1

SEKTORY I PODSEKTORY ORAZ RODZAJE PODMIOTÓW

Sektor	Podsektor (jeżeli występuje)	Rodzaj podmiotu
Energia	Wydobywanie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2017 r. poz. 2126 oraz z 2018 r. poz. 650 i 723).
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2018 r. poz. 755), posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.
		Podmioty prowadzące działalność gospodarczą w zakresie świadczenia usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną.
	Ciepło	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła.
	Ropa naftowa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.
		Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.

		Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy – Prawo geologiczne i górnicze.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych.
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego.
	Dostawy i usługi dla sektora energii	Podmioty prowadzące działalność gospodarczą w zakresie dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii.
	Jednostki nadzorowane i podległe	Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane.
		Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97 z 09.04.2008, str. 72).
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2017 poz. 959 i 1089 oraz z 2018 r. poz. 138 i 650).
		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze wykonujący dla przewoźników lotniczych zadania związane z kontrolą bezpieczeństwa.

		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2017 r. poz. 2117 i 2361 oraz z 2018 r. poz. 650), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2017 r. poz. 2128).
		Podmiot zarządzający portem, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2017 r. poz. 1933)
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych.
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski.
		VTS (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2018 r. poz. 181).

	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a, ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2017 r. poz. 2222 oraz z 2018 r. poz. 12, 138, 159 i 317).
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, 2361 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 685 i 723).
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe.
		Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy – Prawo bankowe.
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 723 i 771).
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2017 r. poz. 1768, 2486 i 2491 oraz z 2018 r. poz. 106, 138, 650, 685, 723 i 771).
		Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
Ochrona zdrowia		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2018 r. poz. 160, 138 i 650).
		Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia.
		Narodowy Fundusz Zdrowia.
		Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej, w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2017 r. poz. 2211 oraz z 2018 r. poz. 650 i 697).
		Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.

		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.
		Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
Zaopatrzenie w wodę pitną i jej dystrybucja		Przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2017 r. poz. 328, 1566 i 2180 oraz z 2018 r. poz. 650).
Infrastruktura cyfrowa		Podmiot, który świadczy usługi DNS.
		Podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiącego obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego.
		Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).

Załącznik nr 2

USŁUGI CYFROWE

Nazwa usługi	Definicja usługi
Internetowa platforma handlowa	Usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową.
Usługa przetwarzania w chmurze	Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników.
Wyszukiwarka internetowa	Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

UZASADNIENIE

I. Potrzeba i cel regulacji

Stale rosnący wpływ technologii teleinformatycznych na rozwój społeczno-gospodarczy państw członkowskich Unii Europejskiej oraz wzrost ich wykorzystania sprawia, że oferowane produkty i usługi są obecnie coraz silniej zależne od zapewnienia cyberbezpieczeństwa. Rozbudowana architektura systemów teleinformatycznych, w tym operacje na dużych zasobach danych służą rozwojowi komunikacji, handlu, transportu i stanowią podstawę funkcjonowania usług kluczowych, cyfrowych i usług świadczonych przez administrację publiczną. Niestety możliwości jakie oferują nowoczesne technologie cyfrowe wykorzystywane są też w celu stosowania praktyk nieuczciwej konkurencji, przerywania ciągłości działania usług wybranych usług (czy to w celu chuligańskim czy też osłabienia pozycji konkurencyjnej danego podmiotu), popełniania przestępstw z wykorzystaniem Internetu, czy też prowadzenia działań o charakterze terrorystycznym.

O skali zagrożeń, jakie wiążą się z rozwojem Internetu, świadczą statystyki publikowane przez zespoły CERT (zespoły reagowania na incydenty komputerowe). W 2016 r. CERT Polska działający w NASK – Państwowym Instytucie Badawczym obsłużył 1926 incydentów, tj. o 32 proc. więcej niż w 2015 r. Do najczęściej zgłaszanych należą następujące kategorie incydentów: oszustwa komputerowe (55,5%), obraźliwe i nielegalne treści (12,31%), złośliwe oprogramowanie (10,96%), próby włamań (5,66%), gromadzenie informacji (3,37%), włamania (2,8%), dostępność zasobów (2,34%), atak na bezpieczeństwo informacji (2,34%), inne (4,72%). Dla przykładu phishing (podszywanie się pod znane marki celem wyłudzenia wrażliwych danych) był zgłaszany do CERT Polska 722 584 razy, a otrzymanych zgłoszeń dotyczących unikalnych adresów IP, które są narażone na ataki oraz wyciek informacji było 1,8 miliona[1)]. CERT firmy Orange w 2017 r. miesięcznie rejestrował nawet 10 mld zdarzeń systemowych (o ponad 1 mld więcej niż rok wcześniej). Zarejestrowanych anomalii w 2017 r. było prawie 148 tys. średnio każdego miesiąca, wśród których tysiąc z nich było sklasyfikowanych jako incydenty i wymagało udzielenia wsparcia. W sumie

[1)] „Krajobraz bezpieczeństwa polskiego Internetu 2016. Raport roczny z działalności CERT Polska”, NASK, https://www.cert.pl/PDF/Raport_CP_2016.pdf, dostęp: marzec 2018.

w 2017 r. CERT Orange Polska obsłużył 12 029 incydentów (17 199 incydentów w 2016 r.)[2)].

Powyższe uwarunkowania wymagały kompleksowego podejścia do zagadnień cyberbezpieczeństwa w państwach członkowskich Unii Europejskiej. W dniu 14 lutego 2013 r. Komisja Europejska przedstawiła wraz z Wysokim Przedstawicielem Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa komunikat w sprawie europejskiej strategii bezpieczeństwa cybernetycznego: „Otwarta, bezpieczna i chroniona cyberprzestrzeń”[3)]. Strategii towarzyszył wniosek legislacyjny w sprawie dyrektywy dotyczącej cyberbezpieczeństwa. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[4)] została przyjęta dnia 6 lipca 2016 r. (zwana dalej dyrektywą 2016/1148). Zobowiązuje ona wszystkie państwa członkowskie UE do zagwarantowania minimalnego poziomu zdolności krajowych w dziedzinie cyberbezpieczeństwa przez ustanowienie organów właściwych oraz pojedynczego punktu kontaktowego do spraw cyberbezpieczeństwa, powołanie zespołów reagowania na incydenty komputerowe (CSIRT) oraz przyjęcia krajowych strategii w zakresie cyberbezpieczeństwa.

Dyrektywa formułuje obowiązki służące zapewnieniu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społeczno-gospodarczej, a więc w energetyce, transporcie, bankowości, instytucjach finansowych, sektorze ochrony zdrowia, zaopatrzenia w wodę i infrastrukturze cyfrowej[5)]. Wprowadza pojęcie operatora usługi kluczowej, czyli podmiotu świadczącego z wykorzystaniem systemów informacyjnych usługę kluczową, w przypadku której incydenty bezpieczeństwa teleinformatycznego mogłyby mieć istotny wpływ na jej świadczenie.

Podjęcie prac związanych z kompleksowym uregulowaniem krajowego systemu cyberbezpieczeństwa wynika zatem z jednej strony z potrzeby zapewnienia systemowego podejścia do krajowego systemu cyberbezpieczeństwa w obliczu stale

[2)] „Raport CERT Orange Polska za rok 2017”, Orange Polska, https://cert.orange.pl/pobierz-opracowanie/15/1, dostęp: marzec 2018.
[3)] Join (2013) 1 Final, 07.02.2013.
[4)] Dz. Urz. UE L 194 z 19.07.2016, str. 1
[5)] Infrastruktura cyfrowa obejmuje punkty wymiany ruchu internetowego, dostawców usług systemu nazw domen, rejestrów nazw domen najwyższego poziomu.

rosnących i dynamicznie się zmieniających zagrożeń cyberbezpieczeństwa dla funkcjonowania państwa, gospodarki i społeczeństwa, a z drugiej strony konieczności wdrożenia do polskiego porządku prawnego dyrektywy 2016/1148.

W kwietniu 2017 r. został przyjęty uchwałą nr 52/2017 Rady Ministrów dokument strategiczny dotyczący bezpieczeństwa cyberprzestrzeni w postaci Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (dalej Krajowe Ramy). Powstał on w efekcie prac zespołu międzyresortowego pod kierunkiem Ministerstwa Cyfryzacji. Jednym z podstawowych zadań wskazanych w Krajowych Ramach jest uzyskanie wysokiego poziomu odporności krajowych systemów teleinformatycznych, służących świadczeniu usług kluczowych, usług cyfrowych oraz usług administracji publicznej. W tym celu przewidziano rozbudowę krajowego systemu cyberbezpieczeństwa w taki sposób, aby był ukierunkowany na zbudowanie zdolności w zakresie bieżącego monitorowania zagrożeń oraz zintegrowanego zarządzania cyberbezpieczeństwem w skali kraju.

Działania powyższe, podjęte przez Ministerstwo Cyfryzacji we współpracy z innymi resortami wynikają ze zmiany ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2018 r. poz. 762) w grudniu 2015 r.[6)], która przypisała do działu informatyzacja kompetencje w zakresie bezpieczeństwa cyberprzestrzeni. Działania są motywowane potrzebą ustanowienia kompleksowego systemu bezpieczeństwa teleinformatycznego państwa. Zalecenie to zostało sformułowane w związku z kontrolą przeprowadzoną przez Najwyższą Izbę Kontroli w 2014 r. w instytucjach publicznych odpowiedzialnych za bezpieczeństwo cyberprzestrzeni.

II. Stan rzeczywisty w dziedzinie regulacji

1. Prawo Unii Europejskiej[7)]

Dyrektywa 2016/1148 jest pierwszym aktem prawa UE w zakresie cyberbezpieczeństwa, wprowadzającym międzysektorowe regulacje. Czas na implementację dyrektywy do porządków prawnych państw członkowskich upływa 9 maja 2018 r. Tekst dyrektywy koncentruje się wokół trzech filarów:

- instytucjach, jakie powinny powstać we wszystkich państwach członkowskich,

[6)] Dz. U. poz. 2281.

[7)] Treść niniejszego rozdziału opiera się na analizach NC Cyber. Źródło: https://cyberpolicy.nask.pl/cp/ramy-prawne/dyrektywa-nis/24,Dyrektywa-Parlamentu-Europejskiego-i-Rady-UE-20161148-z-dnia-6-lipca-2016-r-w-sp.html

- współpracy na poziomie europejskim,
- zobowiązaniach w zakresie bezpieczeństwa sieci i informacji.

W zakresie filaru pierwszego każde państwo członkowskie jest zobligowane do ustanowienia organów właściwych ds. bezpieczeństwa sieci i informacji, odpowiedzialnych za monitorowanie stosowania jej przepisów w sektorach objętych jej zakresem. Z uwagi na różnice w krajowych strukturach zarządzania, państwa członkowskie mogą wyznaczać więcej niż jeden właściwy organ krajowy odpowiedzialny za wykonywanie zadań związanych z cyberbezpieczeństwem operatorów usług kluczowych i dostawców usług cyfrowych.

Ponadto każde państwo członkowskie, w przypadku ustanowienia wielu organów właściwych, musi ustanowić Pojedynczy Punkt Kontaktowy (PPK). Zadaniem Pojedynczego Punktu Kontaktowego jest wzmacnianie współpracy między państwami członkowskimi. PPK będzie gromadził informacje o incydentach w skali kraju i przez kontakt ze swoimi odpowiednikami z zagranicy wzmacniał wymianę informacji o znaczących, transnarodowych incydentach.

Ostatnią wymaganą przez dyrektywę instytucją jest CSIRT, obejmujący cały zakres podmiotowy regulacji. Państwa członkowskie mogą wskazać kilka CSIRT, mogą także wskazać jeden, na przykład w obrębie organu właściwego. Dyrektywa zachowuje dużą elastyczność, jeżeli chodzi o wewnętrzne struktury sytemu cyberbezpieczeństwa. Oznacza to, że kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy dla całego kraju, kilka CSIRT poziomu narodowego, bądź zbudować sieć CSIRT sektorowych.

Zakres podmiotowy dyrektywy ujęty został w dwóch załącznikach. Załącznik II dotyczy operatorów usług kluczowych, załącznik III natomiast reguluje dostawców usług cyfrowych. W odniesieniu do operatorów wskazanych w każdym z załączników obowiązywać będą inne wymagania.

W przypadku dostawców usług cyfrowych (załącznik III) obowiązywać będzie bardziej łagodne i reaktywne podejście obejmujące działania nadzorcze *ex post*, tzn. po zaistnieniu incydentu i tylko przez to państwo, na terenie którego dostawca usługi ma swoją siedzibę. Tym samym, podmioty z załącznika III nie będą podlegały ani opisanemu wcześniej procesowi identyfikacji, ani raportowania, jak w przypadku operatorów usług kluczowych. Takie podejście spowodowane jest międzynarodowym wymiarem operatorów dostarczających usługi cyfrowe, a tym samym obawą przed

fragmentaryzacją jednolitego rynku cyfrowego UE. W wyniku negocjacji ustalono, że regulacjami zostaną objęte serwisy zakupowe, wyszukiwarki internetowe oraz usługi chmury obliczeniowej.

Dyrektywa nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to usługi kluczowe wymienione w dyrektywie.

Najważniejsze jest jednak to, że dyrektywa 2016/1148 stanowi harmonizację minimalną i nie ogranicza możliwości państw członkowskich do regulowania problematyki bezpieczeństwa teleinformatycznego administracji publicznej, a także objęcia zakresem większej liczby podmiotów. Wszystko to zależy od państw członkowskich.

Specyfika uregulowania dostawców usług cyfrowych polega na tym, że zainteresowany właściwy organ powinien podejmować działania wyłącznie wtedy, gdy otrzymał dowód – na przykład od samego dostawcy usług cyfrowych, innego właściwego organu, w tym właściwego organu innego państwa członkowskiego, lub od użytkownika usługi – że dostawca usług cyfrowych nie spełnia wymogów niniejszej dyrektywy, w szczególności w wyniku wystąpienia incydentu. Właściwy organ nie powinien mieć ogólnego obowiązku nadzorowania dostawców usług cyfrowych.

Drugi filar dyrektywy, to współpraca między państwami członkowskimi. Dyrektywa 2016/1148 wprowadza mechanizmy współpracy na dwóch poziomach: technicznym i polityczno-strategicznym. Współpraca techniczna ma być zapewniona przez europejską Sieć CISRT oraz stworzenie mechanizmów wymiany informacji o incydentach transgranicznych między CSIRT wyznaczonymi dla operatorów usług kluczowych oraz dostawcami usług cyfrowych. Natomiast współpraca na poziomie polityczno-strategicznym ma być realizowana przez utworzenie Grupy Współpracy, która zajmie się wypracowaniem wspólnych koncepcji strategicznych oraz będzie przyjmowała m.in. roczne raporty od właściwych organów.

Trzeci filar dyrektywy to zobowiązania w zakresie bezpieczeństwa sieci i informacji. Zobowiązania te są różne w zależności od załącznika. Operatorzy usług kluczowych będą zobowiązani do dokonania oceny zagrożeń cyberbezpieczeństwa, na jakie są narażeni, oraz do przyjęcia odpowiednich i proporcjonalnych środków, mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających ich sieciom i systemom informatycznym, mogących znacząco zakłócić ciągłość działania

kluczowych usług (obowiązkowe raportowanie). Raportowaniu podlegały będą incydenty o „znaczącym wpływie na ciągłość działania operatorów", co *de facto* oznacza, że progi raportowania określą państwa członkowskie w procesie implementacji. Podmioty załącznika III będą natomiast objęte regulacją reaktywnym nadzorem *ex post*.

Dyrektywa nakłada także na państwa członkowskie obowiązek przyjęcia narodowej strategii bezpieczeństwa sieci i informacji, w której określone zostaną m.in.: narodowe cele i priorytety w dziedzinie cyberbezpieczeństwa, role i obowiązki organów administracji publicznej w procesie osiągania wyznaczonych celów, zasady współpracy sektora publicznego i prywatnego oraz krajowa analiza ryzyka i zadania w zakresie edukacji na rzecz cyberbezpieczeństwa.

Przepisy dyrektywy umożliwiają stworzenie zarówno scentralizowanego systemu na poziomie krajowym, jak i podzielenie kompetencji między różne podmioty wymieniające informacje w oparciu o zbudowane mechanizmy współpracy. Ponadto dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformatycznego. Dyrektywa daje organom publicznym konkretne narzędzie do przeciwdziałania i reakcji na incydenty w cyberprzestrzeni. Będzie to możliwe m.in. dzięki nałożonym obowiązkom raportowania, przez obowiązek przygotowania krajowych strategii, skoordynowanie przepływu informacji, czy też zinstytucjonalizowanie współpracy CSIRT.

2. Prawo krajowe

Obecnie w Polsce kwestie zabezpieczania systemów teleinformatycznych są regulowane sektorowo lub wycinkowo, według zadań różnych podmiotów. Istnieją regulacje dotyczące zapewnienia systemu zarządzania bezpieczeństwem informacji w podmiotach publicznych[8)], zwalczania cyberprzestępczości, dotyczące zapobiegania zagrożeniom o charakterze terrorystycznym[9)] bądź czy też zarządzania kryzysowego[10)].

[8)] Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247).

[9)] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730).

[10)] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566).

Istnieją regulacje dotyczące np. konieczności zabezpieczenia usług świadczonych przez przedsiębiorców telekomunikacyjnych[11)] czy banki[12)].

Warto wskazać, że żadna w wymienionych wyżej regulacji nie ujmuje problemu całościowo. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych jest ograniczona do zasad prowadzenia działań antyterrorystycznych oraz współpracy między organami właściwymi w zakresie prowadzenia tych działań. Przepisy ustawy o zarządzaniu kryzysowym odnoszą się do działań związanych z zapobieganiem i zarządzaniem w sytuacjach kryzysowych. Ustawy regulujące pracę organów ścigania, np. ustawa z dnia 6 kwietnia 1990 r. o Policji[13)] czy też ustawa z dnia 6 czerwca 1997 r. – Kodeks karny obejmują kwestie związane z zapobieganiem i zwalczaniem przestępstw w cyberprzestrzeni.

Pewne elementy o charakterze bezsankcyjnym regulujące wymagania bezpieczeństwa teleinformatycznego odnoszące się do sfery infrastruktury krytycznej zostały zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), przyjmowanego na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[14)]. Rządowe Centrum Bezpieczeństwa weryfikuje plany operatorów infrastruktury krytycznej m.in. pod kątem oceny ryzyka, stosowanych zabezpieczeń i przyjętych w obiektach zasad ochrony teleinformatycznej. Należy jednak podkreślić, że inna jest podstawa prawna dyrektywy 2016/1148, którym jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej odnoszący się do wspólnego rynku. Kwestia ochrony krajowej infrastruktury krytycznej jest natomiast kompetencją wyłączną państw członkowskich, ściśle powiązaną ze sferą bezpieczeństwa narodowego, nieobjętą traktatami unijnymi.

Pewne wymagania w zakresie bezpieczeństwa informacji, dotyczące zarówno przedsiębiorców, jak i jednostek sektora finansów publicznych znajdują się w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny[15)], ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[16)], ustawie z dnia 27 sierpnia 2009 r. o finansach

[11)] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650).
[12)] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, 2361 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 685 i 723).
[13)] Dz. U. z 2017 r. poz. 2067 i 2405 oraz z 2018 r. poz. 106, 138, 416, 650 i 730.
[14)] Dz. U. z 2017 r. poz. 209 i 1566.
[15)] Dz. U. z 2017 r. poz. 2204 oraz z 2018 r. poz. 20, 305 i 663.
[16)] Dz. U. z 2016 r. poz. 922 oraz z 2018 r. poz. 138 i 723.

publicznych[17)], ustawie z dnia 29 września 1994 r. o rachunkowości[18)], ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[19)], ustawie z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej[20)], ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[21)], ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach[22)], ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (dalej ustawowo – Prawo bankowe), ustawie z dnia 5 września 2016 r. o usługach zaufania i identyfikacji elektronicznej[23)], ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną[24)], ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej[25)] oraz ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji[26)].

Nie zostały dotychczas jednak określone sposoby realizacji usług obsługi incydentów, zasady współpracy podmiotów realizujących takie usługi oraz sposoby postępowania zespołów reagowania na incydenty komputerowe podczas obsługi incydentu. Brak jest w polskim prawie przepisów służących ustanowieniu obowiązków w zakresie zarządzania ryzykiem, stosowania zabezpieczeń, zgłaszania i obsługi incydentów, objęcia świadczonych usług systemem monitorowania w trybie ciągłym.

Projektowany akt jest pierwszym dokumentem, który całościowo określa zasady funkcjonowania krajowego systemu cyberbezpieczeństwa.

3. Warstwa strategiczno-polityczna krajowego systemu cyberbezpieczeństwa

System ochrony cyberprzestrzeni w Polsce ma charakter zdecentralizowany, a kompetencje dotyczące cyberbezpieczeństwa mogą być realizowane przez Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego, Ministra Spraw Wewnętrznych i Administracji, Policję, Rządowe Centrum Bezpieczeństwa, czy też Ministra Cyfryzacji. Cyberbezpieczeństwem zajmują się także zespoły CSIRT utworzone przez operatorów telekomunikacyjnych, banki, przedsiębiorstwa energetyczne oraz środowiska naukowo-badawcze. Wymienione podmioty realizują

[17)] Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62.
[18)] Dz. U. z 2018 r. poz. 395, 398 i 650.
[19)] Dz. U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 933.
[20)] Dz. U. z 2017 r. poz. 2159 i 2203.
[21)] Dz. U. z 2017 r. poz. 1845 oraz z 2018 r. poz. 697.
[22)] Dz. U. z 2018 r. poz. 217, 357, 398 i 650.
[23)] Dz. U. z 2016 r. poz. 1579 oraz z 2018 r. poz. 650.
[24)] Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650.
[25)] Dz. U. z 2016 r. poz. 1068, z 2017 r. poz. 60 oraz z 2018 r. poz. 650.
[26)] Dz. U. z 2018 r. poz. 419.

zadania w zakresie cyberbezpieczeństwa w sferze cywilnej, zwalczania cyberprzestępczości, zapobiegania zdarzeniom terrorystycznym i obrony narodowej.

Zgodnie z art. 146 ust. 4 pkt 7 i 11 Konstytucji RP, Rada Ministrów zapewnia bezpieczeństwo wewnętrzne państwa i porządek publiczny oraz sprawuje ogólne kierownictwo w dziedzinie obronności kraju. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej definiuje działy administracji rządowej (w tym dział sprawy wewnętrzne obejmujący kwestie bezpieczeństwa wewnętrznego i porządku publicznego oraz dział obrona narodowa), które są następnie przypisywane poszczególnym ministrom.

Wraz ze zmianą ustawy z dnia 4 września 1997 r. o działach administracji rządowej w grudniu 2015 r., przypisującą do działu informatyzacja kompetencje z zakresu bezpieczeństwa cyberprzestrzeni, Ministerstwo Cyfryzacji podjęło się działań związanych z uregulowaniem problematyki cyberbezpieczeństwa dla administracji jak i dla całej cywilnej części kraju.

Minister Cyfryzacji zgodnie z obowiązującym stanem prawnym odpowiada za zapewnienie minimalnych wymagań z zakresu bezpieczeństwa teleinformatycznego w administracji publicznej – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne[27)] oraz rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ramach Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej „KRI" lub „Krajowej Ramy"). Wymogi dotyczące interoperacyjności, dostępności oraz bezpieczeństwa zawarte są w art. 13–16 ustawy, natomiast § 20 rozporządzenia określa wymagania systemu zarządzania bezpieczeństwem informacji zapewniającego poufność, dostępność i integralność informacji. W 2015 r. Minister Cyfryzacji zatwierdził również Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych. Celem Wytycznych jest zapewnienie wsparcia przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych, w tym ww. wymagań w obszarze bezpieczeństwa informacji.

[27)] Dz. U. z 2017 r. poz. 570.

Do Urzędu Komunikacji Elektronicznej zgłaszane są zgodnie z ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (dalej „PT" lub „ustawa – Prawo telekomunikacyjne") najważniejsze incydenty w sieciach telekomunikacyjnych. Ustawa – Prawo telekomunikacyjne oraz wydane na jej podstawie akty wykonawcze zawierają również przepisy związane z kwestiami bezpieczeństwa lub integralności sieci i usług telekomunikacyjnych, ciągłości działania, bezpieczeństwa danych osobowych, realizacją obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego[28)]. Minister Cyfryzacji zgodnie z ustawą o usługach zaufania i identyfikacji elektronicznej zapewnia również funkcjonowanie krajowej infrastruktury zaufania oraz sprawuje nadzór nad dostawcami usług zaufania.

Projektowana ustawa nie reguluje kwestii określonych w innych ustawach, np. dotyczących stanów nadzwyczajnych, czy zarządzania kryzysowego. Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym[29)], ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej[30)] oraz ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej[31)] regulujące funkcjonowanie państwa w warunkach stanów nadzwyczajnych. Stan wyjątkowy i stan wojenny wprowadza Prezydent Rzeczypospolitej Polskiej, na wniosek Rady Ministrów, a stan klęski żywiołowej wprowadza Rada Ministrów.

Zgodnie z art. 7 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (dalej „ustawa o zarządzaniu kryzysowym"), Rada Ministrów sprawuje zarządzanie kryzysowe na terytorium RP (w przypadkach niecierpiących zwłoki minister właściwy do spraw wewnętrznych). Rządowy Zespół Zarządzania Kryzysowego jest organem opiniodawczo-doradczym przy Radzie Ministrów. Do zadań Zespołu należy przygotowywanie propozycji użycia sił i środków niezbędnych do opanowania sytuacji kryzysowych; doradzanie w zakresie koordynacji działań organów administracji rządowej, instytucji państwowych i służb w sytuacjach kryzysowych; opiniowanie sprawozdań końcowych z działań podejmowanych w związku z zarządzaniem kryzysowym; opiniowanie potrzeb w zakresie odtwarzania infrastruktury lub

[28)] Obowiązki w dziedzinie cyberbezpieczeństwa zostały określone w Dziale VII i Dziale VIII Prawa telekomunikacyjnego.
[29)] Dz. U. z 2017 r. poz. 1928.
[30)] Dz. U. z 2017 r. poz. 1932.
[31)] Dz. U. z 2017 r. poz. 1897.

przywrócenia jej pierwotnego charakteru; opiniowanie i przedkładanie Radzie Ministrów Krajowego Planu Zarządzania Kryzysowego; opiniowanie projektu zarządzenia Prezesa Rady Ministrów w sprawie wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego. Na mocy ustawy o zarządzaniu kryzysowym działa także Rządowe Centrum Bezpieczeństwa, które pełni funkcję krajowego centrum zarządzania kryzysowego, odpowiada za planowanie cywilne, tworzy katalog zagrożeń, monitoruje zagrożenia, organizuje szkolenia oraz prowadzi współpracę międzynarodową. Na podstawie art. 25 ustawy o zarządzaniu kryzysowym Minister Obrony Narodowej, na wniosek wojewody, może przekazać do jego dyspozycji oddziały Sił Zbrojnych w celu wykonywania zadań z zakresu zarządzania kryzysowego.

