Warszawa, dnia 11 sierpnia 2020 r.

Poz. 1369

OBWIESZCZENIE
MARSZAŁKA SEJMU RZECZYPOSPOLITEJ POLSKIEJ

z dnia 22 lipca 2020 r.

w sprawie ogłoszenia jednolitego tekstu ustawy o krajowym systemie cyberbezpieczeństwa

1. Na podstawie art. 16 ust. 1 zdanie pierwsze ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461) ogłasza się w załączniku do niniejszego obwieszczenia jednolity tekst ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), z uwzględnieniem zmian wprowadzonych:

1) ustawą z dnia 11 września 2019 r. – Przepisy wprowadzające ustawę – Prawo zamówień publicznych (Dz. U. poz. 2020),

2) ustawą z dnia 16 października 2019 r. o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw (Dz. U. poz. 2248),

3) ustawą z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 695),

4) ustawą z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 875)

oraz zmian wynikających z przepisów ogłoszonych przed dniem 22 lipca 2020 r.

2. Podany w załączniku do niniejszego obwieszczenia jednolity tekst ustawy nie obejmuje:

1) art. 77–82 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), które stanowią:

„Art. 77. W ustawie z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2018 r. poz. 1457) 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. 78. W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2018 r. poz. 762, 810, 1090, 1467 i 1544) wprowadza się następujące zmiany:

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

„10) bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym;”;

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

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

Art. 79. W ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920, z późn. zm.[a)]) po art. 32a dodaje się art. 32aa w brzmieniu:

„Art. 32aa. 1. W celu zapobiegania i przeciwdziałania oraz zwalczania zdarzeń o charakterze terrorystycznym dotyczących istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli, posiadaczy samoistnych i posiadaczy zależnych obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, lub danych przetwarzanych w tych systemach oraz zapobiegania i wykrywania przestępstw o charakterze terrorystycznym w tym obszarze oraz ścigania ich sprawców, ABW wdraża w tych podmiotach system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, zwany dalej „systemem ostrzegania”, prowadzi go i koordynuje jego funkcjonowanie.

2. Wdrożenie elementów systemu ostrzegania w podmiotach, o których mowa w ust. 1, następuje zgodnie z rocznym planem wdrożenia, opracowywanym przez Szefa ABW w terminie do dnia 30 września roku poprzedzającego. W uzasadnionych przypadkach, na wniosek podmiotu, wdrożenie elementów systemu ostrzegania może zostać przeprowadzone z pominięciem planu.

3. ABW niezwłocznie informuje podmiot, o którym mowa w ust. 1, o jego włączeniu do rocznego planu wdrożenia systemu ostrzegania.

4. Podmiot, o którym mowa w ust. 1, ma obowiązek przystąpić do systemu ostrzegania oraz przekazać ABW niezbędne informacje umożliwiające wdrożenie systemu ostrzegania w tym podmiocie.

5. W podmiotach, o których mowa w ust. 1, podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych, wdrożenie systemu ostrzegania może nastąpić za zgodą Ministra Obrony Narodowej.

6. Koszty wdrożenia i utrzymania systemu ostrzegania w podmiotach, o których mowa w ust. 1, pokrywa ABW.

7. ABW, w drodze porozumienia, uzgadnia z podmiotem, o którym mowa w ust. 1, techniczne aspekty uczestnictwa w systemie ostrzegania oraz model konfiguracji systemu.

8. W sytuacji braku możliwości zawarcia porozumienia, o którym mowa w ust. 7, z przyczyn leżących po stronie podmiotu, o którym mowa w ust. 1, ABW informuje podmiot go nadzorujący lub ministra właściwego do spraw informatyzacji.

9. Prezes Rady Ministrów określi, w drodze rozporządzenia, warunki i tryb prowadzenia, koordynacji i wdrażania systemu ostrzegania, w szczególności określi czynności niezbędne do jego uruchomienia i utrzymania oraz wzór porozumienia, o którym mowa w ust. 7, kierując się potrzebą zapewnienia bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa.”.

Art. 80. W ustawie z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018) w art. 89 w ust. 1 pkt 7d otrzymuje brzmienie:

„7d) jej przyjęcie naruszałoby bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, w tym bezpieczeństwo podmiotów 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 (Dz. U. z 2018 r. poz. 1401), a tego bezpieczeństwa lub interesu nie można zagwarantować w inny sposób;”.