Zgodnie z ustawą z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[32)] i ustawą z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (dalej „ustawa o działaniach antyterrorystycznych) ABW odpowiada za rozpoznawanie, zapobieganie i wykrywania zagrożeń sieci teleinformatycznych istotnych dla państwa; przeprowadzanie oceny bezpieczeństwa systemów, wskazywanie podatności; żądanie „blokady dostępności"; prowadzenie rejestru zdarzeń naruszających bezpieczeństwo; analiza naruszeń i wydawanie rekomendacji. Policja wykonuje zadania z zakresu zwalczania cyberprzestępczości (w strukturze Komendy Głównej Policji funkcjonuje Biuro do Walki z Cyberprzestępczością).

W Polsce nie ma przepisów ustawowych określających szczegółowy zakres kompetencji organów w obszarze cyberbezpieczeństwa w odniesieniu do wskazanych w dyrektywie sektorów. Wspomniany już wcześniej dokument o charakterze strategicznym – Krajowe Ramy Polityki Cyberbezpieczeństwa przewiduje określenie zakresu odpowiedzialności, obowiązków i uprawnień uczestników systemu, sposobów wzajemnego oddziaływania na innych uczestników systemu. Krajowe Ramy zakładają w szczególności określenie kompetencji organów właściwych, odpowiedzialnych za sprawowanie nadzoru w zakresie systemów informacyjnych w sektorach, w których świadczone są usługi kluczowe i usługi cyfrowe.

Będący załącznikiem do Krajowych Ram, Plan działań zawiera zestawienie projektów szczegółowych realizowanych przez poszczególne resorty/podmioty. Tym samym Plan

[32)] Dz. U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138, 650, 723 i 730.

działań obejmuje działania o charakterze legislacyjnym, projekty związane z budową systemów informacyjnych służących bieżącemu zarządzaniu cyberbezpieczeństwem, projekty o charakterze organizacyjnym jak ćwiczenia, treningi i testy, czy też działania ciągłe związane choćby z rozbudową polskiego potencjału technologicznego i dotyczące udziału Polski we współpracy międzynarodowej w dziedzinie cyberbezpieczeństwa. W ramach realizacji Krajowych Ram przygotowano i rozesłano w ramach prekonsultacji do poszczególnych ministerstw projekt ustawy o krajowym systemie cyberbezpieczeństwa. Opracowana została koncepcja funkcjonalna projektu Narodowa Platforma Cyberbezpieczeństwa, w tym centralna warstwa analityczna, przeprowadzono ćwiczenia z zakresu cyberbezpieczeństwa CEREX, jak również we współpracy z Ministerstwem Rozwoju (obecnie Ministerstwo Przedsiębiorczości i Technologii) rozpoczęto realizację projektu Cyberpark ENIGMA.

4. Podmioty odpowiedzialne za cyberbezpieczeństwo na poziomie operacyjnym

W Polsce funkcjonują różne zespoły CSIRT, jednak tylko trzy działają od lat w ramach swojej właściwości na poziomie krajowym. Zamiast tworzyć nowe podmioty, projekt ustawy nada określone zadania istniejącym podmiotom, które w ramach swojej działalności zajmują się reagowaniem na incydenty komputerowe.

CERT GOV

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego Zespołu CERT odpowiadającego za koordynację procesu reagowania na incydenty komputerowe występujące w obszarze administracji rządowej oraz infrastruktury krytycznej. Jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym.

SRnIK RON

System Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej realizuje zadania w zakresie koordynacji procesów zapobiegania, wykrywania i reagowania na

incydenty komputerowe w systemach i sieciach teleinformatycznych resortu obrony narodowej.

SRnIK RON zorganizowany jest w trzypoziomową strukturę zgodnie z założeniami NATO (Centrum Koordynacyjne SRnIK, Centrum Wsparcia SRnIK, które realizuje zadania zgodne z zakresem działania Zespołów CERT oraz Administratorzy systemów teleinformatycznych jednostek i komórek organizacyjnych RON).

Do głównych zadań SRnIK należy koordynacja reagowania na incydenty komputerowe, obsługa i analiza zdarzeń oraz incydentów, a także prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego. W ramach podejmowanych zadań SRnIK współpracuje z jednostkami i komórkami organizacyjnymi Resortu Obrony Narodowej, jak również z organizacjami poza resortowymi, krajowymi i międzynarodowymi.

Narodowe Centrum Cyberbezpieczeństwa

W lipcu 2016 r. w ramach NASK, powołane zostało Narodowe Centrum Cyberbezpieczeństwa (NC Cyber). NC Cyber pomyślane jest jako centrum szybkiego reagowania na zagrożenia i zgłaszane incydenty w cyberprzestrzeni, a w razie ewentualnych ataków – podejmowania koniecznych działań we współpracy z ośrodkami w kraju i za granicą w celu przeanalizowania natury, sposobu, zasięgu incydentu oraz wymiany informacji w celu ostrzeżenia kluczowych sektorów i instytucji. NC Cyber wydaje rekomendację postępowania w obliczu zagrożenia oraz koniecznych działań minimalizujących skutki. Centrum operacyjne NC Cyber funkcjonuje w trybie 24/7 przez 365 dni w roku. NC Cyber oparte jest na kilku filarach: operacyjnym, analitycznym badawczo-rozwojowym, szkoleniowym oraz obszarze polityk i standardów. Założeniem powołania NC Cyber była dalsza rozbudowa funkcji operacyjnych i analityczno-technicznych, tak aby można było zarządzać bezpieczeństwem cyberprzestrzeni w krytycznych dla państwa i gospodarki obszarach działalności oraz budowa kompetencji w obszarze strategicznym.

Podmioty publiczne i prywatne mogą współpracować z NC Cyber na podstawie zawartych porozumień w zakresie cyberbezpieczeństwa, mogą również delegować swoich przedstawicieli do bieżącej współpracy. Porozumienia o współpracy zostały już podpisane z ponad 40 podmiotami, w tym przedstawicielami sektora telekomunikacyjnego, finansowego (banków i instytucji finansowych), energetycznego,

kolejowego, dostawcami usług cyfrowych. Zostały zbudowane kanały komunikacji między uczestniczącymi podmiotami (strefa partnera, system informowania o incydentach – MISP).

III. Opis proponowanych zmian – przewidywane skutki prawne wejścia aktu w życie

Projektowana ustawa ma na celu określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakresu i trybu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Projekt ustawy definiuje podstawowe pojęcia niezbędne dla krajowego systemu cyberbezpieczeństwa. W obecnym stanie prawnym brak normatywnych definicji sprawia, że obszar ten jest zarazem niedostatecznie identyfikowany, jak i regulowany. Projektowane definicje są zgodne z treścią dyrektywy 2016/1148, co pozwoli również ocenić osiągnięcie celów tej dyrektywy i Krajowych Ram. Projekt ustanawia też Krajowy system cyberbezpieczeństwa oraz określa podmioty do niego należące.

Projekt ustawy zawiera zasady wskazywania operatorów usług kluczowych, a wypełniając dyspozycje, o których mowa w dyrektywie 2016/1148, określa obowiązki dla operatorów usług kluczowych dotyczące wdrożenia efektywnego systemu zarządzania bezpieczeństwem, obejmującego m.in. zarządzanie ryzykiem, procedury i mechanizmy zgłaszania i postępowania z incydentami czy organizację struktur na poziomie operatora. W załączniku do ustawy znajdują się natomiast wszystkie potencjalne kategorie podmiotów w poszczególnych sektorach gospodarki i działalności państwa, z których mogą być wyłaniani w drodze decyzji administracyjnej operatorzy usług kluczowych.

Projekt ustawy precyzuje obowiązki nakładane na dostawców usług cyfrowych, uwzględniając istniejące w tym zakresie ograniczenia określone przez dyrektywę 2016/1148.

Obowiązki nakładane na podmioty publiczne są uregulowane odrębnie od tych nakładanych na operatorów i dostawców.

Jedną z najistotniejszych części proponowanych zmian jest określenie w projektowanej ustawie systemu reagowania na incydenty i włączenie w ten proces wszystkich

zainteresowanych podmiotów. Założeniem systemu reagowania na incydenty jest jego kompletność (ustanowienie we wszystkich kluczowych sektorach), transparentność i kompleksowość.

Po pierwsze, zakłada się określenie zadań CSIRT, odpowiedzialnych za przeciwdziałanie zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także koordynację obsługi poważnych, istotnych i krytycznych incydentów. Po drugie, ustawa przewiduje włączenie aspektów cyberbezpieczeństwa do sfery zarządzania państwem. CSIRT informują się wzajemnie oraz informują Rządowe Centrum Bezpieczeństwa o incydencie krytycznym, który może spowodować wystąpienie sytuacji kryzysowej dla bezpieczeństwa lub porządku publicznego. Dodatkowo ustawa przewiduje utworzenie Zespołu do spraw Krytycznych Incydentów jako organu pomocniczego, powoływanego w sprawach obsługi i koordynacji wymienionych incydentów krytycznych na poziomie krajowych CSIRT i RCB.

Projekt określa zasady dotyczące sposobu przekazywania do publicznej wiadomości komunikatów nt. cyberbezpieczeństwa oraz określa, zgodnie z wymaganiami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), zasady przetwarzania danych osobowych w ramach funkcjonowania krajowego systemu cyberbezpieczeństwa, w tym zwłaszcza w zakresie przetwarzania danych dotyczących incydentów.

Projekt ustawy ustanawia organy właściwe ds. cyberbezpieczeństwa odpowiedzialne za sprawowanie nadzoru wobec operatorów usług kluczowych w sektorach wymienionych w dyrektywie 2016/1148. Organy właściwe są elementem krajowego systemu cyberbezpieczeństwa odpowiedzialnym również za opracowywanie we współpracy z CSIRT wytycznych bezpieczeństwa teleinformatycznego w wymiarze sektorowym. Ustanawiane przez organy właściwe sektorowe zespoły cyberbezpieczeństwa będą miały możliwość przyjmowania zgłoszeń o incydentach poważnych, ich analizę oraz wsparcie w ich obsłudze we współpracy z właściwym CSIRT.

Projekt zakłada również przypisanie nowych obowiązków ministrowi właściwemu do spraw informatyzacji realizującemu funkcje techniczne na potrzeby krajowego systemu

cyberbezpieczeństwa. Związane są one z prowadzeniem systemu teleinformatycznego wykorzystywanego do wymiany informacji między podmiotami tworzącymi krajowy system cyberbezpieczeństwa, do dynamicznego szacowania ryzyka na poziomie krajowym oraz do ostrzegania o zagrożeniach cyberbezpieczeństwa.

Jednocześnie projekt ustawy ustanawia pojedynczy punkt kontaktowy ds. cyberbezpieczeństwa prowadzony przez ministra właściwego ds. informatyzacji. Według założeń regulacji pojedynczy punkt kontaktowy realizowałby funkcje swoistego „łącznika" i zajmowałby się wymianą informacji na rzecz organów właściwych, organów władz publicznych i CSIRT. Pojedynczy Punkt Kontaktowy zapewni odbieranie i przekazywanie zgłoszeń incydentów poważnych i istotnych z innych krajów członkowskich, reprezentację Rzeczypospolitej Polskiej w Grupie Współpracy, współpracę z Komisją Europejską, współpracy między organami właściwymi w Rzeczypospolitej Polskiej i organami właściwymi państw członkowskich Unii Europejskiej, współpracę między organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej.

Projekt ustawy określa zadania Ministra Obrony Narodowej związane z zakresem ustawy, zwłaszcza w zakresie zapewnienia zdolności Siłom Zbrojnym RP do prowadzenia działań militarnych w przypadkach szczególnych zagrożeń, ocenę wpływu incydentów na system obrony państwa oraz kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego.

Następnie projekt reguluje kwestie nadzoru i kontroli realizacji zadań określonych w ustawie. Określono zakres kontroli, uprawnienia kontrolerów oraz kwestie postępowania w razie stwierdzenia naruszenia przepisów ustawy.

Określono zadania Pełnomocnika Rządu do spraw Cyberbezpieczeństwa (nowego podmiotu zajmującego się koordynacją działań dotyczących zapewnienia cyberbezpieczeństwa w RP) oraz Kolegium do spraw Cyberbezpieczeństwa (organu opiniodawczo-doradczego w sprawach cyberbezpieczeństwa), celem zapewnienia koordynacji realizacji zadań na poziomie rządowym.

Projektowana regulacja określi również ustawowe zasady realizacji i tworzenia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Szczegółowy opis proponowanych zmian

Rozdział 1: Przepisy ogólne

W przepisach ogólnych określono zakres regulacji, słowniczek pojęć ustawowych, katalog podmiotów tworzących krajowy system cyberbezpieczeństwa oraz cele projektowanej ustawy. Ustawa określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, zakres oraz tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Wzorem podejścia przyjętego w dyrektywie 2016/1148 ustawa nie ma zastosowania wobec przedsiębiorców telekomunikacyjnych i dostawców usług zaufania, którzy zostali już objęci europejskimi i krajowymi wymaganiami sektorowymi z zakresu cyberbezpieczeństwa.

Definiowane pojęcia, co do zasady nie pojawiają się w innych aktach prawnych, a ich określenie na poziomie ustawy pozwoli na dokładne wyznaczenie ram przedmiotowych projektowanego aktu. Najważniejsze pojęcia zdefiniowane w art. 2 projektu zostały przedstawione poniżej.

Ustawa usankcjonowała istniejące i działające od lat w ramach swojej właściwości trzy podmioty na poziomie krajowym, które w ramach swojej działalności zajmują się reagowaniem na incydenty komputerowe. Zgodnie z terminologią przyjętą w dyrektywie 2016/ 1148 zostały one określone jako CSIRT (ang. Computer Security Incident Response Teams) i w Polsce są to **CSIRT GOV**, czyli Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, **CSIRT MON**, czyli System Reagowania na Incydenty Komputerowe Resortu Obrony Narodowej oraz **CSIRT NASK**, czyli NC Cyber, które zostały opisane wcześniej.

Ustawa wprowadza również pojęcie **sektorowego zespołu cyberbezpieczeństwa**, a więc zespołu ustanowionego przez organ właściwy dla danego sektora lub podsektora wymienionego w załączniku do ustawy, odpowiedzialnego za obsługę lub wsparcie obsługi incydentów w danym sektorze lub podsektorze. Sektorowe zespoły zostały uregulowane w art. 44 projektu.

Projektodawca zdefiniował **cyberbezpieczeństwo** jako odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych

przez te systemy informacyjne. Jest to definicja oparta na definicji „bezpieczeństwa sieci i systemów informatycznych" z dyrektywy 2016/1148, przy uwzględnieniu zmian niektórych pojęć (np. systemu informacyjnego).

Ustawa wprowadza kilka kategorii **incydentów**, które różnią się w zależności rodzaju podmiotu, który je zgłasza, i stopnia jego oddziaływania (progów). **Incydent poważny**, zgłaszany przez operatora usług kluczowych, związany jest z poważnym obniżeniem jakości lub przerwaniem ciągłości działania świadczonej usługi kluczowej, a **incydent istotny** ma istotny wpływ na świadczenie usługi cyfrowej. **Incydent w podmiocie publicznym** nie jest uzależniony od progu oddziaływania, ale dotyczy wszystkich zdarzeń, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego. Przewidziano również **incydenty krytyczne**, skutkujące znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów gospodarczych, działania instytucji publicznych.

Jedną z najważniejszych definicji ustawowych, które warunkują dalsze działania regulacyjne, operacyjne, techniczne i kontrolne, jest definicja **systemu informacyjnego**. Definicja systemu informacyjnego opiera się na definicji systemu teleinformatycznego, zaczerpniętej z obowiązującej ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (taka sama występuje w ustawie o świadczeniu usług drogą elektroniczną) oraz danych w postaci elektronicznej przetwarzanych w tych systemach. Systemem teleinformatycznym jest zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy – Prawo telekomunikacyjne. Projektodawca, wprowadzając zgodnie z wymogami dyrektywy 2016/1148 definicję systemów informacyjnych, która dodatkowo obejmuje przetwarzane w systemie teleinformatycznym dane w postaci elektronicznej, przyjął podejście, że pojęcie systemu informacyjnego uwzględnia komponent sprzętu, oprogramowania, sieci oraz danych i jest rozumiane z punktu widzenia realizacji usług kluczowych i usług cyfrowych. Do funkcjonalnej realizacji takich usług niezbędne jest uwzględnienie w strukturze elementów systemu informacyjnego także sieci telekomunikacyjnej w zakresie, w jakim służy ona realizacji usługi kluczowej lub cyfrowej. Sieć telekomunikacyjna stanowi integralną część tego systemu

informacyjnego, bez niej bowiem nie byłaby możliwa realizacja tej usługi. Przyjęte definicje oznaczają również, że ustawa obejmuje swoim zakresem zarówno systemy informatyczne (IT – ang. Information Technology) jak również systemy sterowania przemysłowego (OT – ang. Operational Technology), a także infrastrukturę wirtualną (informacyjną), np. zbiory informacji z baz danych. Przesłanką do objęcia wymaganiami z zakresu cyberbezpieczeństwa mogą być ustalone rozporządzeniem Rady Ministrów progi istotności incydentu we wspomnianych systemach informacyjnych – patrz rozdział 2.

Przyjęto również definicję **obsługi incydentu,** jako zespołu czynności umożliwiających wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych oraz ograniczenie skutków incydentu. **Zarządzania incydentem** jest terminem szerszym i obejmuje, poza obsługą, również wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowanie wniosków z obsługi incydentu.

Ustawa wprowadza również pojęcie **podatności**, czyli właściwości systemu informacyjnego, która może być wykorzystana przez **zagrożenie cyberbezpieczeństwa**, które z kolei zostało natomiast zdefiniowane jako potencjalna przyczyna incydentu. Przyjmując powyższe definicje, opierano się na istniejących normach i standardach bezpieczeństwa teleinformatycznego.

W art. 3 zostały określone cele krajowego systemu cyberbezpieczeństwa, którymi będą niezakłócone świadczenie usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

Artykuł 4 wskazuje podmioty, które obejmuje krajowy system cyberbezpieczeństwa, a więc podmioty zobowiązane, podmioty realizujące techniczne, organizacyjne i administracyjno-regulacyjne zadania w systemie, jednostki sektora finansów publicznych. System będzie zatem obejmować m.in. operatorów usług kluczowych, dostawców usług cyfrowych, zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, pojedynczy punkt kontaktowy do spraw cyberbezpieczeństwa, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa i Kolegium do Spraw

Cyberbezpieczeństwa, instytuty badawcze, a także jednostki sektora finansów publicznych objęte zakresem ustawy.

W przepisach szczegółowych projektu zostały natomiast opisane uprawnienia i obowiązki ww. podmiotów, jak również zakres przypisanej im odpowiedzialności. I tak w rozdziale 6 zostały wskazane uprawnienia i wymagane kompetencje CSIRT, pełniących najważniejsze funkcje techniczne w systemie, obejmujące m.in. koordynację i obsługę poważnych, istotnych i krytycznych incydentów. Opisane zostały również sposoby realizacji współpracy z operatorami usług kluczowych, dostawcami usług cyfrowych, podmiotami publicznymi i sektorowymi zespołami cyberbezpieczeństwa. Także w przepisach szczegółowych opisane zostały role o charakterze administracyjno-regulacyjnym, role oraz zależności, które powstają między organem właściwym ds. cyberbezpieczeństwa a operatorem usługi kluczowej, od decyzji administracyjnej o uznaniu za operatora, przez audyty i monitorowanie stosowania przepisów, po przepisy o charakterze władczym, czyli kontrole i administracyjne kary pieniężne. W rozdziałach dotyczących Pełnomocnika Rządu ds. Cyberbezpieczeństwa oraz Pojedynczego Punktu Kontaktowego zostały natomiast opisane zależności jakie są związane z zarządzaniem cyberbezpieczeństwem w skali kraju (np. ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych) oraz na potrzeby współpracy międzynarodowej (np. wymiana informacji na temat zgłoszeń incydentów dotyczących innych państw członkowskich UE).

Jeżeli chodzi o jednostki sektora finansów publicznych, zostaną one zawężone do tych określonych w art. 9 pkt 1–6, 8–9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (dalej „ustawa o finansach publicznych). Są to trzy grupy podmiotów, które w opinii projektodawcy wymagają szczególnej uwagi w zakresie uregulowania kwestii związanych z cyberbezpieczeństwem. Do pierwszej grupy zaliczono organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały, jednostki samorządu terytorialnego oraz ich związki (w tym metropolitarne), jednostki budżetowe i samorządowe zakłady budżetowe, agencje wykonawcze oraz instytucje gospodarki budżetowej. Do drugiej grupy należą ZUS (w tym FUS) i KRUS (w tym jej fundusze). Do trzeciej grupy należą uczelnie publiczne oraz PAN i jego jednostki organizacyjne.

Ponadto uwzględniono konieczność objęcia ustawą niektórych podmiotów z art. 9 pkt 14 ustawy o finansach publicznych (tzw. inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych). Należą do nich: Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej. Ustawą objęte również będą spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. ustawy o gospodarce komunalnej[33)].

Rozdział 2: Identyfikacja i rejestracja operatorów usług kluczowych i Załącznik do ustawy

Artykuł 5 wprowadza do polskiego porządku prawnego nową kategorię podmiotów, czyli operatora usługi kluczowej.

Projektodawca wzoruje się na definicji z dyrektywy 2016/1148 i będzie nim podmiot **spełniający łącznie następujące przesłanki**:

- będzie jednym z podmiotów wymienionych w załączniku do ustawy,
- będzie świadczył usługę kluczową wymienioną w wykazie usług kluczowych,
- świadczenie tej usługi będzie zależeć od systemów informacyjnych,
- incydent miałby istotny skutek zakłócający dla jej świadczenia.

Wobec takiego podmiotu organ właściwy będzie mógł wydać **decyzję administracyjną o uznaniu za operatora usługi kluczowej**.

Wykaz usług kluczowych i progi istotności skutku zakłócającego dla świadczenia tych usług będą określone rozporządzeniem Rady Ministrów (art. 6 projektu). Projektodawca przewidział również tryb decyzji administracyjnych w przypadku zaprzestania spełniania przez podmiot warunków dla operatora usługi kluczowej (art. 5 ust. 6).

Stroną praw i obowiązków określonych w projekcie ustawy jest operator usługi kluczowej, niezależnie od tego, czy powierzył część, czy nawet całość czynności dotyczących świadczenia usługi kluczowej podmiotowi prywatnemu np. generalnemu wykonawcy, a ten dalszym podwykonawcom. Wszelkie kwestie rozkładu

33) Dz. U. z 2017 r. poz. 827.

odpowiedzialności między poszczególnymi podmiotami powinny być uregulowane wewnętrznie przez te podmioty (np. w drodze umów o świadczenie usług).

Artykuł 7 projektowanej ustawy zobowiązuje ministra właściwego do spraw informatyzacji do prowadzenia wykazu operatorów usług kluczowych. Wykaz ten zostanie utworzony z uwzględnieniem podziału na sektory, podsektory i rodzaje podmiotów, który wprowadza ustawa. Wpis do wykazu lub wykreślenie z niego ma charakter deklaratoryjny i będzie czynnością materialno-techniczną, realizowaną w oparciu o decyzje administracyjne organów właściwych, w zakresie identyfikacji operatorów usług kluczowych we właściwych sektorach. Przepis ten określa również tryb udostępniania informacji i katalog podmiotów, którym będą udostępniane informacje z wykazu.

Podstawą ustawową procedury administracyjnej związanej z wyłanianiem operatorów usług kluczowych jest załącznik nr 1 do ustawy, zawierający kategorie podmiotów z danego sektora bądź podsektora, z których mógłby zostać zidentyfikowany operator usługi kluczowej. Dyrektywa 2016/1148 wyznacza poziom harmonizacji minimalnej i dopuszcza możliwość ustanowienia szerszego katalogu grupy podmiotów, z których mógłby zostać wyłoniony w procedurze administracyjnej operator usługi kluczowej. Projektodawca, w wyniku konsultacji z potencjalnymi organami właściwymi, objął zakresem ustawy wszystkie kategorie podmiotów wymienionych w załączniku II do dyrektywy 2016/1148, i dodatkowo objął inne kategorie podmiotów, które nie zostały ujęte we wspomnianym załączniku nr 1 (omówiono oddzielnie). Należy przy tym dodać, że wskazanie danej kategorii podmiotu ma służyć wskazaniu potencjalnych podmiotów, wobec których może zostać wydana obecnie bądź w przyszłości decyzja o uznaniu za operatora usługi kluczowej, ale nie oznacza to automatyzmu uznania takiego podmiotu za operatora usługi kluczowej.

2.1 Sektor energii

a) podsektor energii elektrycznej: załącznik do projektu ustawy, zgodnie z przepisami dyrektywy 2016/1148, obejmuje przedsiębiorstwa energetyczne, operatorów systemu dystrybucyjnego, operatorów systemu przesyłowego. Projekt ustawy odwołuje się tutaj do regulacji zawartych w art. 3 pkt. 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo

energetyczne[34)] (dalej „ustawa – Prawo energetyczne), gdzie zdefiniowano przedsiębiorstwo energetyczne jako podmiot prowadzący działalność gospodarczą w zakresie wytwarzania, przetwarzania, magazynowania, przesyłania, dystrybucji energii lub obrotu nimi albo przesyłania dwutlenku węgla oraz regulacji w art. 3 pkt 24 i 25, gdzie odpowiednio uregulowano operatora systemu przesyłowego i operatora systemu dystrybucyjnego;

b) podsektor ropy naftowej: regulacją będą objęci operatorzy ropociągów oraz operatorzy instalacji służących do produkcji, rafinacji, przetwarzania, magazynowania i przesyłu ropy naftowej. Projekt podobnie jak w przypadku energii elektrycznej odwołuje się do definicji przedsiębiorstwa energetycznego z art. 3 pkt 12 ustawy – Prawo energetyczne, które obejmuje podmioty prowadzące działalność gospodarczą w zakresie wytwarzania, przetwarzania, magazynowania, przeładunku, przesyłania, dystrybucji paliw ciekłych, a więc również ropy naftowej;

c) podsektor gazu: regulacją mogą zostać objęte: przedsiębiorstwa dostarczające gaz, operatorzy systemu przesyłowego, operatorzy systemu dystrybucyjnego, operatorzy systemu magazynowania, operatorzy systemu LNG, przedsiębiorstwa gazowe, operatorzy instalacji służących do rafinacji i przetwarzania gazu ziemnego. W polskim systemie prawnym regulacje dotyczące omawianego sektora znajdują się w wymienionej wcześniej ustawie – Prawo energetyczne. Załącznik odwołuje się zarówno do art. 3 pkt 12 i art. 3 pkt 24–27 ustawy – Prawo energetyczne.

Ponadto oraz ze względu na istotność usług i ich zależność od systemów informacyjnych, w porozumieniu z ministrem właściwym do spraw energii ustalono następujące podsektory lub kategorie podmiotów, wykraczające poza zakres podmiotowy dyrektywy 2016/1148, z których będą mogli być wyłaniani operatorzy usług kluczowych,

d) podsektor wydobywania kopalin: podsektor nie jest zdefiniowany w dyrektywie 2016/1148, a jego obecność jest wymagana dla zachowania ciągłości łańcucha dostaw dla sektora energii. Podsektor ten obejmuje podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej, węgla kamiennego, węgla

[34)] Dz. U. z 2018 r. poz. 755, 650, 685 i 771.

brunatnego i pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze[35)];

e) podsektor ciepło: podsektor nie jest zdefiniowany w dyrektywie 2016/1148. Podsektor ten obejmuje przedsiębiorstwa energetyczne posiadające koncesje na wykonywanie działalności gospodarczej w zakresie wytwarzania, obrotu, przesyłu, dystrybucji ciepłem, zdefiniowane w ustawie – Prawo energetyczne,

f) podsektor dostaw i usług dla sektora energii jak i jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane oraz podmioty prowadzące działalność gospodarczą w zakresie dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii,

g) katalog podmiotów ma obejmować ponadto podmioty prowadzące działalność gospodarczą w zakresie świadczenia usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną, przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej, prowadzące działalność gospodarczą w zakresie przeładunku i obrotu paliwami ciekłymi, w tym ropy naftowej oraz podmiotów prowadzących działalność w zakresie wytwarzania paliw syntetycznych.

2.2 Sektor transportu

W sektorze transportu w załączniku zostały wskazane wyłącznie kategorie podmiotów wskazane w załączniku nr 2 do dyrektywy 2016/1148:

a) podsektor transportu lotniczego: załącznik do ustawy wskazuje na przewoźników lotniczych, zarządzających lotniskiem, jednostki obsługujące urządzenia pomocnicze znajdujące się w portach lotniczych, operatorzy zarządzający ruchem lotniczym zapewniający służbę kontroli ruchu lotniczego (ATC). Załącznik odwołuje się zatem do rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego[36)], a także odpowiednich przepisów ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze[37)];

b) podsektor transportu kolejowego; regulacja, zgodnie z wytycznymi dyrektywy 2016/1148, ma obejmować zarządców infrastruktury, przedsiębiorstwa kolejowe

[35)] Dz. U. z 2017 r. poz. 2126 oraz z 2018 r. poz. 650 i 723.
[36)] Dz. Urz. UE L 97 z 09.04.2008, str. 72.
[37)] Dz. U. z 2017 r. poz. 959 i 1089 oraz z 2018 r. poz. 138 i 650.

i operatorów obiektów infrastruktury usługowej. Sektor ten w polskim systemie prawnym regulowany jest ustawą o transporcie kolejowym[38)]. Wszystkie wymienione pojęcia zostały zdefiniowane w załączniku do ustawy;

c) podsektor transportu wodnego ma obejmować: armatorów w transporcie morskim pasażerów i towarów, armatorów śródlądowego transportu pasażerów i towarów, podmioty zarządzające portami, podmioty zarządzające obiektami portowymi, podmioty prowadzące na terenie portu działalność wspomagającą transport morski oraz operatorów systemów ruchu statków. Załącznik odwołuje się do definicji rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych[39)], armatorów żeglugi śródlądowej – ustawa z dnia 21 grudnia 2000 r. o żegludze śródlądowej[40)], ustawa z dnia 20 grudnia 1996 r. o portach i przystaniach morskich[41)], ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim[42)];

d) podsektor transportu drogowego; objęte regulacją mają być organy administracji drogowej oraz operatorzy inteligentnych systemów transportowych. Sektor transportu drogowego reguluje w polskim systemie prawnym ustawa o drogach publicznych[43)].

2.3 Sektor bankowości i infrastruktury rynków finansowych

Zgodnie z dyspozycjami dyrektywy 2016/1148 regulacja krajowa ma w załączniku obejmować instytucje kredytowe objęte rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 575/2013 w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych.[44)] W polskim systemie prawa regulacje dotyczące instytucji kredytowych znajdują się w ustawie – Prawo bankowe i w ustawie z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych[45)]. Załącznik odwołuje się tutaj do art. 4 ust. 1 pkt 17 ustawy – Prawo bankowe. Dodatkowo załącznik odwołuje się do definicji banku krajowego (art. 4 ust. 1 pkt 1 Prawa bankowego), oddziału banku zagranicznego (art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe), oddziału instytucji kredytowej (art. 4 ust. 1 pkt 18 ustawy – Prawo

[38)] Dz. U. z 2017 r. poz. 1727 i 2361 oraz z 2018 r. poz. 650.
[39)] Dz. Urz. UE L 129 z 29.04.2004, str. 6.
[40)] Dz. U. z 2017 r. poz. 2128.
[41)] Dz. U. z 2017 r. poz. 1933.
[42)] Dz. U. z 2018 r. poz. 181.
[43)] Dz. U. z 2017 r. poz. 2222.
[44)] Dz. Urz. UE L 176 z 27.06. 2013, str. 1.
[45)] Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 723 i 771.

bankowe). Zakresem załącznika niniejszej ustawy będzie objęty również sektor spółdzielczych kas oszczędnościowo-kredytowych, objęty ustawą o spółdzielczych kasach oszczędnościowo-kredytowych.

W zakresie infrastruktury rynków finansowych załącznik do ustawy zgodnie z dyrektywą 2016/1148 odwołuje się do operatorów systemu obrotu i kontrahentów centralnych. Omawiany sektor jest regulowany w polskim systemie prawa przez ustawę o obrocie instrumentami finansowymi. Załącznik do ustawy odwołuje się tutaj do podmiotu prowadzącego rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy o obrocie instrumentami finansowymi (giełdy towarowej lub pieniężnej), obejmuje podmiot wskazany w art. 3 pkt. 49 ustawy o obrocie instrumentami finansowymi, czyli Krajową Izbę Rozliczeniową S.A., podmiot, o którym mowa w art. 48 ust. 7 ustawy o obrocie instrumentami finansowymi, czyli kontrahent centralny „CCP".

2.4 Sektor ochrona zdrowia

Zgodnie z wymogami dyrektywy 2016/1148 w załączniku zostały wskazane podmioty lecznicze, o których mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej[46)]. Dodatkowo ze względu na istotność usług i ich zależność od systemów informacyjnych, w porozumieniu z ministrem właściwym do spraw zdrowia ustalono dodatkowe kategorie podmiotów, wykraczające poza zakres podmiotowy dyrektywy 2016/1148, z których będą mogli być wyłaniani operatorzy usług kluczowych. Będzie to jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia, Narodowy Fundusz Zdrowia (NFZ), działy farmacji szpitalnej i apteki, hurtownie farmaceutyczne, przedsiębiorcy, którzy wnioskują lub uzyskali pozwolenie na dopuszczenie do obrotu produktu leczniczego, wytwórcy, importerzy produktu leczniczego/substancji czynnej i dystrybutorzy substancji czynnej oraz importerzy równolegli.

2.5 Sektor zaopatrzenia w wodę pitną i jej dystrybucja

Regulacja w załączniku ma obejmować dostawców i dystrybutorów „wody przeznaczonej do spożycia przez ludzi". Sektor ten uregulowany jest w polskim systemie prawnym w ustawie z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków[47)]. W ustawie tej znajduje się definicja

[46)] Dz. U. z 2018 r. poz. 138 i 1650.
[47)] Dz. U. z 2017 r. poz. 328, 1566 i 2180 oraz z 2018 r. poz. 650.

przedsiębiorstwa wodno-kanalizacyjnego, który może zostać uznany za operatora usługi kluczowej.

2.6 Sektor infrastruktury cyfrowej

Regulacja w załączniku ma obejmować podmioty prowadzące punkty wymiany ruchu internetowego (IXP), stanowiące obiekt sieciowy, który umożliwia połączenie międzysystemowe między więcej niż dwoma niezależnymi systemami autonomicznymi, podmioty świadczące usługi autorytatywnych serwerów DNS, podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).

Rozdział 3: Obowiązki operatorów usług kluczowych

W artykule 8 określone zostały obowiązki operatorów usług kluczowych w zakresie stosowania zabezpieczeń systemów informacyjnych służących do świadczenia usług kluczowych, szacowania i zarządzania ryzykiem oraz realizowania procedur dotyczących zarządzania incydentem. Operatorzy są odpowiedzialni za zapewnienie bezpieczeństwa świadczonych usług kluczowych oraz ciągłości ich świadczenia. Ich głównym obowiązkiem jest wdrożenie systemu zarządzania bezpieczeństwem, a w pkt 2 wskazano minimalny zakres, jaki ma on obejmować.

Na system ten składają się zabezpieczenia dotyczące bezpieczeństwa fizycznego, zarządzania ciągłością działania, obsługi i zarządzania incydentem, zarządzania podatnościami, objęcia systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym oraz stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Artykuł 9 zawiera natomiast zamknięty katalog obowiązków o charakterze organizacyjnym, które musi realizować operator usług kluczowych. Projektodawca wymienia wśród nich wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa oraz zapewnienie użytkownikom usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczeń.

Powołanie osoby odpowiedzialnej za utrzymywanie kontaktów pozwoli na sformalizowanie i wzmocnienie relacji między poszczególnymi podmiotami. Przez

powołanie tego typu „łącznika” projektodawca ma zamiar zachęcić uczestników należących do systemu do współpracy nie tylko z Ministerstwem Cyfryzacji i CSIRT, ale także między sobą, w ramach wspólnych przedsięwzięć mających na celu zwiększenie bezpieczeństwa świadczonych usług.

W zakresie drugiego obowiązku trzeba wspomnieć o budowaniu świadomości użytkowników. Powszechna świadomość o występujących w cyberprzestrzeni zagrożeniach oraz skutecznych metodach zabezpieczenia się przed tego rodzaju zagrożeniami ma kluczowe znaczenie dla funkcjonowania całego systemu cyberbezpieczeństwa. Mimo ogromnego postępu technologicznego i dostępnych narzędzi to przede wszystkim czynnik ludzki stanowi najważniejsze ogniwo bezpieczeństwa w cyberprzestrzeni.

Często użytkownicy nie są świadomi lub nie umieją rozpoznać zagrożenia, nie zdając sobie sprawy z tego, jakie może ono przynieść skutki. Relacja między użytkownikiem a system IT jest zatem kluczowym aspektem bezpieczeństwa informatycznego. Stosowanie zasad higieny informacyjnej pozwoli na ochronę zarówno systemu operatora usługi kluczowej, samej usługi, jak również na bezpieczeństwo danych użytkownika danej usługi. Obowiązek informowania użytkownika usługi kluczowej o zagrożeniach i stosowaniu zabezpieczeń ma na celu minimalizowanie negatywnych skutków, jakie może ponieść z tytułu złego użytkowania systemu operator usługi kluczowej.

Ze względu na powszechny dostęp do rejestrów przedsiębiorców, zdjęto z operatorów usług kluczowych obowiązek aktualizacji danych w wykazie. Ciężar aktualizacji tych danych będzie spoczywał na organach właściwych, które będą badały sytuację w sektorze. Jednak ze względu na fakt, że niektóre informacje nie są dostępne w publicznych rejestrach (chodzi o informację, w jakich państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej oraz datę zakończenia świadczenia usługi kluczowej), nałożono na operatora obowiązek aktualizacji tych danych.

Artykuł 10 precyzuje obowiązki operatorów usług kluczowych związane z opracowywaniem i ustanowieniem nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. Zawiera upoważnienie do wydania przez Radę Ministrów

rozporządzenia określającego rodzaje tworzonej dokumentacji. Przepis zawiera wyłączenie w zakresie realizacji tego obowiązku przez właścicieli, posiadaczy samoistnych lub zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym, którzy realizują obowiązki tego typu na podstawie tej ustawy. Rozwiązanie powyższe ogranicza tym samym obowiązki administracyjne tworzenia dokumentacji dotyczącej cyberbezpieczeństwa, o ile dany operator usług kluczowych został już objęty obowiązkami, o których mowa w przepisach o zarządzaniu kryzysowym i ma zatwierdzony plan ochrony infrastruktury krytycznej.

Na operatorów usług kluczowych zostaną nałożone obowiązki związane ze zgłaszaniem i obsługą incydentu (art. 11). Operatorzy będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. Przepisy nakładają obowiązki zgłaszania incydentów poważnych niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia. Przewidziana jest elektroniczna forma zgłaszania incydentu, która ma zostać określona przez CSIRT (art. 31).

Podstawowym założeniem projektodawcy jest fakt, jak najszybszego zawiadomienia właściwego CSIRT. Samo zgłoszenie miałoby charakter inicjujący dalsze postępowanie z obsługą incydentu oraz ma ograniczyć jego potencjalne skutki wobec innych podmiotów tworzących krajowy system cyberbezpieczeństwa. W procesie obsługi incydentu operator będzie zobowiązany do współpracy z odpowiednim CSIRT oraz zapewniać, w razie potrzeby, dostęp do informacji o rejestrowanych incydentach, a także informować właściwy CSIRT o usunięciu podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu.

W projektowanych przepisach znajduje się upoważnienie ustawowe do określenia progów uznania incydentu za poważny w sektorach określonych w załączniku do ustawy. Uzupełnieniem pakietu przepisów dotyczących notyfikacji incydentów jest art. 12, zawierający określenie zakresu danych zawartych w zgłoszeniu. Zgłoszenie będzie zawierało dane znane operatorowi w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. W zgłoszeniu operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym

stanowiące tajemnicę przedsiębiorstwa, natomiast CSIRT bądź zespół sektorowy może się zwrócić do operatora o uzupełnienie zgłoszenia dodatkowe o informacje w zakresie niezbędnym do obsługi incydentu.

Systemy wykorzystywane do przekazywania będą spełniać odpowiednie wymogi bezpieczeństwa (istotność sposobów zabezpieczenia tajemnicy), gdyż będą w nich przetwarzane dane istotne dla danego podmiotu, a nawet mogą zawierać informacje prawnie chronione. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa, operator usługi kluczowej przekazuje równolegle zgłoszenie do sektorowego zespołu cyberbezpieczeństwa oraz współdziała na poziomie sektorowym lub podsektorowym z tym zespołem.

Zgodnie z art. 13 możliwe jest informowanie CSIRT o innych kwestiach związanych z cyberbezpieczeństwem, np. o zagrożeniach, o podatnościach, wykorzystywanych technologiach. Jest dodatkowy, dobrowolny mechanizm, który pomoże wzmocnić wymianę informacji między podmiotami krajowego systemu cyberbezpieczeństwa. Daje to też możliwość (ale nie obowiązek) dla CSIRT, na mocy art. 32 ust. 4, aby mogły one przekazywać operatorom usług kluczowych informacje o podatnościach na incydenty i sposobie usunięcia podatności w wykorzystywanych technologiach.

Projektodawca dopuszcza możliwość budowy przez podmioty zobowiązane wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, bądź outsourcingu usług z zakresu cyberbezpieczeństwa. Celem zapewnienia świadczenia przez podmioty świadczące usług z zakresu cyberbezpieczeństwa na rzecz operatorów usług kluczowych bądź dostawców usług cyfrowych na odpowiednim poziomie ustawa określa wymagania dla takich podmiotów. Zakłada się, że wymienione podmioty powinny spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej, dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi, stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów. Sposób realizacji tych wymagań zostanie określony w rozporządzeniu ministra właściwego do spraw informatyzacji. Przepisy umożliwią korzystanie przez podmioty świadczące usługi z zakresu

cyberbezpieczeństwa z pomieszczeń udostępnionych przez operatora usług kluczowych, zabezpieczonych przed zagrożeniami fizycznymi i środowiskowymi. Środki bezpieczeństwa osobowego będą elementem polityki bezpieczeństwa informacji i dostosowane do charakteru informacji przetwarzanych przez podmiot świadczący usługi z zakresu cyberbezpieczeństwa. W przypadku przetwarzania informacji niejawnych zastosowanie będą miały przepisy ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych[48)].

Artykuł 15 określa zasady, tryb przeprowadzania i cele audytów bezpieczeństwa systemów informacyjnych przeprowadzanych przez operatorów usług kluczowych. Operatorzy usług kluczowych są zobowiązani do przeprowadzania audytów bezpieczeństwa systemów informacyjnych co najmniej raz na dwa lata. Audyt może być przeprowadzany w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych, a więc np. audyt systemu zarządzania bezpieczeństwem informacji i zarządzania ciągłością działania. Zamierzeniem projektodawcy jest zapewnienie pełnej wykonalności przepisów dotyczących audytów bezpieczeństwa systemów informacyjnych, jak również konkurencyjności rynku audytu, dlatego audyt będzie przeprowadzany przez akredytowaną jednostkę oceniającą zgodność, zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku[49)], audytorów posiadających stosowne certyfikaty, określonymi w rozporządzeniu ministra właściwego ds. informatyzacji i legitymującymi się odpowiednią praktyką w zakresie prowadzenia audytu bezpieczeństwa systemów informacyjnych. Projektodawca dopuszcza również, aby audyty były realizowane, w przypadku ich ustanowienia w danym sektorze lub podsektorze, przez sektorowe zespoły cyberbezpieczeństwa. Decyzja o wyborze formy audytu jest podejmowana samodzielnie przez operatora usług kluczowych. Obowiązek przeprowadzenia audytu przez operatora usługi kluczowej uważa się również za spełniony, w przypadku gdy u operatora został przeprowadzony audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie ustawy o informatyzacji. Z przeprowadzonego audytu audytor sporządza pisemne sprawozdanie, przekazywane audytowanemu operatorowi usługi kluczowej. Konstrukcja przepisów umożliwia wykorzystanie jego wyników przez organy właściwe i dyrektora Rządowego Centrum Bezpieczeństwa.

[48)] Dz. U. z 2018 r. poz. 412 i 650.
[49)] Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650.

Art. 16 określa terminy realizacji obowiązków ustawowych przez podmioty uznane za operatorów usług kluczowych, które są liczone od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej. Termin sześciomiesięczny odnosi się do obowiązków z zakresu bezpieczeństwa fizycznego, zarządzania ciągłością działania, obsługi i zarządzania incydentem, zarządzania podatnościami, objęcia usług kluczowych systemem monitorowania w trybie ciągłym oraz stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację. Natomiast termin trzymiesięczny dotyczy prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu, zarządzania incydentem, wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zapewnienia użytkownikowi dostępu do wiedzy na temat zagrożeń cyberbezpieczeństwa i sposobów przeciwdziałania oraz powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. Projektodawca wskazał również, że pierwszy audyt przewidziany przepisami ustawy ma być przeprowadzony w terminie roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej.

Rozdział 4: Obowiązki dostawców usług cyfrowych

Wymaganiami z zakresu cyberbezpieczeństwa zostaną również objęci dostawcy usług cyfrowych, czyli osoby prawne albo jednostki organizacyjne nieposiadające osobowości prawnej, mające siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadczące usługi cyfrowe w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, wymienione w załączniku nr 2 do ustawy, czyli internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe.

Zgodnie z uzasadnieniem zawartym w motywie 49 dyrektywy 2016/1148, dostawcy usług cyfrowych powinni zapewnić poziom bezpieczeństwa współmierny do stopnia ryzyka, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług cyfrowych, ze względu na znaczenie tych usług dla działalności innych przedsiębiorców w Unii. Według prawodawcy unijnego, stopień ryzyka dla operatorów usług kluczowych jest wyższy niż dla dostawców usług cyfrowych, co uzasadnia mniejsze wymogi w zakresie bezpieczeństwa. Zgodnie z dyrektywą, pozostawiono dostawcom

usług cyfrowych swobodę podejmowania środków, które uznają za odpowiednie do zarządzania ryzykami. Jednocześnie dyrektywa ograniczyła wpływ państw członkowskich na regulację działalności dostawców usług cyfrowych ze względu na transgraniczny charakter tych usług. Zharmonizowane podejście na poziomie Unii mają zapewnić akty wykonawcze, w tym rozporządzenie wykonawcze 2018/151, o którym będzie mowa poniżej.

Przepisy art. 17 formułują wymagania jakie muszą spełnić dostawcy usług cyfrowych w zakresie zabezpieczeń systemów informacyjnych służących do świadczenia usług cyfrowych. Artykuł 18 zawiera natomiast katalog obowiązków nakładanych na dostawców usług cyfrowych, związanych ze zgłaszaniem i obsługą incydentów istotnych i krytycznych oraz obowiązków dotyczących informowania operatora usług kluczowych o incydencie istotnym mającym wpływ na ciągłość świadczenia usługi kluczowej.

W art. 19 określone zostały elementy jakie powinno spełniać zgłoszenie incydentu istotnego. Podobnie jak w przypadku incydentu poważnego przepisy dotyczące incydentu istotnego zakładają, że zgłoszenie będzie zawierało dane znane dostawcy w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. W zgłoszeniu dostawca usługi cyfrowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, natomiast CSIRT NASK bądź CSIRT MON, będące jednocześnie CSIRT najwyższego poziomu dla dostawców usług cyfrowych mogą się zwrócić do dostawcy o uzupełnienie zgłoszenia o informacje w zakresie niezbędnym do realizacji zadań związanych z obsługą incydentu istotnego.

W zakresie stosowanych zabezpieczeń systemów informacyjnych oraz kryteriów klasyfikacji incydentów za istotne przepisy ustawy odwołują się do rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do

określenia, czy incydent ma istotny wpływ[50)]. Należy podkreślić, że rozporządzenie wykonawcze zawiera katalog szczegółowych wymagań służących tworzeniu zabezpieczeń systemów informacyjnych, dotyczących m.in. bezpieczeństwa fizycznego i środowiskowego, kontroli dostępu, procedur zgłaszania incydentów, zapewnienia ciągłości działania. Zawiera parametry określające, jakie incydenty z zakresu cyberbezpieczeństwa będą musiały być zgłaszane do CSIRT NASK.

Dostawcy usług cyfrowych mogą zlecić realizację zadań obejmujących zastosowanie zabezpieczeń systemów informacyjnych, zgłaszanie i obsługę incydentów podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa, jednak ze względu na ograniczenie możliwości regulacyjnych, projektodawca odstąpił od ujęcia tego w ustawie, pozostawiając pełną swobodę doboru środków dostawcy usług cyfrowych. Warto jednak pamiętać, że stroną praw i obowiązków określonych w projekcie ustawy pozostaje dostawca usługi cyfrowej, niezależnie od tego czy powierzył część czy nawet całość czynności dotyczących świadczenia usługi cyfrowej innemu podmiotowi, a ten dalszym podwykonawcom.

Rozdział 5: Obowiązki podmiotów publicznych

Przepisy rozdziału definiują obowiązki podmiotów publicznych objętych zakresem ustawy. Podmioty publiczne objęte wymogami z zakresu cyberbezpieczeństwa będą zobowiązane do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 21) oraz udostępniania wiedzy na temat zagrożeń cyberbezpieczeństwa oraz stosowania odpowiednich zabezpieczeń przed tymi zagrożeniami (art. 22 ust. 1 pkt 4). Obowiązek ten może być realizowany w różnorodny sposób, najczęściej przez umieszczanie na stronach internetowych informacji o zagrożeniach cyberbezpieczeństwa związanych z realizowanymi zadaniami publicznymi. Nie wiąże się to z obowiązkiem udzielania odpowiedzi na indywidualne zapytania, a już na pewno nie z udostępnianiem wrażliwych informacji o nadzorowanych podmiotach. Podmioty publiczne będą włączone do krajowego systemu cyberbezpieczeństwa dzięki ustanowionemu obowiązkowi zgłaszania incydentów w podmiocie publicznym, zarządzanie incydentem jak również w wypadku takiej potrzeby współpracę w jego obsłudze, a także incydentów krytycznych z zespołami CSIRT. Projektodawca tym samym zobowiązuje

[50)] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.026.01.0048.01.ENG&toc=OJ:L:2018: 026:TOC

podmiot publiczny do obsługi incydentu we własnym zakresie, pozostawiając mu swobodę w zakresie sposobu realizacji tych obowiązków. Proponowane rozwiązanie uwzględnia zatem istniejące już i ciągle rozbudowywane wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo w poszczególnych resortach. Incydenty w podmiotach publicznych będą obejmować takie incydenty, które powodują lub mogą spowodować obniżenie jakości lub przerwanie ciągłości zadania publicznego realizowanego przez podmioty publiczne. Projektodawca w przeciwieństwie do incydentów poważnych i istotnych nie wprowadza jednak progów na zgłoszenie incydentu w podmiocie publicznym. Natomiast podobnie, jak dla incydentów poważnych i krytycznych w zgłoszeniu incydentu w podmiocie publicznym podmiot ten oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. W przypadku podmiotów publicznych, wobec których została wydana decyzja o uznaniu za operatora usług kluczowych, miałyby zastosowanie przepisy rozdziału 3 ustawy definiujące m.in. obowiązki w zakresie wdrożenia systemu zarządzania bezpieczeństwem, opracowywania dokumentacji związanej z cyberbezpieczeństwem oraz przeprowadzania audytów bezpieczeństwa teleinformatycznego przez akredytowane jednostki certyfikujące. Taki podmiot publiczny pozostanie również stroną obowiązków bez względu na okoliczności czy usługa będzie w jego imieniu świadczona np. przez generalnego wykonawcę, podwykonawców.

Oprócz ogólnych wymogów z zakresu cyberbezpieczeństwa, którymi będą objęte wszystkie podmioty publiczne wchodzące w skład krajowego systemu cyberbezpieczeństwa, ustawa wyodrębnia również organy właściwe ds. cyberbezpieczeństwa, tzw. organy właściwe (szerzej Rozdział 8) realizujące dodatkowo funkcje z zakresu nadzoru i kontroli nad operatorami usług kluczowych bądź dostawcami usług cyfrowych.

Rozdział 6: Zadania CSIRT MON, CSIRT NASK, CSIRT GOV

Przepisy rozdziału ustanawiają strukturę CSIRT i porządkują kwestię zakresu odpowiedzialności poszczególnych CSIRT. Przyjęte rozwiązanie ma na celu jednoznaczne umocowanie w obowiązujących przepisach zasady współpracy takich CSIRT. Projektodawca zakłada, że z uwagi na wieloletnie doświadczenie oraz umiejscowienie w najwyższych strukturach, jak i wsparcie władz państwowych,

wszystkie trzy CSIRT spełniają wymogi określone w załączniku nr 1 do dyrektywy 2016/1148 określającym minimalne wymogi dla CSIRT. Umotywowane jest to faktem, że wszystkie trzy zespoły funkcjonują od lat (CERT Polska działa od 1996 r., MIL-CERT i CERT.GOV.PL od 2008 r.), posiadają międzynarodowe uznanie, są członkami międzynarodowych organizacji zrzeszających zespoły CERT (TF-CSIRT, Anti-Phishing Working Group, FIRST), uczestniczą w ćwiczeniach NATO i UE (Cyber Europe, Locked Shields, Cyber Coalition, CMX, CECSP). Bardzo wysoka ocena polskich zespołów jest potwierdzeniem profesjonalizmu i możliwości specjalistów ze wszystkich trzech instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne w Polsce. Uznano też, że CSIRT spełniają wymogi określone w art. 5 ust. 7 dyrektywy 2016/1148 i nie jest konieczna transpozycja tego przepisu przez akt prawny.