[a)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2017 r. poz. 2405 oraz z 2018 r. poz. 138, 650, 723, 730 i 1544.

Art. 81. 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, 650 i 1118) 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 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), 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. Przekazanie, o którym mowa w ust. 1a, następuje 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 5 lipca 2018 r. 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. 82. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401) 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 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560), 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. 10 ust. 5 ustawy z dnia 5 lipca 2018 r. 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. 36 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”.”;

2) art. 109 ustawy z dnia 11 września 2019 r. – Przepisy wprowadzające ustawę – Prawo zamówień publicznych (Dz. U. poz. 2020), który stanowi:

„Art. 109. Ustawa wchodzi w życie z dniem 1 stycznia 2021 r., z wyjątkiem:

1) art. 85 pkt 5, który wchodzi w życie po upływie 14 dni od dnia ogłoszenia;

2) art. 88, który wchodzi w życie z dniem 1 marca 2020 r.”;

3) art. 7 ustawy z dnia 16 października 2019 r. o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw (Dz. U. poz. 2248), który stanowi:

„Art. 7. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem:

1) art. 2, który wchodzi w życie z dniem następującym po dniu ogłoszenia;

2) art. 4, który wchodzi w życie z dniem 1 stycznia 2020 r.”;

4) art. 118 ustawy z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 695), który stanowi:

„Art. 118. Ustawa wchodzi w życie z dniem następującym po dniu ogłoszenia, z wyjątkiem:

1) art. 22, który wchodzi w życie z mocą od dnia 13 marca 2020 r.;

2) art. 28, który wchodzi w życie z dniem 1 lipca 2020 r.;

3) art. 53 pkt 8 w zakresie dodawanego art. 67c – który wchodzi w życie z mocą od dnia 31 marca 2020 r.;

4) art. 73 pkt 45, który wchodzi w życie z mocą od dnia 13 kwietnia 2020 r.;

5) art. 73 pkt 57 w zakresie dodawanego art. 15zzzzm – który wchodzi w życie z mocą od dnia 12 marca 2020 r.;

6) art. 73 pkt 20, 38, 39 i 41, które wchodzą w życie z mocą od dnia 1 kwietnia 2020 r.;

7) art. 73 pkt 68 w zakresie dodawanego art. $31zy^{6}$ – który wchodzi w życie z mocą od dnia 14 marca 2020 r.”;

5) art. 71 i art. 76 ustawy z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 875), które stanowią:

„Art. 71. 1. Przepisy art. 14 pkt 8 i 9 oraz art. 36 stosuje się do ogłoszonych przed dniem wejścia w życie niniejszej ustawy przetargów, konkursów i aukcji.

2. W przypadku gdy w ogłoszonym przetargu, konkursie lub aukcji przed dniem wejścia w życie niniejszej ustawy zostały złożone oferty Prezes Urzędu Komunikacji Elektronicznej:

1) zwraca niezwłocznie złożone oferty uczestnikom;

2) wpłacone przez uczestników przetargu albo aukcji wadium zwraca w terminie 21 dni od dnia unieważnienia przetargu albo aukcji z przyczyny, o której mowa w art. 118d ust. 1a ustawy zmienianej w art. 14 w brzmieniu nadanym niniejszą ustawą.”

„Art. 76. Ustawa wchodzi w życie z dniem następującym po dniu ogłoszenia, z wyjątkiem:

1) art. 1, art. 2, art. 8, art. 46 pkt 47 w zakresie dodawanego art. 31zzg, oraz art. 63–65, które wchodzą w życie po upływie 14 dni od dnia ogłoszenia;

2) art. 7 w zakresie art. 12a ust. 4, art. 27 w zakresie art. 72a ust. 1, oraz art. 30 w zakresie 139b ust. 1, które wchodzą w życie z dniem ogłoszenia z mocą od dnia 30 kwietnia 2020 r.;

3) art. 10:

a) pkt 1 i 2, które wchodzą w życie po upływie 12 miesięcy od dnia ogłoszenia,

b) pkt 3, który wchodzi w życie z dniem 1 stycznia 2021 r.;

4) art. 14 pkt 1–7 i 12, które wchodzą w życie z dniem 21 grudnia 2020 r.;

5) art. 9, art. 16, art. 18 oraz art. 72, które wchodzą w życie z dniem 1 lipca 2020 r.;