Zgodnie z art. 26 projektu CSIRT realizują zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniają koordynację obsługi poważnych incydentów. CSIRT monitorują zagrożenia i incydenty na poziomie krajowym, odpowiadają za szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa, przekazują podmiotom tworzącym krajowy system cyberbezpieczeństwa wczesne ostrzeżenia, informacje dotyczące incydentów i ryzyk, a także rekomendacje działań minimalizujących skutki incydentu. CSIRT dokonują klasyfikacji incydentów, jako krytyczne oraz koordynują ich obsługę, a w razie potrzeby zapewniają wsparcie w obsłudze incydentu poważnego i krytycznego operatorom usług kluczowych.

Należy podkreślić, że wsparcie w obsłudze lub obsługa poważnych incydentów przez CSIRT u operatorów usług kluczowych bądź posiadaczy samoistnych lub zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej lub incydentów istotnych u dostawców usług cyfrowych może odbywać się wyłącznie w uzasadnionych przypadkach i na wniosek tych podmiotów. Zasadą powinna być obsługa incydentu przez osoby związane z podmiotem bądź dla niego pracujące. Do rzetelnej obsługi incydentów niezbędna jest bowiem wiedza odnośnie do konkretnego zaatakowanego systemu, jego funkcjonalności oraz budowy, którą to wiedzę posiadają ich administratorzy. Celem zbudowania bieżącego obrazu sytuacyjnego w zakresie cyberbezpieczeństwa w skali państwa CSIRT w procesie koordynacji obsługi incydentów będą mogły wzajemnie przekazywać informacje techniczne dotyczące danego incydentu do pozostałych CSIRT. CSIRT będą ponadto odpowiedzialne za

przyjmowanie zgłoszeń o incydentach poważnych z innych państw, w tym państw członkowskich Unii Europejskiej i dokonywanie dystrybucji tych informacji do pozostałych CSIRT i do Pojedynczego Punktu Kontaktowego.

Zadania CSIRT uwzględniają przypisane poszczególnym CSIRT zakresy odpowiedzialności na potrzeby zarządzania cyberbezpieczeństwem państwa i zawierają katalogi obsługiwanych podmiotów tworzących krajowy system cyberbezpieczeństwa.

I tak do CSIRT MON (art. 26 ust. 5) będzie należeć obsługa incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa jest Minister Obrony Narodowej.

Do zadań CSIRT NASK będzie należeć przede wszystkim koordynacja obsługi incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, incydentów poważnych zgłaszanych przez operatorów usług kluczowych, którzy nie są objęci ustawą o zarządzaniu kryzysowym. Do zadań CSIRT NASK (art. 26 ust. 6) będzie również należeć obsługa incydentów zgłaszanych przez niektóre jednostki sektora finansów publicznych, jednostki podległe organom administracji rządowej i przez nie nadzorowane (z wyjątkiem jednostek podległych Prezesowi Rady Ministrów), oraz wybrane państwowe osoby prawne, utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych (Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej). Do NASK incydenty mogą też zgłaszać inne, niewymienione podmioty oraz osoby fizyczne. CISRT NASK będzie w tym zakresie pełnił rolę „CSIRT ostatniej szansy".

Do zadań CSIRT NASK należeć również będzie zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzącego działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r.

w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW[51)]. Działalność powyższa jest już obecnie prowadzona w ramach zespołu Dyżurnet.pl. Konieczne jest wskazanie, że głównym celem projektu jest implementacja dyrektywy 2016/1148, jednakże projekt buduje cały system cyberbezpieczeństwa w Polsce, a potrzeba uregulowania kwestii zapewnienia obsługi linii telefonicznej lub serwisu internetowego prowadzącego działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, jest istotnym elementem tego systemu. Zapewnienie bezpieczeństwa dla użytkowników Internetu to nie tylko zabezpieczenie przed incydentami, ale też przed nielegalnymi treściami. Warto w tym miejscu wskazać, że w porównywalnym okresie CERT Polska obsłużył 1926 incydentów, podczas gdy Dyżurnet.pl przeanalizował łącznie 11 759 zgłoszeń, z czego eksperci potwierdzili 3126 incydentów (dane z raportów CERT Polska oraz Dyżurnet.pl za 2016 r.). Nielegalne treści stanowią znaczną część incydentów zgłaszanych w Internecie i konieczne było ich uregulowanie w niniejszej ustawie, celem zapewnienia odpowiedniego zaplecza prawnego do ich obsługi.

Do zadań CSIRT GOV (art. 26 ust. 7) należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez najistotniejsze dla ciągłości państwa jednostki sektora finansów publicznych, jednostki podległe Prezesowi Rady Ministrów i przez niego nadzorowane (m.in. RCB, RZZK, KNF, UZP, URE, PGRP), Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz podmioty objęte ustawą o zarządzaniu kryzysowym, czyli podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne są wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ww. ustawy.

Do zadań CSIRT należeć będzie opracowanie do 30 maja każdego roku na potrzeby Pojedynczego Punktu Kontaktowego i wymiany informacji w ramach Unii Europejskiej zestawienia incydentów poważnych zgłaszanych przez operatorów usług kluczowych w poprzednim roku kalendarzowym (wszystkie CSIRT poziomu krajowego) oraz zestawienia incydentów istotnych zgłaszanych przez dostawców usług cyfrowych

[51)] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32011L0093

(CSIRT NASK). Mając na uwadze charakter cyberprzestrzeni przejawiający się między innymi brakiem występujących w niej granic, a przez to przenikaniem oddziaływań z jednego sektora gospodarki narodowej na inne, ustawa określa zasady wymiany informacji między poszczególnymi CSIRT i zobowiązuje do przyjęcia jednolitych procedur w zakresie obsługi incydentów i szacowania ryzyka. W związku z opisanym powyżej brakiem granic może powstać potrzeba zmiany zakresu odpowiedzialności podmiotowej poszczególnych CSIRT, co będzie możliwe przez zawieranie stosownych porozumień między zespołami CSIRT. W celu zachowania transparentności porozumienia będą publikowane w Dziennikach Urzędowych (art. 28 ust. 10).

Art. 27 zapewnia uspójnienie przepisów projektowanej ustawy z innymi aktami prawnymi rangi ustawowej, a w szczególności z przepisami ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz ustawy z dnia 9 czerwca 2016 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego[52)].

Przepisy art. 28 i art. 29 zobowiązują właściwe CSIRT do wystąpienia do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego lub istotnego do pojedynczego punktu kontaktowego w innym państwie członkowskim UE o incydentach zaistniałych na terytorium Polski, o ile incydenty te miałyby oddziaływanie w tych innych państwach członkowskich. Art. 30 umożliwia obsługiwanie przez CSIRT NASK innych incydentów niż pochodzące od podmiotów wymienionych w art. 28 ust. 6, zapewniając przy tym, że obsługa takich incydentów nie zaburzy realizacji przez ten CSIRT działań na rzecz podmiotów wymienionych w powyższym przepisie.

Regulowane przez obecną ustawę zespoły reagowania na incydenty istnieją i dbają o bezpieczeństwo sieci od wielu lat. Przedstawiany projekt ustawy reguluje i porządkuje ich obowiązki i uprawnienia. Wszystkie zespoły wypracowały przez lata skuteczne i działające zasady komunikacji ze swoimi partnerami, w tym tryb zgłaszania incydentów, zależnie od obszarów ich działania, uwzględniając specyfikę działania poszczególnych instytucji i najczęściej obsługiwanych typów incydentów. Z tego powodu w art. 31 znajduje się dyspozycja, która pozwala w sposób formalny na określenie przez CSIRT sposobów oraz warunków organizacyjnych i technicznych dokonywania zgłoszeń w postaci elektronicznej incydentów poważnych, istotnych,

[52)] Dz. U. z 2017 r. poz. 1978 i 2405 oraz z 2018 r. poz. 650.

incydentów w podmiotach publicznych, incydentów zgłaszanych przez osoby fizyczne. Przepis stanowi też podstawę do ustanowienia elektronicznej formy zgłoszeń informacji o zagrożeniach cyberbezpieczeństwa, podatnościach oraz stosowanych technologiach.

Art. 32 umożliwia uczestniczenie CSIRT w bezpośrednim usuwaniu skutków incydentów poważnych, incydentów istotnych lub incydentów krytycznych. W trakcie obsługi takich incydentów CSIRT może zwracać się do organu właściwego o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej do określonego zachowania, które doprowadzi do ograniczenia skutku incydentu i zapobiegnie mu w przyszłości.

Art. 33 wprowadza nową instytucję – badanie lub ocenę bezpieczeństwa stosowanego sprzętu lub oprogramowania. CSIRT mogą przeprowadzić badanie, które może być podstawą dla Pełnomocnika do wydania rekomendacji. Pełnomocnik, opierając się na technicznej i specjalistycznej wiedzy z poszczególnych CSIRT może, po zasięgnięciu opinii Kolegium, wydać rekomendację dot. stosowania określonego sprzętu lub oprogramowania przez podmioty krajowego systemu. Ze względu na dynamiczną sytuację na rynku dostawców, wydało się uzasadnionym wyznaczyć rekomendacje jako środek pozytywny (oprogramowanie będzie mogło być rekomendowane, a nie tylko uznawane za niepożądane) i dobrowolny (rekomendacje nie będą wiązać prywatnych podmiotów). Będzie to dodatkowy element budujący świadomość użytkowników instytucjonalnych i wspierający bezpieczne korzystanie ze sprzętu i oprogramowania.

Przepis art. 34 zobowiązuje CSIRT, operatorów usług kluczowych i dostawców usług cyfrowych do współpracy z organami ścigania, a przepis ust. 2 tego artykułu zobowiązuje ww. podmioty do współpracy z organem właściwym w sprawach ochrony danych osobowych, o ile w trakcie incydentu naruszone zostały przepisy w zakresie ochrony danych osobowych.

Art. 35 określa sposób wymiany informacji między CSIRT i Rządowym Centrum Bezpieczeństwa o incydencie krytycznym. CSIRT może wystąpić z rekomendacją zwołania Rządowego Zespołu Zarządzania Kryzysowego. Przepis umożliwia wymianę informacji między CSIRT w sytuacji, gdy incydent lub zagrożenie może dotyczyć podmiotów znajdujących się w zakresie kompetencji różnych CSIRT poziomu krajowego.

Przepisy art. 36 umożliwiają skuteczną koordynację działań poszczególnych CSIRT w przypadku obsługi incydentów krytycznych zgłoszonych przez CSIRT. Koordynację

zapewnia się przez powołanie Zespołu do spraw Incydentów Krytycznych. Zespół ten jest pomyślany jako organ pomocniczy służący organizacyjno-technicznej obsłudze incydentu krytycznego, a nie organ decyzyjny o charakterze strategiczno-politycznym. Zespół do spraw Incydentów Krytycznych w szczególności może rekomendować zwołanie Rządowego Zespołu Zarządzania Kryzysowego lub rekomendować Szefowi ABW wnioskowanie o wprowadzenie stopni alarmowania CRP. Istotnym rozwiązaniem praktycznym jest wskazanie na konieczność wyłonienia w drodze konsensusu jednego z CSIRT odpowiedzialnego za koordynację obsługi incydentu, w przypadku gdy incydent dotyka podmiotów znajdujących się w kompetencji różnych CSIRT. Przepis określa także, że incydent o rozległym oddziaływaniu jest przesłanką obligatoryjnego zwołania posiedzenia Rządowego Zespołu Zarządzania Kryzysowego.

Rozdział 7: Zasady udostępniania informacji i przetwarzania danych osobowych

W rozdziale tym zostały wyodrębnione zasady udostępniania informacji i przetwarzania danych osobowych w krajowym systemie cyberbezpieczeństwa. W kwestii udostępniania informacji projekt ustawy wprowadza zasadę, że informacje o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentu, ze względu na bezpieczeństwo państwa, a także mając na uwadze ochronę tajemnic prawnie chronionych operatorów usług kluczowych i dostawców usług cyfrowych, są wyłączone z reżimu ustawy o dostępie do informacji publicznej. W celu zapobiegania incydentom albo dla zapewnienia obsługi trwającego incydentu CSIRT mogą, po konsultacji ze zgłaszającym operatorem usługi kluczowej, opublikować na stronie podmiotowej BIP odpowiednio Ministra Obrony Narodowej, NASK – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o poszczególnych incydentach poważnych (art. 37 ust. 3). Ponadto CSIRT NASK może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, opublikować na stronie podmiotowej BIP NASK – Państwowego Instytutu Badawczego informacje o poszczególnych incydentach istotnych lub wystąpić do organu właściwego dla dostawców usług cyfrowych aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym (art. 37 ust. 4). Projektodawca przewidział zakaz udostępniania informacji przetwarzanych na podstawie ustawy jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego

w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywanie i ściganie.

W związku z wejściem w życie w maju 2018 r. rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej rozporządzenie 2016/679), projektodawca uwzględnił zawarte w ww. rozporządzeniu wymogi względem podmiotów objętych krajowym systemem cyberbezpieczeństwa, w tym zwłaszcza dotyczące przetwarzania danych przez CSIRT i sektorowe zespoły cyberbezpieczeństwa w związku z wsparciem i koordynacją obsługi incydentu. Minister właściwy do spraw informatyzacji, Dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, o którym mowa w art. 60 projektu, oraz organy właściwe będą mogły przetwarzać dane w związku z realizowaniem funkcji regulacyjnych i kontrolnych w węższym niż CSIRT zakresie. Odrębna regulacja została przewidziana dla Agencji Bezpieczeństwa Wewnętrznego, która na mocy art. 6 pkt 2 projektu ustawy o ochronie danych osobowych, została wyłączona spod stosowania przepisów implementowanego rozporządzenia 2016/679. Wobec powyższego CSIRT GOV, jako integralna część Agencji, otrzymuje podstawę do przetwarzania danych osobowych, jednak pozostałe uprawnienia Agencji do przetwarzania danych są opisane w ustawie o Agencji.

Operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty publiczne, podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz niewymienione wprost w ustawie, ale też istniejące: zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawcy sieci i usług łączności elektronicznej oraz dostawcy technologii i usług w zakresie bezpieczeństwa oraz inne podmioty (także publiczne) mają prawo do przetwarzania danych osobowych w zakresie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych przez te sieci i systemy przez organy publiczne, gdyż w rozumieniu rozporządzenia 2016/679 jest to prawnie uzasadniony interes administratora, którego sprawa dotyczy. Dalej rozporządzenie wskazuje, że może to obejmować zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi”,

a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej[53)].

Głównym zadaniem CSIRT nie jest zbieranie i przetwarzanie danych osobowych – jest to działalność uboczna, wynikająca z innych zadań. Podczas wsparcia koordynacji obsługi bądź działalności analitycznej, CSIRT mogą natrafić na dane, które co do zasady danymi osobowymi nie są, jednak w wyniku odpowiedniej korelacji posiadanych informacji, mogą się nimi stać i posłużyć np. do identyfikacji sprawcy incydentu. Danymi osobowymi, które mogą wystąpić podczas obsługi incydentu, mogą być m.in. zawartość ruchu sieciowego, dane podane podczas zgłoszenia incydentu, bazy danych uzyskane w czasie czynności informatyki śledczej, czy też logi i dzienniki zdarzeń (art. 39). Z uwagi na specyfikę działania CSIRT nie jest możliwe określenie katalogu zamkniętego przetwarzanych danych.

Obsługa incydentów może wiązać się z pewnymi zagrożeniami dla prywatności. Z tego powodu zostały ustalone wymogi bezpieczeństwa dla CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. Podmioty te będą także zobowiązane do zachowania tajemnicy oraz ogranicza się okres retencji przez nie danych (dane będą usuwane, kiedy nie są niezbędne do obsługi incydentu oraz po upływie pięciu lat od zakończenia obsługi incydentu, w związku z którym zostały uzyskane). W tym miejscu podkreślenia wymaga, że przetwarzanie danych osobowych w zakresie związanym z bezpieczeństwem narodowym nie podlega regulacjom rozporządzenia 2016/679, ze względu na motyw 16 i art. 2 ust. 2 lit. a rozporządzenia.

Projektując przedstawione rozwiązania, starano się zapewnić proporcjonalność i niezbędność w zakresie przetwarzanych danych. Do CSIRT będą przekazywane tylko dane dotyczące incydentów istotnych, poważnych i krytycznych, zatem tych o formie kwalifikowanej, istotne ze względu na bezpieczeństwo więcej niż bezpośrednio zainteresowanego podmiotu. Stosowana jest zasada, że to przede wszystkim podmiot obsługuje incydenty, które u niego wystąpiły, i w związku z tym przetwarza dane osobowe w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji oraz bezpieczeństwa związanych z nimi usług

[53)] Motyw 49 rozporządzenia 2016/679.

oferowanych lub udostępnianych przez te sieci i systemy (por. motyw 49 rozporządzenia 2016/679).

Warto też w tym miejscu wskazać, że analitycy bezpieczeństwa nie interesują się danymi osobowymi *per se*, ale mogą być one elementem innych przetwarzanych danych, zwłaszcza w świetle szerokiego rozumienia tego, czym są dane osobowe. Dane są przetwarzane w celu ich ochrony, a nie dalszego wykorzystania w innym celu. Przykładem może być próba identyfikacji urządzeń wchodzących w skład dużych sieci botnet. Do ich skutecznego zwalczania konieczna jest identyfikacja ich adresów IP i obserwowanie anomalii w ruchu sieciowym[54)], jednak dane te nie są wykorzystywane w innych celach. Są jednakże niezbędne, aby powstrzymywać chociażby ataki DDoS, które mogą przerwać ciągłość świadczenia różnych usług. W tym i podobnych wypadkach ingerencja wydaje się uzasadniona i proporcjonalna.

Projekt w zakresie w którym przetwarzanie danych nie jest związane z bezpieczeństwem narodowym, przewiduje ograniczenia zakresu niektórych obowiązków i praw dla administratora lub podmiotu przetwarzającego dane osobowe (art. 39 ust. 8), na podstawie art. 23 ust. 1 lit. e rozporządzenia 2016/679. Ograniczenia będą dotyczyć art. 15 (prawo dostępu przysługujące osobie, której dane dotyczą), art. 16 (prawo do sprostowania danych), art. 18 ust. 1 lit. a i d (prawo do ograniczenia przetwarzania w przypadku kwestionowania prawidłowości danych oraz w przypadku sprzeciwu) i art. 19 zdanie drugie (powiadamianie osoby, której dane dotyczą, o odbiorcach, których poinformowano o sprostowaniu lub usunięciu danych osobowych) rozporządzenia 2016/679, w przypadku gdy realizacja uprawnienia wynikającego z tego przepisu uniemożliwiłaby realizację zadań przez CSIRT.

Uzasadnieniem dla powyższych ograniczeń jest konieczność zadbania o interes publiczny, jakim jest obsługa incydentów u operatorów usług kluczowych. Skorzystanie z tych uprawnień mogłoby doprowadzić do konieczności ingerencji w zbierane przez CSIRT materiały i logi, co odbiłoby się negatywnie na możliwościach operacyjnych CSIRT. Konieczne było wyłączenie art. 15 rozporządzenia 2016/679, ze względu na fakt, że realizacja zadań CSIRT byłaby niemożliwa w przypadku, gdyby CSIRT musiały sprawdzać identyfikatory internetowe w swoich bazach na żądanie osób

[54)] Por. np. N. Rodrigues, A. Nogueira, P. Salvador, *Fighting Botnets – A Systematic Approach*, *The Fourth International Conference on Emerging Network Intelligence (EMERGING 2012)*, 23–28 September, 2012, Barcelona, Spain.

fizycznych. Dane przetwarzane przez CSIRT służą w pierwszej kolejności identyfikacji urządzeń oraz wektorów ataku. Podobną argumentację należy zastosować w sprawie sprostowania danych – w opinii projektodawcy, realizacja tego obowiązku nie powinna mieć zastosowania do CSIRT, które zbierają przede wszystkim dane surowe (wynikające m.in. z analizy ruchu sieciowego), które następnie przetwarzają. Konieczność prostowania danych na tak wczesnym etapie (zbierania informacji o incydencie i zmniejszeniu jego skutków) utrudniłoby, a nawet uniemożliwiłoby wsparcie obsługi incydentu. Jeżeli chodzi o wyłączenie obowiązki z art. 18 ust. 1 lit. a i d, uzasadnieniem jest konieczność zapewnienia szybkiego i efektywnego wsparcia obsługi incydentu. Wszelkie opóźnienia w reakcji na incydenty, wynikające z obsługi wniosków dotyczących prawdziwości danych bądź sprzeciwu, miałyby negatywne skutki dla cyberbezpieczeństwa. Aby zminimalizować zakres wyłączeń, dalej jest możliwe żądanie od administratora ograniczenia przetwarzania w przypadkach określonych w lit. b (przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania) oraz lit. c (administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń). Warto jednak zaznaczyć, że w określonych w art. 18 ust. 2 rozporządzenia 2018/679 przypadkach, CSIRT będą mogły dalej przetwarzać dane osobowe – tj. zastosowanie będą miały zasady ogólne rozporządzenia 2016/679. Ze względu na zamknięty krąg odbiorców (CSIRT, podmioty krajowego systemu cyberbezpieczeństwa, organy ścigania) wyłączono także stosowanie art. 19 zd. drugie. Zachowano jednocześnie obowiązek ze zd. pierwszego, z uwagi na wymianę informacji między CSIRT w zw. z zachowanym obowiązkiem z art. 18 ust. 1 lit. b i c.

Co do innych obowiązków określonych w rozporządzeniu 2016/679, warto wskazać, że obowiązek informacyjny z art. 14 nie będzie miał zastosowania w związku z treścią art. 14 ust. 5 lit. c, ze względu na istniejącą podstawę prawną oraz odpowiednie środki ochrony stosowane przez CSIRT. Podobna kwestia dotyczy prawa do bycia zapomnianym, które nie ma zastosowania ze względu na dopuszczalne wyłączenie z art. 17 ust. 3 lit. b rozporządzenia 2016/679 (realizowanie przez CSIRT zadania publicznego określonego w niniejszym projekcie ustawy).

Skorzystanie przez osobę z niektórych uprawnień przewidzianych rozporządzeniem 2016/679 mogłoby mieć negatywny wpływ na skuteczność i efektywność wykonywania

ustawowych obowiązków przez CSIRT, sektorowe zespoły cyberbezpieczeństwa i organy właściwe, a w konsekwencji mogłoby utrudnić realizację celów projektowanej ustawy.

Warunkiem przetwarzania danych wrażliwych, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, jak również przetwarzania danych z uwzględnieniem wyłączeń, o których mowa w art. 39 ust. 2, przez CSIRT i sektorowe zespoły cyberbezpieczeństwa, jest prowadzenie przez te podmioty analizy ryzyka, stosowanie środków ochrony przed złośliwym oprogramowaniem, stosowanie mechanizmów kontroli dostępu oraz opracowywanie procedury bezpiecznej wymiany informacji. Jest to również realizacja art. 23 ust. 3 rozporządzenia 2016/679.

Projektodawca przewiduje również, że przekazywanie danych osobowych między CSIRT oraz sektorowymi zespołami cyberbezpieczeństwa musi się odbywać w zakresie niezbędnym do zapewnienia efektywnej współpracy przewidzianej ustawą.

Dane, w tym dane osobowe, będą przekazywane organom ścigania, gdy incydent, zdaniem CSIRT, wyczerpuje znamiona przestępstwa. CSIRT są również uprawnione do przetwarzania informacji stanowiących tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji ustawowych zadań (art. 40). Ust. 3 tego artykułu przewiduje, że CSIRT oraz sektorowe zespoły cyberbezpieczeństwa zobowiązane są do zachowania tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, pozyskanych w związku z realizacją zadań, o których mowa w ustawie.

Rozdział 8: Organy właściwe do spraw cyberbezpieczeństwa

W rozdziale powyższym zostały określone organy właściwe dla poszczególnych sektorów wymienionych w dyrektywie 2016/1148. Przyjęty w ustawie model regulacyjny zakłada poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym. Obowiązki o charakterze administracyjnym, regulacyjnym i kontrolnym zostały przypisane właściwym ministrom dla wymienionych w dyrektywie 2016/1148 sektorów, czyli sektora energii, transportowego, bankowości i instytucji finansowych, ochrony zdrowia, zaopatrzenia w wodę, infrastruktury cyfrowej i dostawców usług cyfrowych (art. 41). W przypadku sektora ochrony zdrowia, infrastruktury cyfrowej i dostawców usług cyfrowych

uwzględniono odrębność podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej. W art. 42 został wskazany katalog zadań, który będą realizować organy właściwe. Zadania te obejmują prowadzenie analiz, wydawanie decyzji administracyjnych pod kątem uznania za operatora usług kluczowych, wygaśnięcia decyzji o uznaniu za operatora usług kluczowych, monitorowania stosowania przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych we właściwych im sektorach.

Organy właściwe mogą wezwać operatora usługi kluczowej lub dostawcę usługi cyfrowej na wniosek właściwego CSIRT do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego.

Organy właściwe przygotowują we współpracy z CSIRT rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów. Ustawodawca zakłada tutaj, że z uwagi na dynamizm środowiska normatywnego i specyfikę poszczególnych sektorów, organy właściwe określą w wytycznych szczegółowych w jaki sposób należy np. realizować obowiązki w zakresie wdrożenia systemu zarządzania bezpieczeństwem przez operatorów usług kluczowych z danego sektora. Ponadto organy te mają też przewidzianą dyrektywą możliwość prowadzenia współpracy z właściwymi organami państw członkowskich Unii Europejskiej. To uprawnienie jest szczególnie ważne w kontekście organu właściwego dla dostawcy usług cyfrowych, który, współpracując z odpowiednikami w innych państwach członkowskich, może zwracać się o podejmowanie działań wobec dostawców naruszających przepisy ustawy i rozporządzenia wykonawczego 2018/151. Art. 42 ust. 2 projektowanej ustawy wprowadza mechanizm, który pozwoli organowi właściwemu dla dostawców usług cyfrowych zwrócić się do swojego odpowiednika w innym właściwym państwie członkowskim UE o podjęcie analogicznych działań, jakie projekt ustawy przypisuje polskiemu organowi, czyli przeprowadzanie kontroli, zobowiązywanie do usunięcia nieprawidłowości ustalonych w wyniku kontroli oraz nakładanie kar pieniężnych. Tego rodzaju zwrócenie się do organu innego państwa członkowskiego UE będzie możliwe, jeżeli dostawca usługi cyfrowej nie posiada siedziby zarządu na terytorium RP bądź nie wyznaczył przedstawiciela na jej terytorium, ale jego systemy informacyjne znajdują się na terytorium RP. Zawarcie takiego rozwiązania w ustawie jest konieczne z uwagi na fakt, że część dostawców

usług cyfrowych nie posiada w Polsce siedziby ani przedstawiciela, ale wiele osób przebywających na terytorium Polski jest usługobiorcami usług świadczonych przez takich dostawców.