6) art. 29 pkt 7, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 13 marca 2020 r.;

7) art. 33, który wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem pkt 1 w zakresie art. 4b ust. 5, który wchodzi w życie z dniem 1 stycznia 2021 r.;

8) art. 46:

   a) pkt 1 i 2, które wchodzą w życie z dniem 25 maja 2020 r.,

   b) pkt 3:

      – w zakresie art. 4d, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 1 kwietnia 2020 r.,

      – w zakresie art. 4e, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 8 marca 2020 r.,

   c) pkt 19, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 1 maja 2020 r.,

   d) pkt 31, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 1 kwietnia 2020 r.,

   e) pkt 36, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 7 marca 2020 r.;

9) art. 58, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 1 kwietnia 2020 r.;

10) art. 59, który wchodzi w życie z dniem ogłoszenia z mocą od dnia 18 kwietnia 2020 r.”.

Marszałek Sejmu: *E. Witek*

Załącznik do obwieszczenia Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 22 lipca 2020 r. (poz. 1369)

USTAWA

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1)]

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 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875), 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 lub Szefa Agencji Wywiadu.

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

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

3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;

4) cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

5) incydent – 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. 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 (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;

[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).

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 i ograniczenie skutków incydentu;

11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa;

12) ryzyko – kombinację 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 art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568 i 695), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;

15) usługa cyfrowa – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), wymienioną w załączniku nr 2 do ustawy;

16) usługa kluczowa – usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych;

17) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę wystąpienia incydentu;

18) zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań między incydentami, usuwanie przyczyn ich wystąpienia oraz opracowywanie wniosków wynikających z obsługi incydentu;

19) 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, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2019 r. poz. 869, z późn. zm.[2)]);

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 art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2019 r. poz. 712 i 2020);

---

2) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2019 r. poz. 1622, 1649, 2020 i 2473 oraz z 2020 r. poz. 284, 374, 568, 695 i 1175.

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 do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

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

1) podmiot świadczy usługę kluczową;

2) świadczenie tej usługi 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 do spraw cyberbezpieczeństwa w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy ten podmiot został uznany w tych państwach 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 2020 r. poz. 256 i 695).

6. W stosunku do podmiotu, który przestał spełniać warunki, o których mowa w ust. 1 i 2, organ właściwy do spraw cyberbezpieczeństwa 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, wymienionych 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 mógłby mieć incydent, ze względu na jego skalę i czas trwania, na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne,

   d) udział podmiotu świadczącego usługę kluczową w rynku,

   e) zasięg geograficzny obszaru, którego mógłby dotyczyć incydent,

   f) zdolność podmiotu do 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 lub 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 określającą, 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 do spraw cyberbezpieczeństwa złożony niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1–9.

4. Zmiana danych w wykazie operatorów usług kluczowych następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa, 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 do spraw cyberbezpieczeństwa;
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;
12) Służbie Ochrony Państwa.

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 tym ryzykiem;
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 zapewniających 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 na ten temat na swojej stronie internetowej;
3) przekazuje organowi właściwemu do spraw cyberbezpieczeństwa dane, 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 oraz 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 tych 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 2020 r. poz. 164).

4. Operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych 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 2019 r. poz. 1398 oraz z 2020 r. poz. 148, 284, 374 i 695), 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 jego 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 go 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 temu zespołowi w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4;

2) współdziała z tym zespołem na poziomie sektora lub podsektora 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, uwzględniając:

1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej,

2) czas oddziaływania incydentu na świadczoną usługę kluczową,

3) zasięg geograficzny obszaru, którego dotyczy incydent,

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

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

Art. 12. 1. Zgłoszenie, 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 oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;

3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;

4) opis wpływu incydentu poważnego na świadczenie usługi kluczowej, 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 obszaru, którego dotyczy incydent poważny,

   e) wpływ incydentu poważnego na świadczenie usługi kluczowej 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 świadczenie usługi kluczowej, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;

7) informacje o podjętych działaniach zapobiegawczych;

8) informacje o podjętych działaniach naprawczych;

9) inne istotne informacje.

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

3. Operator usługi kluczowej przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz sektorowego zespołu cyberbezpieczeństwa.

4. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz 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 temu zespołowi, w postaci elektronicznej, informacje, o których mowa w ust. 1.