Projektodawca wprowadza w art. 43 dla organów właściwych przepisy uprawniające do żądania przekazania informacji od podmiotów działających w sektorach i podsektorach wymienionych w załączniku nr 1 do ustawy i świadczących usługi zależne od systemów informacyjnych. Projektodawcy chodzi wyłącznie o informacje, które umożliwią organom właściwym wstępną ocenę, czy dany podmiot spełnia przesłanki dla uznania go za operatora usług kluczowych. Dopiero zaś na tej podstawie organ właściwy podejmowałby decyzję w sprawie ewentualnego wszczęcia postępowania administracyjnego. Uzyskanie powyższych informacji w trybie poza kontrolnym pozwoliłoby organowi właściwemu na należytą ocenę ryzyka niespełniania wymogów ustawowych przez poszczególnych operatorów kluczowych, bez nakładania dodatkowych, nadmiernych obowiązków na operatora usług kluczowych, wynikających z konieczności czynnego uczestnictwa w prowadzonej kontroli. Zgodnie z przyjętymi rozwiązaniami wystąpienie o udzielnie informacji oraz brak udzielenia informacji przez podmiot lub operatora usługi kluczowej nie wpływa na możliwości wszczęcia postępowania administracyjnego albo postępowania kontrolnego.

Oprócz funkcjonowania zespołów CSIRT na poziomie krajowym, projektodawca stwarza możliwość powołania sektorowego zespołu cyberbezpieczeństwa przez organ właściwy (art. 44). Do zadań takiego zespołu zalicza się przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze, wspieranie operatorów usług kluczowych, analizę incydentów poważnych oraz współpracę z zespołami CSIRT, a także udział w wymianie informacji o incydentach poważnych o charakterze transgranicznym. Oprócz powyższego, w niektórych przepisach projektowanej ustawy sektorowe zespoły cyberbezpieczeństwa otrzymują analogiczne uprawnienia jak zespoły CSIRT, np. w zakresie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, czy odnośnie do obowiązku operatorów usług kluczowych do zgłaszania incydentów poważnych nie tylko do właściwego zespołu CSIRT, ale także do sektorowego zespołu cyberbezpieczeństwa (o ile został ustanowiony) oraz współdziałania z tym zespołem (art. 11 ust. 3). Analogiczne przepisy, lecz stanowiące o fakultatywnej możliwości przekazywania zgłoszeń, wprowadza się wobec mniej istotnych zdarzeń niż incydent poważny (art. 13 ust. 3). Jak wspomniano na wstępie

ustawa pozostawia regulacjom na poziomie sektorowym określenie szczegółowego trybu ustanawiania takich zespołów.

Stworzenie możliwości powoływania sektorowych zespołów cyberbezpieczeństwa wynika ze specyfiki tych sektorów oraz potrzeby współpracy i koordynacji działań wewnątrz nich, a także uzyskania większych zdolności dzięki połączeniu zasobów, jakimi dysponują podmioty w ramach sektorów. W toku uzgadniania i opiniowania projektu ustawy zgłoszone zostały uwagi wskazujące na potrzebę istnienia zespołów cyberbezpieczeństwa. W niektórych sektorach funkcjonują już takie zespoły. Związek Banków Polskich powołał Bankowe Centrum Cyberbezpieczeństwa, a CERT Polskich Sieci Energetycznych ma się w przyszłości stać zespołem CERT dla sektora elektroenergetycznego.

Rozdział 9: Zadania ministra właściwego do spraw informatyzacji

Ustawa określa nowe role ministra właściwego do spraw informatyzacji w ramach krajowego systemu cyberbezpieczeństwa. Art. 45 projektu ustawy nakłada na ministra właściwego do spraw informatyzacji realizację pakietu zadań o charakterze organizacyjnym i sprawozdawczym. Minister właściwy do spraw informatyzacji jest odpowiedzialny za monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej i realizację planów działań na rzecz jej wdrożenia. Minister właściwy ds. informatyzacji opracowuje roczne sprawozdania dotyczące poważnych incydentów zgłaszanych przez operatorów usług kluczowych oraz incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, będąc odpowiedzialnym za monitorowanie cyberbezpieczeństwa na poziomie krajowym w wymiarze strategicznym. Z drugiej strony w ramach pełnienia funkcji Pojedynczego Punktu Kontaktowego (art. 48–50) minister właściwy do spraw informatyzacji będzie odpowiadać za odbiór i przekazywanie, na wniosek właściwych CSIRT i sektorowych zespołów cyberbezpieczeństwa, zgłoszeń incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej, zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy, wymianę informacji na rzecz organów władz publicznych, organów właściwych w Polsce i za granicą, CSIRT, realizację obowiązków sprawozdawczych wobec Grupy Współpracy i Komisji Europejskiej.

Projekt zobowiązuje w art. 46 ministra właściwego do spraw informatyzacji do zapewnienia rozwoju lub utrzymania systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa, generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa i ostrzeganie o zagrożeniach cyberbezpieczeństwa, zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym. Ustawa stwarza możliwości korzystania z systemu przez zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa i Prezesa UKE na podstawie porozumienia z ministrem. Porozumienie ma również określać zakres i warunki korzystania z systemu teleinformatycznego.

Przepisy art. 47 dopuszczają możliwość delegowania realizacji zadań o charakterze organizacyjnym i technicznym na jednostki podległe lub nadzorowane przez ministra właściwego do spraw informatyzacji.

Rozdział 10: Zadania Ministra Obrony Narodowej

Projekt ustawy określa w art. 51 zadania Ministra Obrony Narodowej w ramach krajowego systemu cyberbezpieczeństwa, w jego militarnym wymiarze. Jako główne zadania tego organu wskazuje się współpracę z właściwymi podmiotami NATO, Unii Europejskiej i innych organizacji międzynarodowych, zapewnienie Siłom Zbrojnym RP zdolności do działań obronnych w cyberprzestrzeni, przeprowadzanie szkoleń specjalistycznych, rozwój zdolności kryptologicznych i zapewniania cyberbezpieczeństwa, kierowanie działaniami związanymi z obsługą incydentów, dokonywanie oceny zagrożeń cyberbezpieczeństwa w czasie stanu wojennego, oceny wpływu incydentów na system obrony państwa oraz prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO. Wprowadzenie do projektowanej ustawy osobnego rozdziału dotyczącego zadań Ministra Obrony Narodowej ma na celu uwzględnienie jego roli w procesie nadzoru nad cyberobroną państwa, uregulowanie odpowiedzialności za sferę militarną krajowego systemu cyberbezpieczeństwa oraz uwzględnienie funkcjonowania tego systemu w czasie obowiązywania stanu wojennego.

Rozdział 11: Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa

W rozdziale 11 uregulowano kwestie związane z nadzorem i kontrolą. Systemem nadzoru, zgodnie z art. 53, objęte zostaną podmioty świadczące usługi z zakresu cyberbezpieczeństwa, operatorzy usług kluczowych oraz dostawcy usług cyfrowych.

W ustawie przewidziano rozdzielenie kompetencji nadzorczych z uwagi na charakter podmiotów podlegających nadzorowi. W zakresie podmiotów świadczących usługi z zakresu cyberbezpieczeństwa nadzór będzie pełnił minister właściwy do spraw informatyzacji.

W ramach nadzoru minister właściwy do spraw informatyzacji będzie zapewniał przestrzeganie przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa takich wymogów w zakresie potencjału organizacyjno-technicznego, odpowiedniego zabezpieczenia pomieszczeń przed zagrożeniami fizycznymi i środowiskowymi oraz wdrożenia zabezpieczeń w związku z przetwarzaniem informacji.

Nadzór w odniesieniu do operatorów usług kluczowych dotyczył będzie spełniania wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, związanych ze świadczonymi usługami kluczowymi. Nadzór ten będzie sprawowany przez organy właściwe. Nadzór w odniesieniu do dostawców usług cyfrowych dotyczył będzie spełniania wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych i zgłaszania incydentów i sprawowany będzie przez organy właściwe dla dostawców cyfrowych.

W projekcie ustawy wskazano jakie uprawnienia w ramach nadzoru przysługiwały będą organom właściwym oraz ministrowi właściwemu do spraw informatyzacji. Warto zauważyć, że wskazane w art. 53 ust. 2 uprawnienia występują w sposób niezależny od siebie. Organy nadzorujące w ramach sprawowanego nadzoru mogą prowadzić kontrole a także stosować uprawnienia o charakterze władczym wobec kontrolowanych podmiotów, polegające na zobowiązaniu do usunięcia nieprawidłowości ustalonych w wyniku kontroli oraz nakładać administracyjne kary pieniężne. Wzorem dyspozycji zawartych w dyrektywie 2016/1148 wprowadzono w ustawie – w art. 53 ust. 3 – szczególne rozwiązania odnoszące się do organu właściwego do spraw dostawców usług cyfrowych. Podjęcie czynności władczych następuje po uzyskaniu dowodu (np. także z organu właściwego z innego państwa członkowskiego), że dostawca usług

cyfrowych nie spełnia wymogów określonych w rozporządzeniu wykonawczym 2018/151 lub nie wykonuje wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych.

W projekcie (art. 54) wskazano także, że do kontroli podmiotów będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców[55)]. Jednocześnie wskazano, że do podmiotów niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej[56)] określające zasady i tryb przeprowadzania kontroli.

Z uwagi na stosowne dyspozycje w ustawie – Prawo przedsiębiorców dotyczące uregulowania sposobu prowadzenia kontroli, w art. 55–59 projektu ustawy uregulowano niezbędne zagadnienia w tym zakresie. 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, wskazano, 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 te uprawnienia 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.

[55)] Dz. U. z 2018 r. poz. 646.
[56)] Dz. U. poz. 1092.

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 – warto za to przypomnieć, że wymierzanie kar pieniężnych będzie się odbywać w drodze postępowania administracyjnego, na zasadach ogólnych (z możliwością odwołania i drogi sądowej).

Rozdział 12: Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa

Wychodząc naprzeciw potrzebie wzmocnienia koordynacji działań i wymiany informacji w warstwie strategiczno-politycznej między instytucjami odpowiedzialnymi za cyberbezpieczeństwo w sferze cywilnej, wojskowej, sektorów usług kluczowych oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości oraz fakt, że dotychczasowe działania miały charakter rozproszony, projektodawca zakłada powołanie instytucji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa. Zgodnie z art. 62 Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa będzie odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań dotyczących

cyberbezpieczeństwa w Rzeczypospolitej Polskiej. Pełnomocnik Rządu, w randze sekretarza stanu lub podsekretarza stanu, będzie powoływany i odwoływany przez Prezesa Rady Ministrów. Do jego zadań będzie należeć m.in. analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT. W realizacji tego procesu zostanie wykorzystany mechanizm Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, o której mowa w rozdziale 13. Elementem Strategii jest podejście do oceny ryzyka, co przyjmie formę metodyki zarządzania ryzykiem na potrzeby cyberbezpieczeństwa, opracowanej w ramach Planu działań do Strategii. Pełnomocnik Rządu będzie również odpowiedzialny za opiniowanie projektów aktów prawnych oraz innych dokumentów rządowych mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa, a także inicjował krajowe ćwiczenia z zakresu cyberbezpieczeństwa.

Projekt ustawy przewiduje również powołanie Kolegium do Spraw Cyberbezpieczeństwa jako organu opiniodawczo-doradczego w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych (art. 64). Potrzebę utworzenia ciała opiniodawczo-doradczego sygnalizowano w trakcie uzgadniania i opiniowania projektu z podmiotami, które będą wchodzić w skład systemu. Działalność Kolegium pozwoli zachować większą spójność systemu i jego transparencję oraz nada zagadnieniu cyberbezpieczeństwa odpowiednią rangę, jak i umożliwi formułowanie spójnych kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa.

Art. 65 projektu określa zakres spraw w jakich Kolegium formułuje oceny lub wyraża opinie, w tym w stosunku do zadań wykonywanych przez zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa oraz organy właściwe. Na czele Kolegium stoi Prezes Rady Ministrów, ponadto w jego skład wchodzą sekretarz Kolegium (powoływany przez Prezesa Rady Ministrów spośród osób posiadających poświadczenie bezpieczeństwa o klauzuli „tajne”), oraz członkowie, którymi są: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej (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. W posiedzeniach Kolegium uczestniczą także: Dyrektor RCB, Szef ABW, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby.

Przepisy zawarte w art. 67 wprowadzają ponadto uprawnienie Prezesa Rady Ministrów, na podstawie rekomendacji Kolegium, do wydawania wiążących wytycznych oraz zasięgania informacji od ministra właściwego do spraw wewnętrznych, Ministra Obrony Narodowej, ministra właściwego do spraw informatyzacji, Szefa Agencji Bezpieczeństwa Wewnętrznego, dyrektora NASK – Państwowego Instytutu Badawczego w celu koordynacji działań w zakresie cyberbezpieczeństwa. Prezesowi Rady Ministrów zostały również nadane uprawnienia wydawania wiążących wytycznych dla zespołu CSIRT w zakresie obsługi incydentów krytycznych, w tym wskazywania CSIRT odpowiedzialny za obsługę incydentu krytycznego.

Rozdział 13: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Rozdział 13 zawiera regulacje dotyczące trybu przyjmowania przez Radę Ministrów i zakresu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Przepisy tego artykułu zawierają wyliczenie przykładowych elementów treści, jakie mają znaleźć się w dokumencie. Zgodne z art. 69 projektu Strategia uwzględnia w szczególności cele i priorytety w zakresie cyberbezpieczeństwa, podmioty zaangażowane w jej wdrażanie i realizację, środki służące realizacji jej celów, środki w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorami publicznym i prywatnym. Strategia ma też uwzględniać podejście do oceny ryzyka, działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Przepisy rozdziału wskazują okres, na jaki jest przyjmowana Strategia oraz zasady współdziałania podmiotów włączonych w proces jej opracowywania. Do czasu przyjęcia nowego dokumentu, rolę Strategii pełni uchwała Rady Ministrów w sprawie Krajowych Ram Cyberbezpieczeństwa na lata 2017–2022.

Rozdział 14: Przepisy o karach pieniężnych

W rozdziale 14 zawarto przepisy regulujące nakładanie administracyjnych kar pieniężnych. Przewiduje się, iż organ właściwy dla danego sektora będzie mógł nałożyć na operatorów usług kluczowych administracyjną karę pieniężną za brak realizacji obowiązków wynikających z ustawy. Przykładowo administracyjną karą pieniężną będzie mógł zostać ukarany operator usługi kluczowej, który nie wdrożył środków technicznych i operacyjnych, nie zgłasza incydentów poważnych, nie zapewnia ich obsługi, w tym nie współdziała w trakcie realizacji tych czynności z właściwym CSIRT. Karom pieniężnym podlega też operator, który nie wyznaczył osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, uniemożliwia lub utrudnia osobie przeprowadzającej czynności kontrolne, nie przeprowadził audytu bezpieczeństwa systemów informacyjnych. Karom pieniężnym podlega też dostawca usługi cyfrowej, jednak z uwagi na ograniczony reżim regulacyjny określony względem tych podmiotów w dyrektywie 2016/1148, kary odnoszą się wyłącznie do kwestii związanych ze zgłaszaniem i obsługą incydentów istotnych, usuwaniem podatności, które doprowadziły lub mogły doprowadzić do incydentu istotnego bądź działaniem na szkodę dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi. W świetle przepisów dyrektywy dopuszczalne jest nakładanie na dostawcę usług cyfrowych sankcji w postaci kar pieniężnych wyłącznie w przypadku naruszeń krajowych przepisów implementujących dyrektywę. Nie jest natomiast dopuszczalne wprowadzanie sankcji za przepisy ustanowione przez ustawodawcę europejskiego, a więc przepisy dotyczące zabezpieczeń systemów informacyjnych służących do świadczenia usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 z 30 stycznia 2018 r.

Zgodnie z zasadą proporcjonalności wysokość kar administracyjnych została odpowiednio zróżnicowana. Za niewypełnianie obowiązków administracyjnych, tj. wyznaczenie osoby odpowiedzialnej za kontakty w ramach krajowego systemu cyberbezpieczeństwa przewiduje się najniższe kary do 15 tys. zł. Przykładowo również przewiduje się od 20 tys. zł kary za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego bądź istotnego. Z kolei z tytułu niewypełniania obowiązków o istotnym charakterze z punktu widzenia cyberbezpieczeństwa, np. za nieprzeprowadzenie audytu, bądź nie usunięcie w wyznaczonym terminie

nieprawidłowości stwierdzonych w wyniku kontroli – przewiduje się kary odpowiednio wyższe i będzie to 200 000 zł.

Oddzielnie należy wspomnieć o administracyjnej karze pieniężnej w wysokości do 1 000 000 zł, którą może nałożyć organ właściwy dla danego sektora na operatora usługi kluczowej bądź dostawcy usługi cyfrowej, który uporczywie narusza przepisy ustawy, powodując bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, bądź zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych.

Należy wskazać, że operatorzy usług kluczowych obowiązani są do realizacji określonych obowiązków w ustawie na podstawie decyzji administracyjnej o uznaniu za operatora usługi kluczowej. Świadczy to o tym, iż w stosunku do tych podmiotów należy stosować podwyższony wymóg zachowania profesjonalizmu i jakości działania w zakresie przestrzegania (z punktu widzenia projektodawcy) zasadniczych reguł cyberbezpieczeństwa. Przewidzenie w treści ustawy możliwości zastosowania wobec ww. podmiotów sankcji administracyjnej jest zasadne z punktu widzenia celów projektu ustawy oraz nie narusza zasad demokratycznego państwa prawnego. Należy też podkreślić, że wszystkie z przewidzianych kar stanowią górną granicę sankcji. Organy właściwe dla danego sektora będą mogły różnicować w ramach ww. granic wysokość kar, dostosowując wysokość sankcji do sytuacji faktycznej w jakiej doszło do naruszenia. Mając na uwadze charakter potencjalnych naruszeń, przewidziano w ustawie mechanizm prewencji, zgodnie z którym przed wszczęciem postępowania w sprawie nałożenia kary pieniężnej, organ właściwy dla danego sektora może wezwać operatora usługi kluczowej do usunięcia naruszenia w wyznaczonym terminie, jeżeli przemawia za tym charakter naruszenia. Powyższa instytucja pozwoli na zdyscyplinowanie operatorów usług kluczowych w wypełnianiu swoich podstawowych obowiązków, a jednocześnie nie będzie generowało konieczności wszczynania postępowań administracyjnych i ich formalnego prowadzenia oraz zakończenia.

Kodeks postępowania administracyjnego reguluje kwestie nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu. Z uwagi na powyższe w projekcie ustawy wskazano wprost, iż w sprawach administracyjnych kar pieniężnych nakładanych na operatorów usług kluczowych zastosowanie znajdzie dział

IVa Kodeksu postępowania administracyjnego (dalej: kpa)[57]. Przepisy działu IVa kpa w sposób kompleksowy regulują aspekty proceduralne nakładania i wymierzania administracyjnych kar pieniężnych, ale też kwestie o charakterze materialnym. Co najistotniejsze z punktu widzenia niniejszej ustawy dział IVa kpa zawiera rozbudowany katalog przesłanek wymiaru administracyjnej kary pieniężnej.

Należy wskazać, że w rozdziale 14 przewidziano wyłącznie przepisy regulujące przesłanki (rodzaje naruszeń) oraz wysokość kar administracyjnych. Wskazano także na tryb ich nakładania i wymierzenia. Zagadnienia działania organów właściwych dla danego sektora przed zainicjowaniem wszczęcia postępowania w celu nałożenia kary administracyjnej regulują przepisy całej ustawy, w tym w szczególności przepisy rozdziału 11 dotyczącego nadzoru i kontroli.

Rozdział 15: Zmiany w przepisach obowiązujących, przepisy przejściowe, dostosowujące i końcowe

W art. 83 projektu ustawy zawarto regułę wydatkową zgodnie z art. 50 ustawy o finansach publicznych. Wskazane kwoty zostały oparte na zawartych w dołączonej do projektu ocenie skutków regulacji i wskazują one różnice w wydatkach budżetu państwa w stosunku do kwot zaplanowanych w ustawie budżetowej. Wskazano kilka możliwych mechanizmów korygujących, w zależności od zadań ustawowych i sytuacji prawnej dysponenta części budżetowej. Zgodnie z art. 50 ust. 6 pkt 8 ustawy o finansach publicznych, nie uwzględniono wydatków dla części – obrona narodowa.

Operatorzy usług kluczowych realizują niektóre obowiązki związane z ustawą w terminie 6 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej. Inne obowiązki związane z wdrożeniem systemu bezpieczeństwa mają być realizowane przez operatora usługi kluczowej w terminie 3 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej. Ustawa wprowadza również przepisy przejściowe umożliwiające sprawną realizację obowiązków sprawozdawczych w pierwszym roku obowiązywania ustawy wobec Komisji Europejskiej i Grupy Współpracy. W przypadku systemu teleinformatycznego, o którym mowa w art. 46, przewidziane jest uruchomienie systemu do eksploatacji z dniem 1 stycznia 2021 r.

Projekt ustawy będzie miał wpływ na sytuację małych i średnich przedsiębiorców świadczących usługi kluczowe, jeżeli zostanie w stosunku do nich wydana decyzja

[57] Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650.

o uznaniu za operatora usługi kluczowej oraz średnich przedsiębiorców świadczących usługi cyfrowe. Projekt nie będzie miał wpływu na mikroprzedsiębiorców i małych przedsiębiorców świadczących usługi cyfrowe. Szczegółowy wpływ regulacji zawartych w projekcie przedstawiono w pkt 4 oceny skutków regulacji. W projekcie przewidziano możliwość nakładania kar pieniężnych na operatorów usług kluczowych w przypadku naruszenia przepisów ustawy.

Ustawa zawiera przepisy zmieniające do ustawy z dnia 7 września 1991 r. o systemie oświaty oraz ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Zamierzeniem zmian w ustawie – Prawo telekomunikacyjne jest włączenie Prezesa UKE w przekazywanie informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług u przedsiębiorców telekomunikacyjnych na potrzeby wymiany informacji w ramach krajowego systemu cyberbezpieczeństwa, o którym mowa w niniejszej ustawie.

Podstawą projektowanej nowelizacji ustawy z dnia 7 września 1991 r. o systemie oświaty są cele postawione w Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Jednym z nich jest cel szczegółowy 3 – Zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni, a w ramach tego celu pkt 5: Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli. Zakłada on m.in. rozpoczynanie już na etapie kształcenia wczesnoszkolnego edukacji w zakresie cyberbezpieczeństwa oraz opracowanie i wdrożenie zmian do podstaw programowych nauczania tematyki bezpiecznego korzystania z cyberprzestrzeni. Cel ten został uwzględniony w rozporządzeniu Ministra Edukacji Narodowej z dnia 14 lutego 2017 r. w sprawie podstawy programowej wychowania przedszkolnego oraz podstawy programowej kształcenia ogólnego dla szkoły podstawowej, w tym dla uczniów z niepełnosprawnością intelektualną w stopniu umiarkowanym lub znacznym, kształcenia ogólnego dla branżowej szkoły I stopnia, kształcenia ogólnego dla szkoły specjalnej przysposabiającej do pracy oraz kształcenia ogólnego dla szkoły policealnej (Dz. U. poz. 356) oraz w rozporządzeniu Ministra Edukacji Narodowej z dnia 30 stycznia 2018 r. w sprawie podstawy programowej kształcenia ogólnego dla liceum ogólnokształcącego, technikum oraz branżowej szkoły II stopnia (Dz. U. poz. 467). Uwzględnia on również podnoszenie kompetencji i umiejętności nauczycieli w zakresie

edukacji informatycznej. Działaniom tym towarzyszą zmiany w systemie doskonalenia i kształcenia nauczycieli.

Zmiany w ustawie o zarządzaniu kryzysowym mają z kolei na celu ograniczenie obowiązków w zakresie przygotowania dokumentacji w zakresie cyberbezpieczeństwa, w przypadku gdy właściciele, posiadacze samoistni i zależni obiektów, instalacji lub urządzeń wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w ustawie o zarządzaniu kryzysowym, są jednocześnie operatorami usług kluczowych oraz posiadają zaakceptowane przez Dyrektora RCB plany ochrony infrastruktury krytycznej. Przepisy zmieniające ustawę o zarządzaniu kryzysowym mają również na celu umocowanie odpowiednio Zespołu do spraw Incydentów Krytycznych, oraz określają sposób przygotowywania wkładu w zakresie cyberbezpieczeństwa przez Pełnomocnika Rządu do spraw Cyberbezpieczeństwa do raportu o zagrożeniach bezpieczeństwa państwa.

Projekt ustawy o krajowym systemie cyberbezpieczeństwa jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projekt nie wymaga przedstawienia właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia. Ogłoszona w Dzienniku Ustaw ustawa zostanie przekazana do Komisji Europejskiej jako krajowy środek wykonawczy.

Projekt ustawy został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

Nazwa projektu Projekt ustawy o krajowym systemie cyberbezpieczeństwa **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, zastępca dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 25 kwietnia 2018 r. **Źródło:** 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 194 z 19.07.2016, str. 1). **Nr w wykazie prac legislacyjnych Rady Ministrów** UD31

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Współcześnie rozwój społeczny i gospodarczy w znacznym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji. Obecność technologii teleinformatycznych, w tym operacje na dużych zasobach danych, służą świadczeniu szerokiej gamy usług, mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, w tym m.in. usług finansowych, transportowych, z zakresu ochrony zdrowia, energii, zaopatrzenia w wodę pitną. Każde znaczące zakłócenie funkcjonowania cyberprzestrzeni będzie miało również wpływ na poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, a także świadczenie usług przez przedsiębiorców, a w rezultacie również na ogólnie pojmowane bezpieczeństwo państwa. W związku z tym niezbędne jest wprowadzenie rozwiązań pozwalających na stworzenie skutecznego i efektywnego systemu bieżącego monitorowania oraz zarządzania cyberbezpieczeństwem w skali kraju.

Projektowana ustawa stanowi implementację dyrektywy 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, zwanej dalej „dyrektywą 2016/1148/UE". Ponadto wpisuje się w cel 5 Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 – Osiągnięcie zdolności do skoordynowanych w skali kraju działań służących zapobieganiu, wykrywaniu, zwalczaniu oraz minimalizacji skutków incydentów naruszających bezpieczeństwo systemów informacyjnych istotnych dla funkcjonowania państwa.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Celem ustawy jest w szczególności:

1) organizacja oraz określenie sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, w tym:
   a) wskazanie sektorów gospodarki narodowej, dla których zastosowanie będą miały przepisy ustawy oraz określenie kryteriów kwalifikacji podmiotów objętych regulacją, a więc operatorów usług kluczowych;
   b) określenie minimalnych wymagań bezpieczeństwa teleinformatycznego dla systemów informacyjnych operatorów usług kluczowych i dostawców usług cyfrowych;
   c) przedstawienie rozwiązań systemowych i struktur zajmujących się cyberbezpieczeństwem na poziomie regulacyjnym, koordynacyjnym i technicznym;
   d) ustalenie ustawowych wymagań i powinności z zakresu cyberbezpieczeństwa dla zespołów reagowania na incydenty bezpieczeństwa komputerowego;
2) określenie sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy,
3) prawne umocowanie dokumentu ustanawiającego krajową Strategię Cyberbezpieczeństwa Rzeczpospolitej Polskiej;

Efektem wprowadzonej regulacji będzie podniesienie odporności usług kluczowych świadczonych z wykorzystaniem technologii informatycznych na ataki pochodzące z cyberprzestrzeni. Tym samym projektowana regulacja przyczyni się do lepszego zapewnienia ciągłości działania tych usług, tak aby zarówno obywatele, jak i przedsiębiorstwa miały do nich stały i niezakłócony dostęp.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Dyrektywa 2016/1148 jest w trakcie transpozycji w innych państwach członkowskich UE, jednakże w wielu z nich wprowadzono w ostatnich miesiącach albo jeszcze przed wejściem w życie dyrektywy różnorodne rozwiązania prawne i organizacyjne w zakresie zapewnienia cyberbezpieczeństwa, których część została opisana poniżej.

Wielka Brytania

W lutym 2017 r. w Wielkiej Brytanii została zainagurowana działalność Narodowego Centrum Cyberbezpieczeństwa

(National Cyber Security Centre – NCSC). Zadaniem Centrum jest pomoc administracji publicznej i przedsiębiorstwom w reagowaniu na poważne incydenty w dziedzinie cyberbezpieczeństwa oraz zwiększenie bezpieczeństwa w Internecie, dzięki działalności doradczej oraz pomocy technicznej. Przykładowe działania obejmują przeszukiwanie luk w zabezpieczeniach stron internetowych sektora publicznego, czy blokowanie fałszywych maili celem zapobiegania atakom phishingowym.

NCSC, organizacyjnie, jest częścią brytyjskiej agencji wywiadu i bezpieczeństwa (Government Communications Headquarters – GCHQ). Zostało powołane w celu implementacji dyrektywy 2016/1148 i pełni rolę punktu kontaktowego. Koszty uruchomienia i funkcjonowania NCSC do 2020 r., w tym koszty organizacyjne i zatrudnienia 100 najlepszych specjalistów z zakresu cyberbezpieczeństwa, którzy wcześniej pracowali w prywatnych przedsiębiorstwach, to 1,9 mld funtów.

Powołanie NCSC jest kolejnym etapem rozbudowy systemu cyberbezpieczeństwa w Wielkiej Brytanii. Do tej pory kluczową instytucją w systemie był CERT-UK liczący około 55 pracowników i realizujący typowe zadania dla CERT/CSIRT, czyli zarządzanie krajowymi incydentami z zakresu cyberbezpieczeństwa, w tym wsparcie dla podmiotów dotkniętych incydentem oraz promowanie świadomości dotyczącej zagrożeń w cyberprzestrzeni. Funkcjonują również partnerstwa publiczno-prywatne, polegające na wymianie informacji na temat zagrożeń i luk bezpieczeństwa w systemach teleinformatycznych (Cyber-security Information Sharing Partnership – inicjatywa CERT-UK) oraz mniejsze, kilkunastoosobowe zespoły analityczne, jak np. Fusion Cell złożony z przedstawicieli rządu i służb państwowych (pracowników m.in. GCHQ, MI5, MI6 i Policji). Biorąc pod uwagę system prawa w Wielkiej Brytanii rolą NCSC jest zachęcanie organizacji do zarządzania własnym ryzykiem w zakresie cyberbezpieczeństwa. Centrum wydaje rekomendacje, wytyczne i zapewnia wsparcie dotyczące cyberbezpieczeństwa, w tym w zakresie zarządzania incydentami.

Republika Czeska

Organem odpowiedzialnym za cyberbezpieczeństwo w Czechach jest Narodowa Agencja ds. Bezpieczeństwa Informacji i Cyberbezpieczeństwa (National Cyber and Information Security Agency – NCISA). Ogólne przepisy dotyczące wyznaczania operatorów usług kluczowych są w czeskiej ustawie o cyberbezpieczeństwie (ustawa 181/2014), szczegółowe w akcie wykonawczym (obecnie procedowanym). Wymogi techniczne bezpieczeństwa, zarządzanie ryzykiem i inne kwestie dotyczące szczegółowego stosowania ustawy zostały określone w rozporządzeniu 316/2014 (rozporządzenie w sprawie środków bezpieczeństwa, incydentów związanych z cyberbezpieczeństwem, środków reaktywnych i wymogów dotyczących cyberbezpieczeństwa) wydanym przez NCISA. Wszystkie wymienione akty zostały znowelizowane w ramach implementacji dyrektywy 2016/1148.

Ze względu na fakt, że dyrektywa 2016/1148 jest regulacją dotyczącą jednolitego rynku, czeskie rozwiązanie nie obejmuje w pełni infrastruktury krytycznej (choć niektóre podmioty będące jednocześnie infrastrukturą krytyczną i operatorem usługi kluczowej mogą się pojawić), różne są wymagania i obowiązki. Lista operatorów usług kluczowych nie jest publiczna, jednak nie przewidziano dla niej szczególnej klauzuli. Komercyjne CERT nie są regulowane ustawą – działają na zwykłych zasadach biznesowych, ale nie pełnią żadnej szczególnej funkcji w systemie (oba CERT wymienione w czeskiej regulacji są publiczne). Operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów (kara pieniężna za samo niezgłoszenie incydentu wynosi ok. 38 000 EUR, podobne kary obowiązują za niezastosowanie się do wytycznych pokontrolnych organu właściwego). Organ właściwy może ponadto, w określonych przypadkach, zabronić podmiotowi stosowania systemu teleinformatycznego, który nie spełnia wymogów bezpieczeństwa określonych w ustawie.

Holandia

Narodowe Centrum Cyberbezpieczeństwa (NCSC)[1)] jest od 2012 r. głównym podmiotem odpowiedzialnym za zapewnienie bezpieczeństwa cyberprzestrzeni w Holandii i podlega Ministerstwu Bezpieczeństwa i Sprawiedliwości. NCSC samodzielnie lub na wniosek wydaje wytyczne i rekomendacje urzędom administracji publicznej i operatorom sektorów krytycznych w związku z najważniejszymi ujawnionymi podatnościami i w sytuacji poważnych zdarzeń kryzysowych w dziedzinie cyberbezpieczeństwa. Centrum dysponuje sieciami typu „honey-pot" dla administracji centralnej i sektorów krytycznych (projekty sieci były zbudowane w kooperacji z polskim NASK). W jego strukturze znajduje się m.in. narodowy/rządowy CERT, uczestniczący w sieci European Governmental CERTs (EGC). W związku z rewizją strategii cyberbezpieczeństwa przyjętą w 2013 r. kompetencje NCSC zostały poszerzone o struktury odpowiedzialne za wymianę i analizę informacji niejawnych. Ponadto dodano kompetencje w zakresie monitorowania w czasie rzeczywistym zdarzeń w cyberprzestrzeni i przekształcono NCSC w centrum zdalnego zarządzania/reagowania na incydenty.

Finlandia

W wymiarze operacyjnym ochronę cyberprzestrzeni mają zapewnić poszczególne jednostki administracji w oparciu o przygotowane plany działania, które powstają na podstawie sporządzanych analiz ryzyka, które reguluje ustawa o ocenie bezpieczeństwa informacji (the Act on the Assessment of Information Security – 1406/2011)[2)]. Analizę ryzyka

[1)] https://www.ncsc.nl/english/organisation

[2)] http://www.finlex.fi/fi/laki/alkup/2011/20111406#Pidp3049664

zgodnie z ustawą może przeprowadzić narodowy regulator telekomunikacyjny (FICORA) bądź akredytowane przez regulatora jednostki. Centralny plan działania dla całej administracji został przyjęty w 2014 r. Pod auspicjami Ministerstwa Finansów funkcjonuje Zarząd Bezpieczeństwa Informacji Rządowej (The Government Information Security Management Board – VAHTI) koordynujący przekazywanie kluczowych informacji w zakresie centralnej administracji rządowej i wydawanie sektorowych wytycznych bezpieczeństwa.

Elementem działań operacyjnych jest budowa zdolności i rozwój monitoringu zagrożeń cyberprzestrzeni dotyczących kluczowych obszarów realizacji funkcji państwa w czasie rzeczywistym. W ramach struktury fińskiego regulatora rynku telekomunikacyjnego Viestintävirasto zostało powołane Centrum Cyberbezpieczeństwa (Cyber Security Centre). Centrum analizuje informacje od poszczególnych podmiotów z administracji i sektorów krytycznych dotyczące incydentów, głównych podatności, zakłóceń i ich efektów. Centrum współpracuje również z Policją, która jest właściwa do prowadzenia postępowań z zakresu cyberprzestępczości. Pod auspicjami Ministerstwa Finansów został również zainicjowany projekt budowy Security Operations Centre (SOC) w administracji centralnej - Central Government 24/7 Information Security Operations (SecICT). W skład SOC'a ma wejść m.in. rządowy CERT. Zakłada się wymianę informacji między Centrum a nowo tworzonym SecICT.

Kluczowym punktem strategii i przyjętych planów działania w zakresie cyberbezpieczeństwa jest także uruchomienie bezpiecznej sieci teleinformatycznej dla administracji publicznej (ustawa o TUVE), dzięki której można będzie przekazywać informacje dotyczące sektorów krytycznych, w tym informacje niejawne. Przesłanką utworzenia takiej sieci są korzyści centralizacji bezpieczeństwa teleinformatycznego. Fiński urząd ds. komunikacji elektronicznej, Viestintävirasto, zatrudnia około 240 osób.

Francja

Francja jest jednym z pierwszych krajów, które podjęły działania legislacyjne w celu wzmocnienia swojego cyberbezpieczeństwa w dziedzinie infrastruktury usług kluczowych. Politykę państwa w zakresie ochrony systemów teleinformatycznych prowadzi premier za pośrednictwem Agencji Bezpieczeństwa Systemów Informacyjnych (Agence nationale de la sécurité des systèmes d'information – ANSSI), zatrudniającej ok. 500 pracowników. Agencja dzięki pionowi operacyjnemu („operations room") i rozmieszczonym w ministerstwach sieciach typu „honey-pot" ma dostęp do bieżącej informacji na temat ataków i innych zagrożeń na poziomie centralnym; jednocześnie pełni rolę CSIRT odpowiedzialnego za obsługę incydentów i zagrożeń na szczeblu krajowym CERT-FR (CERT Narodowy).

Przepisy dotyczące bezpieczeństwa teleinformatycznego zostały wprowadzone do ustawy z dnia 18 grudnia 2013 r. o programowaniu wojskowym, która definiuje "operatorów o istotnym znaczeniu", zbliżonych do definicji "operatorów usług kluczowych" w dyrektywie 2016/1148/UE. Ustawa przewiduje, że operatorzy o istotnym znaczeniu powinni przestrzegać konkretnych środków bezpieczeństwa teleinformatycznego oraz są zobowiązani do zgłaszania incydentów do ANSSI. Agencja zapewnia wsparcie tym operatorom, wydając wytyczne bezpieczeństwa teleinformatycznego. Agencja jest zaangażowana w koordynację implementacji dyrektywy 2016/1148/UE. Aktualne podejście do implementacji zakłada, że wymagania bezpieczeństwa dla operatorów usług kluczowych będą podobne jak dla operatorów infrastruktury krytycznej, a liczba operatorów usług kluczowych będzie wyższa niż liczba podmiotów objętych wymaganiami z zakresu infrastruktury krytycznej. We Francji obecnie zidentyfikowano ponad 200 operatorów infrastruktury krytycznej w 12 sektorach. ANSSI będzie wyznaczone zarówno jako pojedynczy punkt kontaktowy i organ właściwy w zakresie bezpieczeństwa sieci i informacji.

Niemcy

Rozwiązania przewidziane w dyrektywie 2016/1148/UE zostały już wprowadzone w niemieckim porządku prawnym ustawą z dnia 25 lipca 2015 r. o zmianie ustawy z dnia 14 sierpnia 2009 r. o Federalnym Urzędzie ds. Bezpieczeństwa Informacji (*niem.* BSI). Ustawa zmienia istniejące ustawy o bezpieczeństwie infrastruktury krytycznej, prawie telekomunikacyjnym i inne, nie tworząc jednak spójnego systemu. Nałożyła na różne podmioty (przede wszystkim operatorów infrastruktury krytycznej i przedsiębiorców telekomunikacyjnych) nowe obowiązki dotyczące stosowania odpowiednich środków bezpieczeństwa, informowania klientów czy organów władzy publicznej o możliwych nadużyciach czy zagrożeniach. BSI dostał dodatkowe kompetencje w zakresie opracowywania standardów w zakresie cyberbezpieczeństwa, kontaktów z organami właściwymi.

BSI pełni funkcję federalnego urzędu ds. cyberbezpieczeństwa. Do jego zadań należy bieżąca analiza zagrożeń, przygotowywanie środków do ich zwalczania oraz zabezpieczanie przed nimi gospodarki. W ramach BSI funkcjonuje Cyber-Abwehrzentrum (Cyber-AZ), którego zadaniem jest koordynacja ochrony cyberprzestrzeni w Niemczech poprzez wczesne ostrzeganie, informację i prewencję. W stosowanie prawa dotyczącego bezpieczeństwa teleinformatycznego są zaangażowane ponadto Federalne Ministerstwo Spraw Wewnętrznych, Federalny Urząd Ochrony Ludności i Pomocy w przypadku Katastrof, kraje związkowe (landy), departamenty federalnych ministerstw: Transportu i Infrastruktury Cyfrowej, Gospodarki i Technologii, Edukacji i Nauki. Liczba operatorów usług kluczowych w Niemczech obejmuje ok. 1885 podmiotów, które są objęte dwoma pakietami rozporządzeń.

W Niemczech ustawa wprowadziła sektor spożywczy, niewystępujący w załączniku 2 dyrektywy 2016/1148/UE dyrektywy, natomiast nie objęła administracji publicznej, z uwagi na federalną strukturę państwa.

Niemiecki BSI zatrudnia w celu realizacji swoich zadań około 600 pracowników, a Cyber-AZ – 10 pracowników delegowanych.

Stany Zjednoczone

System bezpieczeństwa teleinformatycznego w Stanach Zjednoczonych jest opisany w wielu aktach prawnych. W Stanach Zjednoczonych odpowiednikiem europejskich regulacji z zakresu ochrony cyberprzestrzeni jest ustawa „Cyber Intelligence Sharing and Protection Act" z 2013 roku. Ustawa ma na celu zapewnienie wsparcia organom publicznym w zakresie zwiększenia odporności użytkowanych systemów teleinformatycznych oraz analizę zagrożeń pojawiających się w cyberprzestrzeni[3)]. Ponadto istnieją ustawy o oszustwach i nadużyciach komputerowych, jak i dotyczące uzyskania nieautoryzowanego dostępu do komputera, zakłóceń, pozyskiwania danych oraz o ochronie prywatności w komunikacji elektronicznej[4)]. Wydany został również Executive Order 13636/2013 – „Improving Critical Infrastructure Cybersecurity", który zidentyfikował 16 kluczowych obszarów infrastruktury oraz ustanowił organy nadzoru mające na celu poprawę bezpieczeństwa wśród podmiotów regulowanych. Założeniem amerykańskiego systemu cyberbezpieczeństwa jest silne partnerstwo publiczno-prywatne pomiędzy jednostkami administracji, środowiskiem naukowym i sektorem przedsiębiorstw w zakresie wymiany informacji na temat zagrożeń cyberprzestrzeni. Departament Bezpieczeństwa Wewnętrznego USA jest odpowiedzialny za sferę ochronę infrastruktury krytycznej – pod kątem zagrożeń fizycznych, a także dotyczących cyberprzestrzeni. Ministerstwo udziela wsparcia dla operatorów infrastruktury krytycznej, publikuje również raporty nt. potencjalnych zagrożeń i podatności. Dodatkowo amerykański instytut zajmujący się standaryzacją NIST (National Institute of Standards and Technology) realizuje wiele uznanych międzynarodowo projektów zwiększenia cyberbezpieczeństwa infrastruktury krytycznej (bez konieczności dodatkowych zmian prawnych).

Ministerstwo posiada 24-godzinne Narodowe Centrum Koordynacji, Komunikacji i Cyberbezpieczeństwa – National Cybersecurity and Communications Integration Center (NCCIC) dysponujące kompleksową informacją na temat cyberbezpieczeństwa, reagujące na incydenty, zarządzające bezpieczeństwem teleinformatycznym. Centrum jest również punktem wymiany informacji z federalną administracją rządową, agencjami wywiadowczymi i organami ścigania. Działalność Centrum opiera się na dobrowolnej współpracy administracji publicznej i sektorów krytycznych. Centrum może również prowadzić działania proaktywne na rzecz zapobiegania incydentom w sieciach teleinformatycznych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze wydobywania kopalin	24	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (trzy podmioty prowadzące kopalnie węgla brunatnego, dwadzieścia podmiotów prowadzących kopalnie węgla kamiennego, jeden podmiot prowadzący kopalnię miedzi)	Spełnienie wymogów z art. 10, –16 projektu ustawy Operatorzy usług kluczowych będą zobowiązani m.in. do wdrożenia systemu zarządzania bezpieczeństwem (art. 10), przygotowania dokumentacji z zakresu cyberbezpieczeństwa (art. 11), identyfikowania, rejestrowania oraz klasyfikowania incydentu, jak również zapewnienia obsługi incydentu i zgłaszania incydentu poważnego do właściwego CSIRT (art. 12), wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa (art. 15).
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze energii elektrycznej	30	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (pięć największych podmiotów wytwarzających prąd, OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze ciepła	3	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (trzy podmioty prowadzące elektrociepłownie, nieobjęte podsektorem energia elektryczna)	
Podmioty świadczące usługi kluczowe w sektorze	4	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz	

[3)] https://www.congress.gov/bill/114th-congress/house-bill/234

[4)] https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf

energii w podsektorze ropy naftowej		danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie, magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi)	
Podmioty świadczące usługi kluczowe w sektorze energii w podsektorze gazu	22	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający lub magazynujący gaz lub gaz ziemny oraz dziesięć największych przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE)	
Podmioty świadczące usługi kluczowe w sektorze energii w zakresie dostaw i usług dla sektora energii oraz jednostki nadzorowane i podległe ministrowi właściwemu do spraw energii oraz ministrowi właściwemu do spraw gospodarki złożami kopalin	15	Dane za BIP Ministra Energii: dwanaście instytutów badawczych, Zakład Unieszkodliwiania Odpadów Promieniotwórczych, Agencja Rezerw Materiałowych i Prezes Wyższego Urzędu Górniczego	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych ULC (czterech przewoźników lotniczych, zarządzający ośmioma największymi portami lotniczymi, piętnaście podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych).	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu morskiego)	21	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych MGMiŻŚ (założono objęcie dziesięciu największych armatorów, ośmiu portów morskich oraz trzech operatorów VTS)	

Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu śródlądowego)	0	Informacje z MGMiŻŚ.	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu drogowego	24	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych MI (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach). Jest możliwe poszerzenie tej grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod uwagę w szacunkach.	
Podmioty świadczące usługi kluczowe w sektorze bankowości i infrastruktury rynków finansowych	69	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, dziesięć największych krajowych zakładów ubezpieczeń, dziesięć największych instytucji płatniczych, dwa banki państwowe, jedna giełda, PWPW, dwaj operatorzy systemu obrotu i jeden kontrahent centralny).	
Podmioty świadczące usługi kluczowe w sektorze zaopatrzenia w wodę pitną i jej dystrybucję	31	Przedsiębiorstwa wodno--kanalizacyjne na wykazie IK.	
Podmioty świadczące usługi kluczowe w sektorze ochrony zdrowia	253	Szacunki oparte na danych z rejestrów Głównego Inspektora Farmaceutycznego, CSIOZ i MZ. Wyjaśnienie: Na potrzeby szacunków poczyniono następujące założenia. Uznano, że operatorami usług kluczowych będą podmioty lecznicze (podmioty realizujące świadczenia szpitalne), które miały więcej niż 18 000 hospitalizacji rocznie. Odpowiednio dla województw jest to: Dolnośląskie – 12 Kujawsko-Pomorskie – 8	

		Lubelskie – 8 Lubuskie – 3 Łódzkie – 8 Małopolskie – 10 Mazowieckie – 18 Opolskie – 3 Podkarpackie – 8 Podlaskie – 8 Pomorskie – 5 Śląskie – 15 Świętokrzyskie – 5 Warmińsko-mazurskie – 3 Wielkopolskie – 12 Zachodniopomorskie – 5. Pozostałe podmioty, które spełniały wymogi z załącznika nr 1 do projektu ustawy, to NFZ, CSIOZ, pięćdziesiąt największych podmiotów prowadzących hurtownie farmaceutyczne, pięćdziesiąt największych podmiotów prowadzących największe apteki oraz dwudziestu największych wytwórców, importerów lub dystrybutorów substancji czynnych. Uszczegółowienie powyższych danych, w tym doprecyzowanie informacji w zakresie faktycznej liczby podmiotów objętych niniejszą regulacją zostanie dokonane w treści uzasadnień do projektów rozporządzeń wykonawczych do ustawy definiujących progi istotności incydentu oraz wykazu usług kluczowych.	
Podmioty świadczące usługi kluczowe w sektorze infrastruktury cyfrowej	8	Szacunki oparte na analizie informacji rynkowych	
Dostawcy usług cyfrowych	co najmniej 25	Szacunki oparte na analizie informacji rynkowych	Dostawcy usług cyfrowych są odpowiedzialni za m.in. zapewnienie cyberbezpieczeństwa świadczonych przez nich usług cyfrowych poprzez: • podjęcie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykami, na jakie narażone są systemy informacyjne

			wykorzystywane przez nich do świadczenia usług cyfrowych, • podjęcie środków zapobiegających i minimalizujących wpływ incydentów na usługi cyfrowe, w celu zapewnienia ciągłości tych usług, • przeprowadzanie czynności umożliwiających wykrywanie, rejestrowanie analizowanie oraz klasyfikowanie incydentu, jak również zgłaszanie incydentów istotnych do właściwego CSIRT i zapewnienie obsługi incydentu.
Naukowa i Akademicka Sieć Komputerowa	1	-	Przyjęcie roli CSIRT NASK wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Agencja Bezpieczeństwa Wewnętrznego	1	-	Przyjęcie roli CSIRT GOV wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Minister Obrony Narodowej	1	-	Przyjęcie roli CSIRT MON wraz z zadaniami z zakresu cyberbezpieczeństwa określonymi w ustawie
Podmioty świadczące usługi z zakresu cyberbezpieczeństwa	Co najmniej 30 podmiotów	Analiza własna na podstawie dostępnych publicznie ofert przedsiębiorców	Spełnienie wymogów z art. 15 ust. 2 projektu ustawy
Centralna administracja rządowa	Ministerstwa (18) oraz jednostki im podległe i nadzorowane	-	Podmioty publiczne będą zobowiązane m.in. do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 23 i art. 24), zapewnienia zarządzania incydentem w podmiocie publicznym oraz zgłaszania takiego incydentu i zapewnienia jego obsługi (art. 24).
Terenowa administracja rządowa	Wojewodowie (16), ich jednostki podległe i nadzorowane, administracja zespolona i niezespolona w województwie	-	
Administracja samorządowa	Województwa (16), powiaty (314), miasta na prawach powiatu (66), gminy (2478)	Dane z GUS	
Sądy i trybunały	Sądy powszechne (318 sądów rejonowych, 45 okręgowych, 11 apelacyjnych), Naczelny Sąd Administracyjny, Sąd Najwyższy, Trybunał	Dane MS	

	Konstytucyjny, Trybunał Stanu		
Prokuratury	415 jednostek (Prokuratura Krajowa, jedenaście prokuratur regionalnych, czterdzieści pięć prokuratur okręgowych, trzysta pięćdziesiąt osiem prokuratur rejonowych)	Dane MS	
Uczelnie publiczne i PAN	132	Informacja robocza z MNiSW – 94 uczelnie publiczne nadzorowane przez MNiSW oraz 38 nadzorowanych przez innych ministrów (MZ, MON, MGMiŻŚ, MKiDN, MSWiA). Stan na dzień 21.03.2018 r.	
Narodowy Bank Polski	1	-	
Bank Gospodarstwa Krajowego	1	-	
Organy właściwe w rozumieniu ustawy. W zakresie dla operatorów usług kluczowych: Komisja Nadzoru Finansowego, minister właściwy do spraw informatyzacji, minister właściwy do spraw transportu, minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej, minister właściwy do spraw energii, minister właściwy do spraw zdrowia, minister właściwy do spraw gospodarki wodnej, Minister Obrony Narodowej.	7	-	Wykonywanie zadań określonych w art. 42–44 projektu ustawy (analiza przedsiębiorców w danym sektorze pod kątem spełniania wymogów uznania za operatora usługi kluczowej, wydawanie decyzji administracyjnych w tym zakresie, przygotowywanie rekomendacji i wytycznych z zakresu cyberbezpieczeństwa, możliwość tworzenia sektorowych zespołów cyberbezpieczeństwa).
Minister właściwy do spraw informatyzacji	1	-	Wykonywanie zadań z ustawy – art. 45 i art. 46 (możliwe upoważnienie jednostki nadzorowanej lub podległej – art. 47); prowadzenie pojedynczego punktu kontaktowego (art. 48); nadzór nad podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa prowadzenie wykazu operatorów usług kluczowych. Realizacja funkcji organu właściwego dla sektora infrastruktury cyfrowej oraz

			dostawców usług cyfrowych, z wyłączeniem tych będących we właściwości Ministra Obrony Narodowej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Przeprowadzono ustalenia z ministerstwami, które uczestniczyły w pracach międzyresortowego zespołu roboczego ds. przygotowania ustawy (skład osobowy bazował na zespole ds. opracowania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022). Przeprowadzono również konsultacje wewnątrz resortu Ministerstwa Cyfryzacji.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248), projekt ustawy został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji oraz na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny".