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 i 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 o świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz o rozwiązaniu umowy w terminie 14 dni od dnia 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 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zwanego dalej „audytem”.

2. Audyt może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544 oraz z 2020 r. poz. 1086), 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 w ciągu ostatnich 3 lat przed dniem rozpoczęcia audytu 3 audytów 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. z 2020 r. poz. 224);

5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2020 r. poz. 1200).

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 audytu przez 2 lata.

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 posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych 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 3 miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej;

2) art. 8 pkt 2, 3, 5 i 6 oraz art. 10 ust. 1–3 – w terminie 6 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, z wyjątkiem mikroprzedsiębiorców i małych przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2019 r. poz. 1292 i 1495 oraz z 2020 r. poz. 424 i 1086). Rodzaje usług cyfrowych określa załącznik nr 2 do ustawy.

2. Dostawca usługi cyfrowej podejmuje właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają 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 obszaru, którego dotyczy incydent;

4) zakres zakłócenia funkcjonowania usługi;

5) zakres 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 go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 19. 1. Zgłoszenie, 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 oraz adres poczty elektronicznej osoby składającej zgłoszenie;

3) imię i nazwisko, numer telefonu oraz 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 istotny miał wpływ,

   b) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania,

   c) zasięg geograficzny obszaru, którego dotyczy incydent istotny,

   d) zakres zakłócenia funkcjonowania usługi cyfrowej,

   e) zakres wpływu incydentu istotnego na działalność gospodarczą i społeczną;

5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent istotny 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 dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu istotnego.

3. Dostawca usługi cyfrowej przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 18 ust. 1 pkt 4, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

4. Właściwy 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 ich 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, obejmujące imię i nazwisko, numer telefonu oraz 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 go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

Art. 23. 1. Zgłoszenie, 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 oraz adres poczty elektronicznej osoby składającej zgłoszenie;

3) imię i nazwisko, numer telefonu oraz 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 obszaru, 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 dokonywania 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 art. 22 ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

4. Właściwy 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 ich 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 z której świadczeniem 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 posiadaczy zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych 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 urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, zwanych dalej „rekomendacjami dotyczącymi stosowania urządzeń informatycznych 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, dotyczącej 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, z 2002 r. poz. 1571 oraz z 2020 r. poz. 374 i 568) 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 art. 1 ust. 2 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 prowadzących 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 17.12.2011, 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 którym 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 w dzienniku urzędowym odpowiednio Ministra Obrony Narodowej, Ministra Cyfryzacji lub 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 2019 r. poz. 796).

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 2019 r. poz. 687).

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 albo 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 dokonania 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, incydentu 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, mogą 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 urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie urządzenia informatycznego lub oprogramowania, informuje pozostałe CSIRT o fakcie podjęcia badań oraz urządzeniu informatycznym lub oprogramowaniu, którego badanie dotyczy.

3. CSIRT MON, CSIRT NASK lub CSIRT GOV w przypadku identyfikacji podatności, o której mowa w ust. 1, składa wniosek w sprawie rekomendacji, o których mowa w ust. 4.

4. Pełnomocnik po uzyskaniu opinii Kolegium wydaje, zmienia lub odwołuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

4a.[3)] W przypadku uzyskania przez Pełnomocnika informacji o zagrożeniu cyberbezpieczeństwa, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, Pełnomocnik może wydać rekomendacje, o których mowa w ust. 4, z urzędu.

4b.[3)] Przed wydaniem rekomendacji w trybie ust. 4a, Pełnomocnik przeprowadza konsultację z CSIRT MON, CSIRT NASK lub CSIRT GOV.

5. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, nie później niż w terminie 7 dni od dnia otrzymania rekomendacji.

6. Pełnomocnik odnosi się do zastrzeżeń otrzymanych w trybie ust. 5 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania, i podtrzymuje rekomendacje dotyczące stosowania urządzeń informatycznych lub oprogramowania albo wydaje zmienione rekomendacje.

7. Podmiot krajowego systemu cyberbezpieczeństwa informuje Pełnomocnika, na jego wniosek, o sposobie i zakresie uwzględnienia rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania.

8. Nieuwzględnienie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania stanowi podstawę do wystąpienia przez Pełnomocnika do organu sprawującego nadzór nad podmiotem, o którym mowa w ust. 7, z informacją o ich nieuwzględnieniu.

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 ochrony danych osobowych, współpracują z organem właściwym do spraw ochrony danych osobowych.

[3)] Dodany przez art. 83 ustawy z dnia 11 września 2019 r. – Przepisy wprowadzające ustawę – Prawo zamówień publicznych (Dz. U. poz. 2020), która wejdzie w życie z dniem 1 stycznia 2021 r.

Art. 35. 1. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym oraz informują o nim Rządowe Centrum Bezpieczeństwa.

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 obszaru, 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, zwanego dalej „Zespołem".

4. W przypadku uzyskania informacji o zagrożeniach cyberbezpieczeństwa CSIRT MON, CSIRT NASK i CSIRT GOV mogą informować się wzajemnie oraz informować o tych zagrożeniach 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, incydentach krytycznych 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 ani przepisów o ochronie danych osobowych.

Art. 36. 1. Zespół jest organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym 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 realizującego 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 do spraw cyberbezpieczeństwa 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. 1, 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. 1;
2) określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 1;
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 2019 r. poz. 1429 oraz z 2020 r. poz. 695).

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 do spraw cyberbezpieczeństwa 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 których mowa w ust. 2 i 3, nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani 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, 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) 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. Urz. 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 osobowe 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 art. 2 pkt 43 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 do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 15 i ust. 5–8 oraz art. 44 ust. 1–3.

6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 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 przekazywać sobie wzajemnie dane, 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, o których mowa w ust. 3, nie wymaga realizacji obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz 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, 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 swoich stronach internetowych:

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

2) cele przetwarzania i podstawę prawną przetwarzania;

3) kategorie przetwarzanych danych osobowych;

4) informacje o odbiorcach danych osobowych;

5) informacje o tym, przez jaki okres 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 informacje, 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 obowiązane 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, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacje dotyczące 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, ani nie spełnia wymagań określonych w rozporządzeniu wykonawczym 2018/151, organ właściwy do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa z podmiotami, o których mowa w ust. 3.

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

6. Komunikat o zawarciu porozumienia ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. 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 do spraw cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych.

8. Rekomendacje dotyczące działań mających 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, wspólnych specyfikacji technicznych, 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, zmieniającego 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 uchylającego 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) oraz wytycznych Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) w tym zakresie.

Art. 43. 1. Organ właściwy do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa może, bez wszczynania kontroli, wystąpić do operatora usługi kluczowej o udzielenie informacji, które umożliwią 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 właściwy do spraw cyberbezpieczeństwa, występując do podmiotu, o którym mowa w załączniku nr 1 do ustawy, lub operatora usługi kluczowej 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, o którym mowa w załączniku nr 1 do ustawy, lub operator usługi kluczowej, do których organ właściwy do spraw cyberbezpieczeństwa skierował wystąpienie, mogą przekazać informacje w sprawie, której dotyczy wystąpienie, lub poinformować o odmowie udzielenia informacji.

5. Wystąpienie o udzielenie informacji oraz brak udzielenia informacji 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 ani 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 opracowywanie 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, zwanej dalej „Strategią", 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 ust. 1 i art. 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 jednostkom, o których 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 do spraw cyberbezpieczeństwa 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 ust. 1 pkt 3;

2) dobre praktyki, o których mowa w art. 45 ust. 1 pkt 4, związane ze zgłaszaniem incydentów;

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. Dane przekazywane Grupie Współpracy nie obejmują informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego.

3. Pojedynczy Punkt Kontaktowy przekazuje organom właściwym do spraw cyberbezpieczeństwa, 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 o:

   a) wyznaczonych organach właściwych do spraw cyberbezpieczeństwa, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,

   b) przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa;

2) co 2 lata informacje umożliwiające ocenę wdrażania 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 (Dz. Urz. UE L 194 z 19.07.2016, str. 1), obejmujące w szczególności:

   a) środki umożliwiające identyfikację operatorów usług kluczowych,

b) wykaz usług kluczowych,

c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym sektorze, o którym 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 Rzeczypospolitej Polskiej;

5) kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego;

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. 14 ust. 2;

2) organy właściwe do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa lub minister właściwy do spraw informatyzacji prowadzi kontrole w zakresie, o którym mowa w ust. 1;

2) organ właściwy do spraw cyberbezpieczeństwa 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, 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 dnia 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 w protokole wzmiankę 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 do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń.