W ramach uzgodnień i opiniowania projektu ustawy przeprowadzono konferencję uzgodnieniową w dniu 8 grudnia 2017 r. W toku opracowywania projektu po konferencji zmieniono wiele przepisów projektu (m.in. definicje incydentów i kwestie kontroli oraz kar pieniężnych) i zmieniono załącznik od ustawy w porozumieniu z ministerstwami i urzędami odpowiedzialnymi za dane sektory gospodarki. Na wniosek niektórych resortów przygotowane zostały przepisy regulujące ustanawianie i zasady funkcjonowania sektorowych zespołów cyberbezpieczeństwa. Odbyła się dyskusja na temat uprawnień CSIRT, administrowania systemem informatycznym wspierającym obsługę incydentów, jak i kwestii nadzoru nad systemem cyberbezpieczeństwa z resortami i organami odpowiedzialnymi za działanie CSIRT (MC wysunęło propozycję powołania kolegium ds. cyberbezpieczeństwa). W konsultacjach z właściwymi CSIRT podniesiono kwestię zgodności określonych w projekcie ustawy praw i obowiązków z rozporządzeniem ogólnym o ochronie danych osobowych (rozporządzenie 2016/679, tzw. RODO). Ponadto projekt był przekazany do zaopiniowania związkom zawodowym i organizacjom pracodawców.

W dniu 31 października 2017 r. projekt został także skierowany do zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego i w dniu 13 grudnia 2017 r. został uzgodniony przez Komisję Wspólną Rządu i Samorządu Terytorialnego.

Raport z konsultacji publicznych i opiniowania projektu ustawy zawierający listą podmiotów, do których projekt został wysłany, znajduje się w załączniku nr 2 do niniejszego dokumentu.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2018 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	**3,19**	**6,82**	**6,89**	**6,89**	**6,89**	**6,89**	**6,89**	**6,89**	**6,89**	**6,89**	**6,89**	**72,02**
budżet państwa	2,08	3,12	3,12	3,12	3,12	3,12	3,12	3,12	3,12	3,12	3,12	**33,28**
JST	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**0,00**
pozostałe jednostki (oddzielnie)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**0,00**
Fundusz Ubezpieczeń Społecznych	0,78	2,63	2,68	2,68	2,68	2,68	2,68	2,68	2,68	2,68	2,68	**27,53**
Fundusz Pracy	0,13	0,41	0,42	0,42	0,42	0,42	0,42	0,42	0,42	0,42	0,42	**4,32**
Narodowy Fundusz Zdrowia	0,20	0,66	0,67	0,67	0,67	0,67	0,67	0,67	0,67	0,67	0,67	**6,89**
Wydatki ogółem	**9,08**	**17,01**	**20,78**	**20,76**	**22,35**	**22,35**	**22,35**	**22,35**	**22,35**	**22,35**	**22,35**	**224,08**
budżet państwa	9,08	17,01	20,78	20,76	22,35	22,35	22,35	22,35	22,35	22,35	22,35	**224,08**
JST	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
pozostałe jednostki (oddzielnie)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
Saldo ogółem	**-5,89**	**-10,19**	**-13,89**	**-13,87**	**-15,46**	**-15,46**	**-15,46**	**-15,46**	**-15,46**	**-15,46**	**-15,46**	**-152,06**
budżet państwa	-7,00	-13,89	-17,66	-17,64	-19,23	-19,23	-19,23	-19,23	-19,23	-19,23	-19,23	**-190,80**
JST	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**0,00**
pozostałe jednostki (oddzielnie)	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	**0,00**
Fundusz Ubezpieczeń Społecznych	0,78	2,63	2,68	2,68	2,68	2,68	2,68	2,68	2,68	2,68	2,68	**27,53**
Fundusz Pracy	0,13	0,41	0,42	0,42	0,42	0,42	0,42	0,42	0,42	0,42	0,42	**4,32**

Narodowy Fundusz Zdrowia	0,20	0,66	0,67	0,67	0,67	0,67	0,67	0,67	0,67	0,67	0,67		**6,89**

Źródła finansowania	Wydatki części 27 – Informatyzacja w kwocie łącznej ok. 167,34 mln zł, na którą składają się: 1) koszt budowy NPCnet w 2018 r. w wysokości 0,58 mln zł, 3,98 mln zł w 2019 r. oraz 2,32 mln zł w 2020 r.; 2) koszt utrzymania NPCnet od 2021 r. w wysokości 2,58 mln zł; 2) działalność CIRST NASK w 2018 r. wysokości 5,87 mln zł, 8,5 mln zł od 2019 r.; 3) podłączenie do NPCnet w 2020 wysokości 4,11 mln zł, 1,33 mln zł w 2021 oraz 2,92 mln zł od 2022 r.; 4) stworzenie 9 stanowisk pracy w wysokości ok. 9,57 mln zł, w tym: wynagrodzenie w wysokości 0,35 mln zł w 2018 r. oraz 0,70 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,03 mln zł, a od 2020 r. – 0,06 mln zł, pochodne w wysokości 0,07 mln zł w 2018 r. oraz 0,15 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,08 mln zł w 2018 r.; 5) koszt utrzymania NPC 1,5 mln zł w 2020 r., natomiast w latach kolejnych w wysokości 4 mln zł. zostaną sfinansowane w 2018 r. w ramach limitu wydatków, natomiast w kolejnych latach środki zostaną ujęte w planie finansowym. Koszt stworzenia nowych stanowisk pracy: dedykowanych do zadań w każdym z pozostałych organów właściwych: − Komisja Nadzoru Finansowego – stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r.; − minister właściwy do minister właściwy do spraw transportu - stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r.; − minister do spraw gospodarki wodnej – stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r.; − minister do spraw gospodarki morskiej – stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r.; − minister właściwy do spraw energii – stworzenie 8 stanowisk pracy w wysokości ok. 8,42 mln zł, w tym: wynagrodzenie w wysokości 0,31 mln zł w 2018 r. oraz 0,61 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,03 mln zł, a od 2020 r. – 0,06 mln zł, pochodne w wysokości 0,06 mln zł w 2018 r. oraz 0,13 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,08 mln zł w 2018 r.; − minister właściwy do spraw zdrowia – stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r.; − Minister Obrony Narodowej - stworzenie 4 stanowisk pracy w wysokości ok. 4,21 mln zł, w tym: wynagrodzenie w wysokości 0,16 mln zł w 2018 r. oraz 0,31 mln zł od 2019 r., dodatkowe wynagrodzenie roczne w 2019 r. w wysokości 0,01 mln zł, a od 2020 r. – 0,03 mln zł, pochodne w wysokości 0,03 mln zł w 2018 r. oraz 0,06 mln zł w 2019 r., koszt organizacji stanowisk pracy w wysokości 0,04 mln zł w 2018 r. Ze względu na nową formę raportowania do systemu teleinformatycznego przez prezesa UKE zakłada się utworzenie dwóch etatów. Szacowany koszt jednostkowy wyniesie ok. 8 tys. brutto

	miesięcznie, co oznacza koszt w 2018 r. 98 tys. zł brutto, w 2019 r. – 203 tys. zł, zaś od 2020 r. 212 tys. zł brutto, przy czym od 2019 r. uwzględniono również wydatki na dodatkowe wynagrodzenia, tzw. „13”. Finansowanie podmiotu odpowiedzialnego za obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową Pełnomocnika oraz obsługę Kolegium – którą ma zapewniać ministerstwo lub inny urząd administracji rządowej, w którym powołano Pełnomocnika – będzie realizowane w ramach limitu wydatków dla właściwej części budżetowej bez podstawy do ubiegania się o dodatkowe środki z budżetu na ten cel w roku bieżącym, jak i w kolejnych latach budżetowych. Celem realizacji zadań określonych w projekcie związanych z prowadzeniem Zespołu do spraw Incydentów Krytycznych, Dyrektor Rządowego Centrum Bezpieczeństwa (finansowany z cz. 42 – sprawy wewnętrzne) otrzyma środki na wyposażenie budynku RCB w niezbędny sprzęt i przystosowanie sal (szczegółowe informacje w części poniżej). Zwiększone wydatki MON związane z pełnieniem funkcji organu właściwego zostaną sfinansowane w ramach wydatków obronnych określonych w art. 7 ustawy o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych RP. Wydatki organów właściwych zostaną sfinansowane w 2018 r. w ramach limitu wydatków, natomiast w kolejnych latach środki zostaną ujęte w planie finansowym. Szczegółowe informacje wydatków, jakie generuje projektowana regulacja zawarte zostały w części „Dodatkowe informacje (…)”.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Dochody** **Wpływy z kar** Na potrzeby krajowego systemu cyberbezpieczeństwa przewiduje się wpływy do budżetu państwa z tytułu kar płaconych przez operatorów usług kluczowych (art. 73 ust. 1) oraz dostawców usług cyfrowych (art. 73 ust. 2). Założono pięć przypadków rocznie dla kar określonych w art. 73 ust. 1 pkt 4 oraz 6–9, art. 73 ust. 2 pkt 1–3 oraz art. 74 ust. 5 (łagodniejsze kary), trzy przypadki rocznie dla kar określonych w art. 73 ust. 1 pkt 2–3, 5, 10 i 13 (dotkliwsze kary), dwa przypadki rocznie kar, o których mowa w art. 73 ust. 1 pkt 11–12 i jeden przypadek na dziesięć lat sytuacji, o której mowa w art. 73 ust. 4. Zgodnie z powyższym, szacuje się dochody z kar w 2018 r. wysokości 2,08 mln zł, natomiast od 2019 r. w wysokości 3,12 mln zł rocznie. Należy w tym miejscu zaznaczyć, że dane dotyczące kar pieniężnych to szacunki, a nie cele. Należy podkreślić, że kary będą nakładane w drodze decyzji administracyjnej w następstwie naruszenia prawa, zgodnie z kodeksem postępowania administracyjnego, tym samym wyklucza to możliwość dowolności w zakresie ich nakładania. **Wpływy ze składek** W części dotyczącej dochodów uwzględniono wpływy z tytułu podatku dochodowego oraz obowiązkowych składek na ubezpieczenia zdrowotne i społeczne. Uwzględniono zarówno składki opłacane w sektorze publicznym (w wyniku utworzenia nowych stanowisk), jak i prywatnym (szacowane nowe miejsca pracy). Założono, że pracownicy organów właściwych i pojedynczego punktu kontaktowego podejmą pracę w maju 2018 r., a pracownicy podmiotów świadczących usługi z zakresu cyberbezpieczeństwa – od listopada 2018 r. Oszacowano, że wpływy ze składek mogą wynieść ok. 1,11 mln zł w 2018 r., natomiast w 2019 r. – 3,7 mln zł i latach następnych ok. 3,77 mln zł. **Wydatki** **Koszt budowy NPC i utrzymania NPC** Na potrzeby krajowego systemu cyberbezpieczeństwa powstanie system teleinformatyczny, który pozwoli na wymianę informacji o podatnościach, zagrożeniach i incydentach, jak również będzie zbierać informacje o poziomie ryzyka wystąpienia poważnego incydentu i prowadzić rejestr incydentów, w tym poważnych i krytycznych. System teleinformatyczny wesprze również agregację i korelację pozyskiwanych informacji w celu określenia: ryzyka wystąpienia incydentu, publikowania ostrzeżeń o zaistniałych incydentach, opracowania informacji o poziomie ryzyka dla RP, jak również prognozę skutków materializacji zagrożeń cyberbezpieczeństwa. Wydatki związane z budową NPC są już ponoszone w ramach umowy o wykonanie i finansowanie projektu realizowanego w ramach programu CyberSecIdent „Cyberbezpieczeństwo i eTożsamość”. Ponadto przewiduje się, że na utrzymanie systemu teleinformatycznego z budżetu państwa, części 27 – Informatyzacja, zostanie przeznaczone w 2020 r. (za okres IX–XII) 1,5 mln zł, a od

	2021 po 4 mln zł rocznie (2 mln zł na wsparcie programistyczne i rozwój deweloperski oraz 2 mln zł na serwis i koszty osobowe związane z utrzymaniem usługi). W zakresie finansowania systemu, to jest w ramach Programu CyberSecIdent, realizowanego przez NCBiR, powstanie moduł centralny systemu oraz projekt pilotażowy dla trzech wybranych podmiotów. W ramach przewidzianych środków, których źródłem będzie budżet państwa cz. 27 – Informatyzacja, przewiduje się jego rozbudowę i utrzymanie. **Koszt budowy NPCnet** Zostanie utworzona sieć szkieletowa łącząca uczestników oraz centra operacyjne Narodowej Platformy Cyberbezpieczeństwa, zbudowana z wykorzystaniem istniejących sieci telekomunikacyjnych, umożliwiająca w modelu docelowym obsłużenie do tysiąca podmiotów. Sieć NPCnet będzie uwzględniała wymagania w zakresie zapewnienia wysokiego poziomu poufności, dostępności i integralności w szczególności przez zastosowanie kryptograficznej ochrony przesyłanych informacji. Koszt budowy (w latach 2018-2020) będzie wynosił 6,88 mln zł, z czego 0,58 mln zł w 2018 r., 3,98 mln zł w 2019 r. oraz 2,32 mln zł w 2020 r. Koszt utrzymania NPCnet od 2021 r. wyniesie 2,58 mln zł rocznie. Źródłem finansowania budowy i utrzymania NPCnet będzie budżet państwa cz. 27 – Informatyzacja. **Finansowanie działalności CSIRT NASK** Działania operacyjne prowadzone są w trybie 24/7/356 i biorą w niej udział operatorzy (1 linia), analitycy (2 linia) i eksperci CERT Polska (3 linia). Dodatkowo uwzględnione są koszty zespołów wspomagających odpowiedzialnych za utrzymanie ciągłości działania infrastruktury i usług niezbędnych do realizacji tych zadań. Uwzględniono również koszty wzmocnienia laboratorium i jego obsadzenia celem wykonywania badań sprzętu i oprogramowania (art. 33 projektu) – szacuje się średnio osiem badań w skali roku. Koszty uwzględniają koszty pośrednie związane z wynagrodzeniami i kosztami pracodawcy. Działalność CSIRT NASK będzie finansowana w ramach dotacji podmiotowej (od 2019 r.) w wysokości ok. 8,5 mln zł rocznie; kwota dotacji podmiotowej zostanie uwzględniona w projekcie budżetu na rok 2019. Natomiast w 2018 r. zostaną sfinansowane w ramach środków budżetu państwa cz. 27 – Informatyzacja. **Finansowanie zadań CSIRT MON i CSIRT GOV** Zadania CSIRT MON będą finansowane w ramach wydatków obronnych określonych w art. 7 ustawy o przebudowie i modernizacji technicznej oraz finansowaniu Sił Zbrojnych RP, natomiast zadania CSIRT GOV będą finansowane z cz. 57 - Agencja Bezpieczeństwa Wewnętrznego. Nie powinny stanowić podstawy do ubiegania się o dodatkowe środki. **Wynagrodzenia dla organów właściwych i pojedynczego punktu kontaktowego** Ustawa nakłada na ministra właściwego ds. informatyzacji obowiązki sprawozdawcze wobec Komisji Europejskiej, jak również inne w sprawach tzw. transgranicznych operatorów usług kluczowych oznaczają konieczność stworzenia dodatkowych 5 stanowisk pracy w celu realizacji ww. zadań. Przewidziany koszt w 2018 r. (VII–XII) to 231 tys. zł, 2019 r. – 480 tys. zł, a od 2020 r. 500 tys. zł rocznie. W związku z realizacją przez Ministerstwo Cyfryzacji funkcji organu właściwego dla sektora infrastruktury cyfrowej i dostawców usług cyfrowych niezbędne będzie stworzenie po 4 stanowiska pracy dedykowane do ww. zadań. Przewidziany koszt w 2018 r. (VII–XII) to 186 tys. zł, 2019 r. – 388 tys. zł, a od 2020 r. 404 tys. zł rocznie. Uwzględniono także koszt stworzenia nowych stanowisk pracy dedykowanych do ww. zadań w każdym z pozostałych organów właściwych (Komisja Nadzoru Finansowego – 4 etaty, minister właściwy do spraw transportu – 4 etaty, minister właściwy do spraw gospodarki morskiej – 4 etaty, minister do spraw gospodarki wodnej – 4 etaty, minister właściwy do spraw energii – 8 etatów, minister właściwy do spraw zdrowia – 4 etaty, Minister Obrony Narodowej – 4 etaty). Przewidziany koszt w 2018 r. to 1,481 mln zł, 2019 r. – 3,088 mln zł, a od 2020 r. 3,214 mln zł rocznie. Dla niektórych organów właściwych przewidziano zwiększone środki ze względu na uzasadnione potrzeby wynikające ze specyfiki danego sektora. W ten sposób minister właściwy do spraw energii uzyska osiem stanowisk w miejsce czterech. Uzasadnieniem zwiększenia etatów jest zakres i liczba analiz niezbędnych do wykonania w ww. obszarze, który najpełniej obrazuje ilości podmiotów ujętych w stosownych bazach i rejestrach udostępnianych przez Prezesa Urzędu Regulacji Energetyki. Przykładowo rejestr przedsiębiorstw energetycznych posiadających koncesję w zakresie paliw ciekłych zawiera blisko 6500 rekordów, Rejestr przedsiębiorstw energetycznych posiadających koncesję w zakresie innym niż paliwa ciekłe zawiera ponad 3100 rekordów, wykaz operatorów systemów elektroenergetycznych obejmuje 184 podmioty, wykaz operatorów w systemie gazowym obejmuje ponad 60 podmiotów.

Ponadto analizie będą musiały zostać poddane podmioty z podsektorów „Dostawy i usługi dla sektora energii" – ich liczba na obecnym etapie prac jest trudna do oszacowania oraz „Jednostki nadzorowane i podległe" – dodatkowe 15 podmiotów. Biorąc pod uwagę wskazaną powyżej liczbę podmiotów w sektorze Energia, które będą musiały być poddane analizie pod kątem uznania ich za operatorów usługi kluczowej, a następnie ilość decyzji administracyjnych niezbędnych do wydania w tym zakresie oraz konieczność zapewnienia właściwej kontroli nad działalnością operatorów usług kluczowych, wnioskowana liczba etatów została skalkulowana na minimalnym poziomie umożliwiającym realizację zadań.

Do obliczenia ww. wydatków na wynagrodzenia przyjęto dla 1 etatu mnożnik 3,20 przy maksymalnym 20% dodatku stażowym. Ponadto od 2019 r. uwzględniono wydatki na dodatkowe wynagrodzenie, tzw. „13".

Wydatki na wynagrodzenia dla pracowników organów właściwych zostaną sfinansowane w roku 2018 w ramach określonego limitu wydatków na rok budżetowy 2018.

Koszt organizacji jednego stanowiska pracy zaopatrzonego w sprzęt IT, tj.: pakiet office On Premise, komputer stacjonarny oraz w wyposażenie wyniesie ok. 9 000,00 zł. Łącznie koszt utworzenia stanowisk pracy dla 43 etatów wyniesie ok. 387 000,00 zł.

Podłączenie do NPCnet

Dla lepszej współpracy w ramach systemu cyberbezpieczeństwa, konieczne jest podłączenie jak największej liczby podmiotów do modułu NPCnet, który pozwoli na bezpieczną i szyfrowaną wymianę informacji o zagrożeniach, podatnościach i incydentach. Planuje się podłączyć w tym celu CSIRT NASK (jako centrum operacyjne dla wymiany informacji dla podmiotów w jego właściwości) oraz UKE (celem ułatwienia współpracy UKE ze zgłaszającymi incydenty na podstawie art. 175a ustawy – Prawo telekomunikacyjne przedsiębiorcami telekomunikacyjnymi, którzy mimo iż są wyłączeni spod obowiązków określonych w dyrektywie NIS, to posiadają cenne informacje na temat incydentów w sieciach telekomunikacyjnych). Koszt podłączenia UKE wyniesie 1,31 mln zł w 2020 r. i 0,18 mln zł w 2021 r., a następnie 0,35 mln zł rocznie od 2022 r. i zostanie poniesiony z części budżetowej, której dysponentem jest minister właściwy do spraw informatyzacji. Natomiast koszt podłączenia NASK wyniesie 2,8 mln zł w 2020 r. i 1,15 mln zł w 2021 r., a następnie 2,57 mln zł rocznie od 2022 r. i zostanie poniesiony z części 27 - Informatyzacja.

Obsługa Zespołu do spraw Incydentów Krytycznych

W związku z powierzeniem nowych zadań pojawiła się konieczność zakupu nowego sprzętu przez RCB w 2018 r.

Specyfikacja niezbędnego sprzętu została ujęta w tabeli poniżej.

Element wyposażenia	Ilość	Cena jednostkowa brutto	Wartość brutto
Stacja robocza All in One/Laptop	15	4 000,00 zł	60 000,00 zł
Licencje na oprogramowanie antywirusowe	15	150,00 zł	2 250,00 zł
Licencje pakiet biurowy na stacje robocze	15	1 609,00 zł	24 135,00 zł
Server	1	31 575,00 zł	31 575,00 zł
Licencja na system operacyjny - server	2	3 149,00 zł	6 298,00 zł
Licencje dostępowe -server	40	169,00 zł	6 760,00 zł
Licencja servera poczty elektronicznej	1	3 100,00 zł	3 100,00 zł
Licencje dostępowe do servera poczty elektronicznej	20	379,00 zł	7 580,00 zł
System do zarządzania kopiami zapasowymi	1	10 000,00 zł	10 000,00 zł
			151 698,00 zł
Scianka wizyjna 4 monitory 46" + system przekazu sygnału + stelaż	1	60 000,00 zł	60 000,00 zł
Okablowanie + urządzenia sieciowe	1	30 000,00 zł	30 000,00 zł
			90 000,00 zł
Łączny szacowany koszt inwestycji			**241 698,00 zł**

Dodatkowo - w celu zabezpieczenia sprzętu na potrzeby zbierania informacji o wystąpieniu incydentu krytycznego (art. 35 ust. 4) oraz przygotowanie pomieszczenia na miejsce spotkań Zespołu do spraw Incydentów Krytycznych przy założeniu, iż zarówno system oraz pomieszczenie będzie wykorzystywane do przetwarzania informacji niejawnych należy zabezpieczyć środki finansowe na 2019 r. w kwocie odpowiednio:

1) zakup urządzeń informatycznych na stanowisko dostępowe niejawnego systemu teleinformatycznego – 60 tys. brutto (z wyłączeniem środków komunikacji elektronicznej, o których mowa w art. 36 ust. 6);
2) adaptacja sali w celu utworzenia „specjalnej strefy ochronnej" służącej do prowadzenia

	posiedzeń o charakterze niejawnym o klauzuli „Tajne” – 300 tys. brutto. **Inne uwagi dotyczące wydatków** Nie przewidziano wydatków jednostek samorządu terytorialnego (JST) i innych podmiotów realizujących zadania publiczne w rozumieniu ustawy o informatyzacji, z uwagi na fakt, że stosuje się wobec nich rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. W związku z tym każda jednostka, która wdraża usługi świadczone drogą elektroniczną powinna dołożyć należytej staranności celem zapewnienia ich bezpiecznego funkcjonowania. W procesie projektowym oraz utrzymania usług koszty te są naliczane normatywnie. Trzeba mieć także na uwadze, że podmioty realizujące zadania publiczne co do zasady mają zaimplementowany system zarządzania bezpieczeństwem informacji (SZBI) – dlatego też zadania wynikające z art. 21 ust. 3 i art. 22 projektu ustawy będą realizowane w ramach SZBI. Ewentualne zwiększone koszty Narodowego Funduszu Zdrowia wynikające z niniejszej ustawy zostaną pokryte w ramach kosztów administracyjnych, w tym wynagrodzeń, określonych w zatwierdzonym planie finansowym Funduszu na rok 2018, bez konieczności ich zwiększania.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z 2018 r.)	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych, którzy stworzyli SOC u siebie	0	27,06	12,06	12,06	12,06	12,06	135,6
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych, którzy stworzyli SOC u siebie	0	49,56	19,56	19,56	19,56	19,56	225,6
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych, którzy wykupili usługę SOC	0	19,56	19,56	19,56	19,56	19,56	195,6
	podłączenie CSIRT sektorowego do NPCnet (fakultatywne)	0	6,55	0,9	1,75	1,75	1,75	21,45
	podłączenie partnerów do NPCnet (fakultatywne)	0	5,22	2,655	3,555	3,555	3,555	36,32
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w ustawie (szczegółowy opis poniżej). Na marginesie warto zaznaczyć, że większość dużych przedsiębiorstw ma wdrożoną już część rozwiązań ustawowych. Często te rozwiązania mają charakter sektorowy – jak CERT utworzony przez Polskie Sieci Elektroenergetyczne dla sektora energetycznego czy powstający CERT dla Związku Banków Polskich.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w ustawie. W zależności od tego, czy będą to operatorzy usług kluczowych, czy podmioty świadczące usługi z zakresu cyberbezpieczeństwa, obowiązki będą się różnić – szczegółowy opis poniżej.						