Rozdział 12
Pełnomocnik i Kolegium

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.[4)] Pełnomocnikiem jest minister, sekretarz stanu albo podsekretarz stanu.

4. Obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową Pełnomocnika zapewnia ministerstwo albo 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 z udziałem organów administracji publicznej, organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV;

2) nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów właściwych do spraw cyberbezpieczeństwa, 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) Ze zmianą wprowadzoną przez art. 61 ustawy z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 695), która weszła w życie z dniem 18 kwietnia 2020 r.

4) upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;

5) inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa;

6) wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

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 informacje 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 do spraw cyberbezpieczeństwa.

Art. 65. 1. Do zadań Kolegium należy wyrażanie opinii w sprawach:

1) kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa;

1a)[5] planowanych do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 118 ust. 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2019 r. poz. 2460 oraz z 2020 r. poz. 374, 695 i 875), jeżeli ta decyzja jest wydawana po przeprowadzeniu aukcji, o której mowa w art. 116 ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i organy właściwe do spraw cyberbezpieczeństwa 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 do spraw cyberbezpieczeństwa;

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 stosowania urządzeń informatycznych lub oprogramowania.

1a.[6] Opinia w sprawie projektu rozstrzygnięcia decyzji, o której mowa w ust. 1 pkt 1a, wydawana jest przez Kolegium w terminie 14 dni od dnia otrzymania projektu przekazanego do zaopiniowania przez Prezesa Urzędu Komunikacji Elektronicznej.

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.

---

[5] Dodany przez art. 36 pkt 1 ustawy z dnia 14 maja 2020 r. o zmianie niektórych ustaw w zakresie działań osłonowych w związku z rozprzestrzenianiem się wirusa SARS-CoV-2 (Dz. U. poz. 875), która weszła w życie z dniem 16 maja 2020 r.

[6] Dodany przez art. 36 pkt 2 ustawy, o której mowa w odnośniku 5.

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 lub 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 do spraw cyberbezpieczeństwa 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, CSIRT NASK, sektorowych zespołów cyberbezpieczeństwa, organów właściwych do spraw cyberbezpieczeństwa oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium.

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

9. Rada Ministrów określi, w drodze rozporządzenia, szczegółowy 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, Straży Granicznej i Służby Ochrony Państwa;

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

Art. 68. Rada Ministrów przyjmuje Strategię, w drodze uchwały.

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, innymi 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, innymi ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii co 2 lata.

Art. 72. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej Strategię w terminie 3 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 obowiązków, o których 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 usuwa podatności, o których mowa w art. 32 ust. 2;

10) nie wykonuje obowiązku, o którym mowa w art. 14 ust. 1;

11) nie przeprowadza audytu;

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, o którym mowa w art. 18 ust. 1 pkt 4;

2) nie wykonuje obowiązku, o którym mowa w art. 18 ust. 1 pkt 5;

3) nie usuwa podatności, o których mowa w art. 32 ust. 2.

3. Wysokość kary pieniężnej, o której mowa w:

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

2) ust. 1 pkt 2, wynosi do 100 000 zł;

3) ust. 1 pkt 3, wynosi do 50 000 zł;

4) ust. 1 pkt 4, wynosi do 15 000 zł;

5) ust. 1 pkt 5, wynosi do 50 000 zł;

6) ust. 1 pkt 6, wynosi do 15 000 zł za każdy stwierdzony przypadek zaniechania obsługi incydentu;

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

8) ust. 1 pkt 8 i 9, wynosi do 20 000 zł;

9) ust. 1 pkt 10, wynosi 100 000 zł;

10) ust. 1 pkt 11 i 13, wynosi do 200 000 zł;

11) ust. 1 pkt 12, wynosi do 50 000 zł;

12) ust. 2 pkt 1, wynosi do 20 000 zł za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego;

13) ust. 2 pkt 2 i 3, wynosi do 20 000 zł.

4. Kara, o której mowa w:

1) ust. 1 pkt 4, nie może być niższa niż 1000 zł;

2) ust. 1 pkt 1–3, 6–9 i 12, nie może być niższa niż 5000 zł;

3) ust. 1 pkt 5, 10, 11 i 13, nie może być niższa niż 15 000 zł.

5. Jeżeli w wyniku kontroli organ właściwy do spraw cyberbezpieczeństwa stwierdzi, że operator usługi kluczowej albo 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 do spraw cyberbezpieczeństwa nakłada karę w wysokości do 1 000 000 zł.

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

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

Art. 75. Organ właściwy do spraw cyberbezpieczeństwa 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.

Art. 76. 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 do spraw cyberbezpieczeństwa uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

Rozdział 15

Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe

Art. 77–82. (pominięte)[7)]

Art. 83. Zagrożenia cyberbezpieczeństwa, mogące doprowadzić do sytuacji kryzysowej, po raz pierwszy zostaną ujęte w Raporcie o zagrożeniach bezpieczeństwa narodowego, który zostanie sporządzony z udziałem Pełnomocnika, po wejściu w życie ustawy.

Art. 84. Prezes Rady Ministrów powoła Pełnomocnika w terminie 3 miesięcy od dnia wejścia w życie ustawy.

Art. 85. Minister właściwy do spraw informatyzacji przekaże Komisji Europejskiej informacje o:

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

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

Art. 86. Organy właściwe do spraw cyberbezpieczeństwa 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. 87. 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. 88. 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. 89. Minister właściwy do spraw informatyzacji uruchomi system teleinformatyczny, o którym mowa w art. 46 ust. 1, do dnia 1 stycznia 2021 r.

Art. 90. Strategia zostanie przyjęta do dnia 31 października 2019 r.

Art. 91. 1. Roczny plan wdrożenia, o którym mowa w art. 32aa ust. 2 ustawy zmienianej w art. 79[8)], Szef Agencji Bezpieczeństwa Wewnętrznego opracuje po raz pierwszy na rok 2019.

2. Podmiot, który do dnia wejścia w życie ustawy przystąpił do realizowanego przez Agencję Bezpieczeństwa Wewnętrznego programu ARAKIS-GOV, uznaje się za podmiot, który przystąpił do systemu ostrzegania, w rozumieniu art. 32aa ust. 4 ustawy zmienianej w art. 79.

3. Podmiot, o którym mowa w ust. 2, który do dnia wejścia w życie ustawy nie dokonał pełnego wdrożenia elementów systemu ostrzegania, w rozumieniu art. 32aa ust. 4 ustawy zmienianej w art. 79 obowiązany jest do ich uzupełnienia w terminie roku od dnia wejścia w życie ustawy.

4. Zawarte przed dniem wejścia w życie ustawy porozumienia w sprawie udziału w programie ARAKIS-GOV uznaje się za porozumienia, o których mowa w art. 32aa ust. 7 ustawy zmienianej w art. 79.

---

7) Zamieszczone w obwieszczeniu.

8) Artykuł 79 zawierał zmiany do ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

Art. 92. 1.[9] Dotychczasowe przepisy wykonawcze wydane na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 77[10] dotyczące realizacji danego programu rządowego przyjętego na podstawie art. 90u ust. 1 pkt 6 ustawy zmienianej w art. 77, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 77 w brzmieniu nadanym niniejszą ustawą, dotyczących realizacji tego programu rządowego, nie dłużej jednak niż do dnia 31 marca 2021 r., i mogą być zmieniane.

2. Dotychczasowe przepisy wykonawcze, wydane na podstawie art. 176a ust. 5 ustawy zmienianej w art. 81[11], zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 176a ust. 5 ustawy zmienianej w art. 81, jednak nie dłużej niż przez 24 miesiące od dnia wejścia w życie niniejszej ustawy.

3. Dotychczasowe przepisy wykonawcze, wydane na podstawie art. 5a ust. 6 ustawy zmienianej w art. 82[12], zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 5a ust. 6 ustawy zmienianej w art. 82, jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 93. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – Gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 6450 tys. zł;
2) w 2019 r. – 13 349 tys. zł;

---

[9] W brzmieniu ustalonym przez art. 2 ustawy z dnia 16 października 2019 r. o zmianie ustawy – Prawo oświatowe oraz niektórych innych ustaw (Dz. U. poz. 2248), która weszła w życie z dniem 3 grudnia 2019 r.; wszedł w życie z dniem 19 listopada 2019 r.

[10] Artykuł 77 zawierał zmiany do ustawy z dnia 7 września 1991 r. o systemie oświaty.