	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje ustawowe przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele. Zwiększą pewność ciągłości usług. Zwiększy się kontrola nad przebiegiem potencjalnych ataków (dzięki wprowadzeniu mechanizmów komunikowania się CSIRT krajowych między sobą). Część kosztów wypełnienia obowiązków ustawowych, w przypadku niektórych sektorów, może przełożyć się na wyższy koszt usługi dla odbiorcy końcowego.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Wpływ na konkurencyjność gospodarki i przedsiębiorczość będzie różnił się w zależności od typu podmiotu (operator usług kluczowych, dostawca usług cyfrowych, podmiot świadczący usługi z zakresu cyberbezpieczeństwa) i sektora. a) **Operatorzy usług kluczowych** – zwiększenie poziomu bezpieczeństwa świadczonych usług, poprzez wprowadzenie efektywnego zarządzania systemem cyberbezpieczeństwa, objęcie ochroną przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Nałożenie na operatorów dodatkowych obowiązków związanych z zapewnieniem bezpieczeństwa ich systemów informacyjnych, ciągłości świadczonych usług. Według szacunków Ministerstwa, zostanie wyznaczonych 335 operatorów usług kluczowych. Jest to oczywiście liczba przybliżona, pozwala jednak na dokonanie wstępnych obliczeń. Zakładając, że celem realizacji obowiązków wynikających z ustawy przedsiębiorcy zaczną stosować właściwe zabezpieczenia dla swoich systemów, uznano że będzie naturalne dla przedsiębiorców, aby w ramach jednego lub kilku sektorów wymieniać się informacjami i wspólnie zwalczać zagrożenia. Tego typu podmioty już powstały dla sektora finansowego (Bankowe Centrum Cyberbezpieczeństwa, zrzeszające banki należące do Związku Banków Polskich) czy też energetycznego (CERT PSE). Według założeń Ministerstwa, utrzymanie jednego podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa będzie kosztować 2,41 mln zł rocznie. Najwięksi przedsiębiorcy będą korzystać z własnych zespołów, dostosowanych do potrzeb danego przedsiębiorcy, działających na poziomie sektorowym (por. np. działalność ZBP w tym zakresie). Uznano, że powstanie co najmniej pięć takich zespołów i oszacowano, że ich koszt roczny na jednego uczestnika wyniesie około 142 tys. zł rocznie. Inni przedsiębiorcy (mniej zależni w swej działalności od technologii) będą mogli korzystać z usług mniejszych zespołów, które mogą obsłużyć więcej podmiotów. Zakładając, że utrzymanie takiego zespołu będzie kosztować 1,956 mln zł rocznie i że przedsiębiorców tego typu będzie około 150, szacowany koszt dla operatora będzie wynosił około 130 tys. zł rocznie. Przedsiębiorcy, którzy nie będą w stanie utworzyć własnego SOC, mogą skorzystać z usług rynkowych. Zakładając, że 10 istniejących zespołów jest w stanie obsłużyć w ramach działalności komercyjnej pozostałych 298 operatorów, to szacowany koszt obsługi jednego operatora usług kluczowych będzie wynosił około 195,6 tys. zł rocznie. W zależności od przyjętego modelu realizacji obowiązków jest możliwe obniżenie tej kwoty. Projekt ustawy dopuszcza elastyczne rozwiązania, celem realizacji obowiązków. Szacunkowe wyliczenia zawarto w załączniku 2 do OSR. Operatorzy usług kluczowych będą zobowiązani m.in. ponieść koszty audytu zewnętrznego raz na dwa lata. Szacuje się, że koszt jednostkowy wykonania audytu wyniesie 50 tys. zł. Audyt po raz pierwszy będzie przeprowadzony w 2019 r., a następnie co 2 lata. a. Sektor energia, podsektor wydobywanie kopalin Podsektor tworzą podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego, węgla brunatnego i rud miedzi na podstawie koncesji. Zapewnienie ciągłości działania działalności sektora wydobywczego jest niezbędne dla zachowania ciągłości łańcucha dostaw w sektorze. b. Sektor energia, podsektor energia elektryczna Podsektor tworzą duże przedsiębiorstwa obsługujące wiele podmiotów, korzystające z systemów informacyjnych w znacznym stopniu. Wdrożenie regulacji przyczyni się do zapewnienia ciągłości dostaw prądu, zwiększy odporność przedsiębiorstw na ataki na infrastrukturę teleinformatyczną. Regulacja obejmie wytwórców energii elektrycznej, operatorów sieci przesyłowej (jest to jedna firma – Polskie Sieci Energetyczne S.A.), operatorów sieci dystrybucji: pięciu znaczących dla rynku gospodarstw domowych (Innogy Stoen Operator Sp. z o.o, PGE

	Dystrybucja S.A., ENEA Operator Sp. z o.o., Tauron Dystrybucja S.A., ENERGA – Operator S.A.), dziewięciu największych dla rynku przedsiębiorstw (m.in. dla portów morskich oraz największych przedsiębiorstw); oraz sprzedawców – według danych URE najwięksi sprzedawcy to podmioty należące do tych samych grup kapitałowych, co najwięksi dystrybutorzy. c. Sektor energia, podsektor ropa naftowa Podsektor tworzą duże przedsiębiorstwa, korzystające z systemów informacyjnych. Wdrożenie regulacji ustawowych przyczyni się do poprawy bezpieczeństwa i stworzenia systemu odpornego na ataki. Regulacja obejmie: operatora ropociągów (PERN S.A.); przedsiębiorstwa zajmujące się wydobyciem, przetwarzaniem, magazynowaniem i przesyłem ropy naftowej (Polskie Górnictwo Naftowe i Gazownictwo i LOTOS Petrobaltic S.A.) oraz rafinerie (PKN „Orlen", Grupa LOTOS S.A.). d. Sektor energia, podsektor gazu Podsektor tworzą duże przedsiębiorstwa, korzystające z systemów informacyjnych. Wdrożenie regulacji będzie miało znaczenie dla zapewnienia ciągłości dostaw do odbiorców końcowych. Regulacja obejmie przedsiębiorstwa dostarczające gaz, operatorów systemu dystrybucji (m.in. PSG sp. z o.o.), operatora systemu przesyłowego (w Polsce tą funkcję pełni Gaz-System S.A), operatorów systemu magazynowania (PGNiG, który obsługuje siedem największych magazynów gazu w Polsce), operator systemu LNG (także jest Gaz-System S.A.), a także operatora instalacji służących do rafinacji i przetwarzania gazu ziemnego (również PGNiG). Poza ww. podmiotami, objęte ustawą zostaną również podmioty prowadzące działalność gospodarczą w zakresie dostaw maszyn i urządzeń oraz świadczące usługi na rzecz sektora energii, jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane. e. Sektor transport, podsektor transport lotniczy Główne podmioty tworzące sektor skorzystają na włączeniu ich w system cyberbezpieczeństwa – zyskają ochronę przed skutkami ataków na infrastrukturę cyfrową, a także informacje na temat zagrożeń. Regulacja obejmie: czterech przewoźników lotniczych, zarządców portów lotniczych (w Polsce działa 8 bazowych dla sieci europejskiej portów w rozumieniu rozporządzenia UE 1315/2013), instytucję zapewniającą służbę żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze oraz podmioty obsługujące urządzenia pomocnicze znajdujące się w portach, których liczbę szacuje się na ok. 15. f. Sektor transport, podsektor transport kolejowy Podsektor jest zróżnicowany, jednak mające kluczowe znaczenie przedsiębiorstwa działają na rynku od lat i korzystają w znacznym stopniu z systemów informacyjnych. Włączenie ich w system cyberbezpieczeństwa przyczyni się do zwiększenia bezpieczeństwa świadczonych usług. Regulacja obejmie: zarządców infrastruktury kolejowej – głównie PKP Polskie Linie Kolejowe S.A., przedsiębiorstwa kolejowe, obsługujące zarówno transport pasażerski (Przewozy Regionalne, Koleje Mazowiecki, PKP SKM Śródmieście, PKP Intercity), jak i transport towarowy (m.in. PKP Cargo, DB Cargo Polska). Regulacja obejmie także operatorów obiektów infrastruktury usługowej, gdy tylko zostaną zidentyfikowani w rejestrze Prezesa Urzędu Transportu Kolejowego. g. Sektor transport, podsektor transport wodny Główne podmioty zyskają na włączeniu ich do systemu cyberbezpieczeństwa a bezpieczeństwo świadczonych przez nie usług będzie wyższe. Ustawa obejmie armatorów, podmioty zarządzające portami (regulacja ma na celu objąć zwłaszcza podmioty zarządzające portami morskimi w Gdańsku, Gdyni. Szczecinie, Świnoujściu, Policach, Kołobrzegu, Elblągu i Ustce), a także operatorów systemów ruchu statków.

h. Sektor transport, podsektor transport drogowy

Zadania wykonywane przez rodzaje podmiotów określone w dyrektywie są zarządzane przez administrację publiczną. Zadania w przypadku inteligentnych systemów transportowych (ITS) są często zlecane przedsiębiorstwom. Rozwiązania ustawowe wprowadzą regulacje dotyczące bezpieczeństwa systemów informacyjnych, które do tej pory były realizowane w zależności od podmiotu i cechował je brak jednolitości.

Regulacja obejmie organy administracji drogowej - Generalną Dyrekcję Dróg Krajowych i Autostrad oraz samorządy, operatorów inteligentnych systemów transportowych.

i. Sektor bankowość i infrastruktura rynków finansowych, podsektor bankowość

W dużej mierze podmioty świadczące usługi bankowe są świadome znaczenia cyberbezpieczeństwa. Podwaliny pod to położyła rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym używanym przez banki. Niniejsza regulacja obejmie przede wszystkim duże banki, a decydujące znaczenie będzie miało określenie progów kwalifikacyjnych w rozporządzeniu.

j. Sektor bankowość i infrastruktura rynków finansowych, podsektor infrastruktura rynków finansowych

Podmioty tworzące sektor to duże przedsiębiorstwa o stabilnej sytuacji rynkowej, które podobnie jak sektor bankowy objęte są stosownymi rekomendacjami Komisji Nadzoru Finansowego. Regulacja obejmie operatora systemu obrotu, czyli Giełdę Papierów Wartościowych i jej spółki zależne, oraz kontrahentów centralnych.

k. Sektor ochrony zdrowia

Sektor ochrony zdrowia w Polsce ma charakter rozproszony, a zapewnienie ciągłości działania w tym sektorze ma szczególne znaczenie dla funkcjonowania całego państwa. Sprostanie regulacjom pozwoli na zapewnienie ciągłości działania usługi zależnych od systemów informacyjnych, która ma kluczowe znaczenie dla życia i zdrowia obywateli.

Regulacja obejmie rozproszone podmioty różnego rodzaju, zarówno z sektora publicznego, jak i prywatnego. Część podmiotów może być prowadzona przez organizacje pożytku publicznego.

l. Sektor zaopatrzenia w wodę i jej dystrybucja

Sektor jest rozproszony, trudno ocenić obecny stan zabezpieczenia. Z uwagi na charakter sektora – dodatkowe koszty mogą stanowić problem, zwłaszcza gdyby miały być przerzucone na odbiorców (niechęć do zwiększenia kosztów dostaw wody i odbioru ścieków). Wdrożenie systemu cyberbezpieczeństwa pozwoli zabezpieczyć kluczową usługę z punktu widzenia życia i zdrowia obywateli.

Regulacja obejmie przedsiębiorstwa wodno-kanalizacyjne. Dostarczanie wody pitnej i odbiór ścieków to zadania własne gmin i powiatów.

m. Sektor infrastruktura cyfrowa

Podmioty tworzące sektor są świadome znaczenia cyberbezpieczeństwa. Wdrożenie regulacji ustawowych zapewni lepszą komunikację między nimi i ustandaryzowanie bezpieczeństwa sieci teleinformatycznych. Regulacja obejmie NASK (jako podmiot obsługujący Domain Name System i Top Level Domain[5]), a także podmioty obsługujące IXP – siedem największych podmiotów obsługujących powyżej dwudziestu uczestników i ruch w węźle większy niż 50 Gbps. W zakresie systemów używanych przez resort obrony narodowej, regulacja obejmie też MON.

b) **Dostawcy usług cyfrowych** – ustawa nakłada na dostawców usług cyfrowych głównie wymogi sprawozdawcze wobec właściwego CSIRT oraz uprawnienia nadzorcze *ex post* organu właściwego.

c) **Podmioty świadczące usługi z zakresu cyberbezpieczeństwa** – ustawa zwiększy zapotrzebowanie na usługi tego typu podmiotów. Nałoży na nie także obowiązki, które przyczynią się do wzrostu wiarygodności podmiotów i pozwolą na lepszą komunikację między nimi (która z kolei przyczyni się do ograniczenia rozprzestrzeniania się incydentów). Przedsiębiorcy, którzy będą chcieli świadczyć usługi z zakresu

[5)] Obecnie w Polsce nie ma podmiotu zarządzającego funkcjonalnymi domenami najwyższego poziomu (gTLD). W przypadku pojawienia się takiego podmiotu, po przekroczeniu progów określonych w uchwale Rady Ministrów, może on otrzymać decyzję o nadaniu statusu operatora usług kluczowych.

	cyberbezpieczeństwa (dla operatorów usług kluczowych), będą ponosili koszty prowadzenia takiej działalności. Według szacunków Ministerstwa, koszt utrzymania centrum operacyjnego bezpieczeństwa wyniesie zgodnego z wymogami ustawy, mogącego świadczyć usługi dla operatorów usług kluczowych, to 1,96 mln zł rocznie, przy założeniu 1,06 mln zł kosztów kadry (siedmiu operatorów I linii, dwóch analityków II linii i jednego eksperta III linii). Założono istnienie pięciu podmiotów tego typu, świadczących usługi dla operatorów usług kluczowych, którzy nie zdecydują się na utworzenie tego typu jednostek w ramach własnej działalności. Powyższe koszty mogą się różnić w zależności od wybranego wariantu działania. Podmiot może świadczyć wybrane usługi z katalogu usług cyberbezpieczeństwa. Np. same usługi z zakresu reagowania na incydenty, usługi z zakresu reagowania na incydenty i SOC, usługi audytowe itp. **Podłączenie do NPCnet** Możliwe będzie podłączenie się przedsiębiorców (zarówno operatorów usług kluczowych, jak i innych podmiotów, nieuregulowanych w niniejszym projekcie ustawy) do NPCnet celem sprawnej i bezpiecznej wymiany informacji o zagrożeniach. Decyzja o podłączeniu i wynikające z niej koszty pozostają po stronie przedsiębiorcy. Dla szacunków w niniejszym projekcie założono, że do NPCnet podłączą się podmioty, będące obecnie partnerami Narodowego Centrum Cyberbezpieczeństwa[6)], które obecnie wymieniają się informacjami w zakresie bezpieczeństwa swoich sieci i systemów. **Ocena wpływu na prywatność** Artykuł 35 rozporządzenia 2016/679 (tzw. RODO) nakłada obowiązek, w określonych okolicznościach, sporządzenia oceny wpływu regulacji na prywatność (*Privacy Impact Assessment*, PIA). Zgodnie ze stanowiskiem Grupy Roboczej Art. 29 (dalej: GR29)[7)] „do oceny wielu operacji przetwarzania, które są podobne pod względem charakteru, zakresu, kontekstu, celu i ryzyka można wykorzystać jedną ocenę skutków dla ochrony danych.”[8)] GR29 uważa, że „ocena skutków dla ochrony danych [dla poszczególnych czynności] nie jest wymagana (…) jeżeli operacja przetwarzania (…) ma podstawę prawną (…) w prawie państwa członkowskiego, które reguluje daną operację przetwarzania, oraz jeżeli oceny skutków dla ochrony danych dokonano już w związku z przyjęciem tej podstawy prawnej (art. 35 ust. 10), chyba że państwo członkowskie uznało za niezbędne dokonanie oceny skutków dla ochrony danych przed rozpoczęciem czynności przetwarzania”. W toku prac nad ustawą przygotowano wstępne materiały do sporządzenia PIA, jednak po ich analizie uznano, że system wymiany informacji o incydentach będzie co prawda obejmował duże zbiory danych, jednak ze względu na zastosowane zabezpieczenia, wąską grupę odbiorców danych osobowych (analitycy i eksperci z CSIRT) oraz uboczny charakter danych osobowych w procesie obsługi incydentu, ryzyko naruszenia praw i wolności osób prywatnych podczas przetwarzania tych danych nie jest znaczne. Ponadto przetwarzane dane gromadzi się na podstawie ustawy, a nie zgód osób, których dane dotyczą. Przy zachowaniu odpowiedniej staranności oraz standardów bezpieczeństwa ryzyko wpływu na prywatność nie będzie znaczne. Obowiązki CSIRT regulują przepisy, które mają na celu modyfikację ryzyka. Dalsze regulowanie ochrony danych na poziomie ustawy (np. poprzez szczegółowe rozwiązania techniczne, warunki przechowywania danych, szczegółowe zasady i procedury dotyczące komunikacji) wydaje się nieproporcjonalne. Odstąpienie od oceny wpływu na prywatność na poziomie ustawy nie oznacza, że poszczególni przedsiębiorcy czy CSIRT nie będą musieli jej przeprowadzić dla własnej organizacji, w drodze wewnętrznej regulacji, biorąc pod uwagę lokalne uwarunkowania, charakter działalności, typy przetwarzanych danych oraz sposoby zabezpieczenia przedmiotowych danych.

[6)] Obecnie jest to 45 podmiotów (stan na dzień 09 lutego 2018 r.).

[7)] Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania Grupy zostały określone w przepisach art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

[8)] Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679*, Bruksela 2017.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu	
☐ nie dotyczy	
Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Komentarz:

Realizacja zamierzeń ustawy wymaga wykonywania przez przedsiębiorstwa obowiązków, takich jak ochrona swoich systemów informacyjnych, zapewnianie cyberbezpieczeństwa i monitorowanie świadczonych usług kluczowych, zorganizowanie ścisłej współpracy z CSIRT i odpowiednimi urzędami, w tym wymiana informacji dotyczącej incydentów; analiza, dokumentacja, rejestracja, naprawianie, usuwanie przyczyn, objęcie ochroną usługi kluczowe i prognozowanie skutków materializacji zagrożeń cyberbezpieczeństwa oraz informowanie użytkownika usług kluczowych o możliwych zagrożeniach.

Projekt ustawy nakłada obowiązki dla przedsiębiorców, którzy zostaną zidentyfikowani jako operatorzy usług kluczowych i/lub dostawy usług cyfrowych – spełnienie wymogów z art. 10-16 projektu ustawy.

Operatorzy usług kluczowych będą zobowiązani m.in. do:

- wdrożenia systemu zarządzania bezpieczeństwem (art. 10),
- przygotowania dokumentacji z zakresu cyberbezpieczeństwa (art. 10),
- identyfikowania, rejestrowania oraz klasyfikowania incydentu, jak również zapewnienia obsługi incydentu i zgłaszania incydentu poważnego do właściwego CSIRT (art. 11),
- wyznaczenia osoby kontaktowej w sprawach cyberbezpieczeństwa świadczonych usług kluczowych,
- zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa (art. 14).

Dostawcy usług cyfrowych są odpowiedzialni za m.in. zapewnienie cyberbezpieczeństwa świadczonych przez nich usług cyfrowych poprzez:

- określenie i podjęcie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych w celu zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług cyfrowych,
- podjęcie środków zapobiegających i minimalizujących wpływ incydentów dotyczących bezpieczeństwa ich systemów informacyjnych na usługi cyfrowe, w celu zapewnienia ciągłości tych usług,
- informowanie CSIRT o incydencie istotnym (w tym transgranicznym),
- identyfikowanie, rejestrowanie i klasyfikowanie incydentu, jak również zgłaszanie incydentów istotnych i zapewnienie obsługi incydentu.

9. Wpływ na rynek pracy

Z najnowszego raportu firmy analitycznej IDC wynika, że wartość sektora zajmującego się cyberbezpieczeństwem w ciągu roku wzrosła o ponad 7 proc., w związku z tym polski rynek rozwiązań bezpieczeństwa IT rozwija się niezwykle dynamicznie i nowi eksperci będą pojawiać się na rynku. Rosnący popyt będzie napędzany w znacznej mierze przez inwestycje ze strony sektora publicznego i prywatnego. Wzrośnie zapotrzebowanie w szczególności na specjalistów w dziedzinie bezpieczeństwa IT/ICT oraz specjalistów bezpieczeństwa przy systemach Operational Technology (np. SCADA).

Ustawa usankcjonuje utworzenie u operatora usługi kluczowej stanowiska ds. cyberbezpieczeństwa oraz wpłynie na certyfikację tego typu kompetencji. Ponadto ustawa umożliwi rozwój przedsiębiorstw zajmujących się ochroną systemów informacyjnych.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☒ zdrowie

Omówienie wpływu	Projekt spełnia wymagania interoperacyjności, czyli zdolność systemów teleinformatycznych do efektywnej współpracy w celu zapewnienia wzajemnego dostępu użytkowników do usług świadczonych w tych sieciach. Zakresem ustawy będą również objęte najważniejsze podmioty w ochronie zdrowia, co przyczyni się do poprawy ciągłości działania użytkowanych systemów teleinformatycznych służących świadczeniu usług kluczowych w tym sektorze.

11. Planowane wykonanie przepisów aktu prawnego

Celem zapewnienia niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do ich świadczenia założeniem projektodawcy jest po pierwsze stworzenie przepisów i procedur służących zapewnieniu cyberbezpieczeństwa w podmiotach zobowiązanych, czyli u operatorów usług kluczowych oraz struktur i rozwiązań systemowych odpowiedzialnych za zarządzanie cyberbezpieczeństwem w skali kraju. Ostatnim elementem projektu ustawy jest uruchomienie systemu teleinformatycznego umożliwiającego zbieranie informacji od podmiotów zobowiązanych i zarządzanie krajowym systemem cyberbezpieczeństwa.

W pierwszej kolejności zostaną przyjęte przez organy właściwe rekomendacje sektorowe w zakresie wzmocnienia cyberbezpieczeństwa. Rekomendacje powinny zawierać wytyczne sektorowe dotyczące rejestracji/zgłaszania, incydentów do krajowym systemie cyberbezpieczeństwa. Powyższe umożliwi określenie w wymiarze sektorowym elementów systemu zarządzania bezpieczeństwem, do których zobowiązani są operatorzy usług kluczowych na podstawie art. 9 projektu ustawy. W pracach mogą zostać wykorzystane dotychczasowe dobre praktyki w tym zakresie, a więc Rekomendacja D[9)] dotycząca zarządzania ryzykiem towarzyszącym systemom informatycznym i telekomunikacyjnym używanym przez banki, przepisy rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych*[10)], wymagania bezpieczeństwa teleinformatycznego odnoszące się do sfery infrastruktury krytycznej[11)]. Forma prawna, jakimi są rekomendacje, zapewnia neutralność technologiczną wobec zmian środowiska normalizacyjnego z zakresu zarządzania bezpieczeństwem informacji, z drugiej strony będzie zbieżna z innymi regulacjami ze sfery cyberbezpieczeństwa, a więc np. ustawy z dnia 5 września 2016 r. *o usługach zaufania i identyfikacji elektronicznej* – art. 39[12)]. Uzupełnieniem wymagań sektorowych będą przepisy decyzji wykonawczej Komisji Europejskiej odnoszące się do dostawców cyfrowych. Częścią prac sektorowych jest zainicjowanie przez ministra właściwego do spraw informatyzacji prac nad ustaleniem progów istotności skutku zakłócającego dla świadczenia usług kluczowych pozwalających na uznanie usługi za usługę kluczową. Prace nad progami winny być zakończone przed 1 lipca 2018 r., tak aby możliwe było zidentyfikowanie przez organy właściwe operatorów usług kluczowych. W ramach prac sektorowych opracowywane będą również przepisy rozporządzenia Rady Ministrów odnoszące się do zakresu informacji, które powinny zawierać dokumentację cyberbezpieczeństwa.

Równocześnie z pracami dotyczącymi sektorów będą prowadzone prace nad nowymi rozwiązaniami systemowymi i strukturami zajmującymi się cyberbezpieczeństwem na poziomie technicznym oraz zainicjowaniem działań przez pojedynczy punkt kontaktowy. Zgodnie z przepisami ustawowymi rolę pojedynczego punktu kontaktowego ds. cyberbezpieczeństwa będzie pełnić minister właściwy ds. informatyzacji.

Ostatnim elementem projektu ustawy jest uruchomienie ustawowych zadań zespołów realizujących zadania CSIRT poziomu krajowego oraz systemu teleinformatycznego wspierającego realizację zadań przez podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa. Z drugiej strony przewidziane jest uruchomienie systemu teleinformatycznego, który zapewni realizację funkcji narodowego centrum cyberbezpieczeństwa. Projekt ustawy zakłada uruchomienie z dniem 1 września 2020 r. systemu teleinformatycznego wspierającego realizację zadań podmiotów krajowego systemu cyberbezpieczeństwa, w szczególności umożliwiającego:

1) zgłaszanie i obsługę incydentów,
2) szacowanie ryzyka teleinformatycznego,
3) ostrzeganie o zagrożeniach cyberbezpieczeństwa.

---

9) Wydana przez Komisję Nadzoru Finansowego w styczniu 2013r., na podstawie art. 137 pkt 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376 j.t. z późn. zm.).

10) Dz. U. z 2012 r. Nr 526 z późn. zm.

11) Zawarte w załączniku nr 1 do Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), przyjmowanego na podstawie ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 j.t.).

12) Dz. U. z 2016 r. poz. 1579.

Celem zminimalizowani obciążeń dla operatorów usług kluczowych, projekt ustawy przewiduje, że w przypadku gdy operator usługi kluczowej jest równocześnie właścicielem, posiadaczem samoistnym i zależnym obiektów, instalacji lub urządzeń infrastruktury krytycznej i posiada plan ochrony infrastruktury krytycznej, o którym mowa w art. 6 ust. 5 ustawy o zarządzaniu kryzysowym, nie jest on zobowiązany do przygotowania dodatkowej dokumentacji dotyczącej cyberbezpieczeństwa systemów wykorzystywanych do świadczenia usług kluczowych, zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 10 ust. 5 projektowanej ustawy. Jednakże uwzględnia on informacje z zakresu cyberbezpieczeństwa w swoim planie ochrony infrastruktury krytycznej.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

1. Zgodność z ustawą. Częstotliwość pomiaru: 1 / 2 lata od wejścia ustawy w życie. Źródło pomiaru: wyniki audytów.
2. Jakość zabezpieczeń. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: raporty CSIRT, ćwiczenia.
3. Skuteczność zarządzania incydentami. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: czas od momentu zaistnienia zdarzenia do czasu jego wykrycia w systemie.
4. Przegląd poważnych incydentów. Częstotliwość pomiaru: 2 / rok od wejścia ustawy w życie. Źródło pomiarów: rejestr poważnych incydentów (w tym ilość zgłaszających, ilość poważnych incydentów, ilość operatorów usług kluczowych).
5. Dostępność usług świadczonych przez operatorów usług kluczowych. Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: dziennik awarii systemów informacyjnych służących do świadczenia usług kluczowych.
6. Zwiększenie świadomości: Częstotliwość pomiaru: 1 / rok od wejścia ustawy w życie. Źródło pomiaru: plany szkoleń i przeprowadzone kampanie społeczne.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Załącznik 1. Obliczenia dotyczące wariantów finansowania SOC u operatorów usług kluczowych

Załącznik 2. Raport z konsultacji publicznych i opiniowania projektu ustawy wraz załączonymi tabelami zawierającymi odniesienie się projektodawcy do uwag zgłoszonych w ramach opiniowania i konsultacji publicznych

Załącznik nr 1 do OSR

Koszty osobowe SOC							
Typ stanowiska	Koszt miesięczny	Wariant 1 (mały SOC)			Wariant 2		
		FTE	Typ pracy	Roczny budżet	FTE	Stanowisko	Roczny budżet
Operator I linii	8 000,00	7	dyżur (24h)	672 000,00	9	dyżur (24h)	864 000,00
Analityk II linii	10 000,00	2	stanowisko (8h)	240 000,00	3	"na zakładkę" (08.00-20.00)	360 000,00
Ekspert III lini	12 000,00	1	stanowisko (8h)	144 000,00	2	stanowisko (8h)	288 000,00
SUMA		10		1 056 000,00	14		1 512 000,00

Koszty administracji SOC są wliczone w koszty osobowe.

Pozostałe nakłady:	
Licencje (narzędzie do zbierania i korelowania incydentów, procesy wsparciowe realizowane ręcznie lub open source np. obsługa procesu zarządzania incydentami, pomiary SLA itd.)	2 000 000,00
Sprzęt (macierze i sprzęt serwerowy - wyłącznie do obsługi SOC)	1 000 000,00
Koszty utrzymania infrastruktury rocznie	30%
	900 000,00

Łączny koszt SOC (koszty osobowe i pozostałe nakłady)	
Koszt wariantu 1:	1 956 000,00
Koszt wariantu 2:	2 412 000,00