[11] Artykuł 81 zawierał zmiany do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

[12] Artykuł 82 zawierał zmiany do ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

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, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 0 zł;

2) w 2019 r. – 255 tys. zł;

3) w 2020 r. – 3605 tys. zł;

4) w 2021 r. – 5605 tys. zł;

5) w 2022 r. – 5605 tys. zł;

6) w 2023 r. – 9705 tys. zł;

7) w 2024 r. – 705 tys. zł;

8) w 2025 r. – 705 tys. zł;

9) w 2026 r. – 705 tys. zł;

10) w 2027 r. – 8705 tys. zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 70 – Komisja Nadzoru Finansowego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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.

9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 76 – Urząd Komunikacji Elektronicznej, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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.

10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 42 – Sprawy wewnętrzne, będący skutkiem finansowym wejścia w życie niniejszej ustawy, 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.

11. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętych na dany rok budżetowy maksymalnych limitów wydatków, o których mowa w ust. 1–6 i 8, zostaną zastosowane mechanizmy korygujące polegające na:

1) ograniczeniu wydatków związanych z realizacją zadań organu właściwego do spraw cyberbezpieczeństwa 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 albo 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 do spraw cyberbezpieczeństwa.

12. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 7, zostanie zastosowany mechanizm korygujący polegający na ograniczeniu liczby podmiotów wdrażających system wczesnego ostrzegania o zagrożeniach występujących w sieci Internet, wskazanych w rocznym planie wdrożenia, opracowywanym przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

13. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 9, zostanie zastosowany mechanizm korygujący polegający na ograniczeniu wydatków związanych z realizacją zadań ustawowych dotyczących obsługi incydentów.

14. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 10, zostanie zastosowany mechanizm korygujący polegający na ograniczeniu wydatków związanych z zapewnieniem wyposażenia niezbędnego do obsługi Zespołu.

15. W przypadku gdy wielkość wydatków w poszczególnych miesiącach zgodna jest z planem finansowym, przepisów ust. 11–14 nie stosuje się.

16. 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. 11, dokonuje minister właściwy do spraw gospodarki morskiej.

17. 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. 11, dokonuje minister właściwy do spraw gospodarki wodnej.

18. 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. 11, dokonuje minister właściwy do spraw informatyzacji.

19. 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. 11, dokonuje minister właściwy do spraw transportu.

20. 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. 11, dokonuje minister właściwy do spraw ochrony zdrowia.

21. 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. 11, dokonuje minister właściwy do spraw energii.

22. Szef Agencji Bezpieczeństwa Wewnętrznego 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 mechanizmu korygującego, o którym mowa w ust. 12, dokonuje Szef Agencji Bezpieczeństwa Wewnętrznego.

23. Komisja Nadzoru Finansowego 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. 11, dokonuje Komisja Nadzoru Finansowego.

24. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmu korygującego, o którym mowa w ust. 13, dokonuje Prezes Urzędu Komunikacji Elektronicznej.

25. Minister właściwy do spraw wewnętrznych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 10, i dokonuje oceny jego wykorzystania. Wdrożenia mechanizmu korygującego, o którym mowa w ust. 14, dokonuje minister właściwy do spraw wewnętrznych.

Art. 94. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia[13)].

[13)] Ustawa została ogłoszona w dniu 13 sierpnia 2018 r.

Załączniki do ustawy z dnia 5 lipca 2018 r.

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 2020 r. poz. 1064).
		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 2020 r. poz. 833, 843 i 1086), 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 z dnia 10 kwietnia 1997 r. – 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 której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – 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 z dnia 9 czerwca 2011 r. – 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 z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – 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 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, 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 z dnia 10 kwietnia 1997 r. – 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 uchylającego 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 2019 r. poz. 1580 i 1495 oraz z 2020 r. poz. 284).
		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 2020 r. poz. 1043), 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 2019 r. poz. 1568, 1901 i 2170 oraz z 2020 r. poz. 284).
		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 2020 r. poz. 998 i 1086).
		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 2020 r. poz. 680).
	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 2020 r. poz. 470, 471 i 1087).
		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 2019 r. poz. 2357 oraz z 2020 r. poz. 284, 288, 321 i 1086).
		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 z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2019 r. poz. 2412 oraz z 2020 r. poz. 288 i 321).
		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 2020 r. poz. 89, 284, 288 i 568).
		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 2020 r. poz. 295 i 567).

		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 2020 r. poz. 944).
		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) – stronie 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 2019 r. poz. 1437 i 1495 oraz z 2020 r. poz. 284 i 471).
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.