Projekt z dnia 3 października 2022 r.

U S T A W A

z dnia …… 2022 r.

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw [1),2),3)]

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863) wprowadza się następujące zmiany:

1) przed rozdziałem 1 dodaje się oznaczenie i tytuł działu I w brzmieniu:

„DZIAŁ I. POSTANOWIENIA OGÓLNE”;

2) w art. 1:

a) w ust. 1:

– po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno–komunikacyjnych oraz uchylenia rozporządzenia (UE) nr

---

1) Niniejsza ustawa w zakresie swojej regulacji:
   1) służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (Akt o Cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15);
   2) wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE. L 2018 Nr 321, str. 36).

2) Niniejsza ustawa została notyfikowana Komisji Europejskiej w dniu …… pod numerem ……, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597), które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego [ujednolicenie] (Dz. Urz. UE L 241/1 z 17.09.2015, str. 1).

3) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym, ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych.

526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanego dalej „rozporządzeniem 2019/881;”,

– w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4–6 w brzmieniu:

„4) zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów;

5) zasady wyznaczania operatora strategicznej sieci bezpieczeństwa oraz jego zadania;

6) zasady przyznania zasobów częstotliwości z zakresu 703 – 713 MHz oraz 758 – 768 MHz;”,

b) w ust. 2:

– uchyla się pkt 1,

– pkt 2 otrzymuje brzmienie:

„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), z wyjątkiem art. 67a i art. 67b oraz art. 73 i art. 74;”;

3) art. 2 otrzymuje brzmienie:

„Art. 2. Użyte w ustawie określenia oznaczają:

1) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającym wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30), zwanym dalej „rozporządzeniem 765/2008”;

2) bezpieczeństwo sieci lub usług komunikacji elektronicznej – zdolność sieci telekomunikacyjnych lub usług komunikacji elektronicznej do odpierania, przy zakładanym poziomie ryzyka, wszelkich działań naruszających dostępność, autentyczność, integralność lub poufność:

a) tych sieci lub usług,

b) przetwarzanych danych i treści objętych tajemnicą komunikacji elektronicznej,

c) innych świadczonych przez przedsiębiorcę komunikacji elektronicznej usług związanych z usługami komunikacji elektronicznej lub sieciami telekomunikacyjnymi tego przedsiębiorcy;

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

4) certyfikat – europejski certyfikat cyberbezpieczeństwa lub krajowy certyfikat cyberbezpieczeństwa;

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

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

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

8) CSIRT INT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Wywiadu na rzecz jednostek organizacyjnie podległych Ministrowi Spraw Zagranicznych lub przez niego nadzorowanych oraz Agencji Wywiadu;

9) CSIRT sektorowy – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie sektora lub podsektora, ustanowiony przez organ właściwy do spraw cyberbezpieczeństwa dla danego sektora lub podsektora;

10) CSIRT Telco – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej;

11) cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych podmiotów przed cyberzagrożeniami;

12) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na systemy informacyjne, użytkowników takich systemów oraz na inne podmioty;

13) deklaracja zgodności – oświadczenie dostawcy produktu ICT, usługi ICT lub procesu ICT, że wyrób jest zgodny z europejskim programem certyfikacji

cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881 lub krajowym programem certyfikacji cyberbezpieczeństwa;

14) dostarczanie sieci telekomunikacyjnej – przygotowanie sieci telekomunikacyjnej w sposób umożliwiający świadczenie w niej usług, jej eksploatację, nadzór nad nią lub zapewnianie dostępu telekomunikacyjnego;

15) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w art. 2 pkt 3–6 rozporządzenia 765/2008;

16) incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;

17) incydent krytyczny – incydent lub incydent telekomunikacyjny 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;

18) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej;

19) 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”;

20) incydent telekomunikacyjny – każde zdarzenie, które ma rzeczywisty, niekorzystny skutek dla bezpieczeństwa sieci lub usług komunikacji elektronicznej;

21) 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;

22) ISAC – centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa;

23) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia 765/2008;
24) komunikat elektroniczny – każdą informację wymienianą lub przekazywaną między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej; nie obejmuje on informacji przekazanej jako część transmisji radiofonicznych lub telewizyjnych transmitowanych poprzez sieć telekomunikacyjną, z wyjątkiem informacji odnoszącej się do możliwego do zidentyfikowania użytkownika otrzymującego informację;
25) krajowy certyfikat cyberbezpieczeństwa – certyfikat cyberbezpieczeństwa wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa;
26) krajowa deklaracja zgodności – deklaracja zgodności wydana w ramach krajowego programu certyfikacji cyberbezpieczeństwa;
27) krajowy program certyfikacji cyberbezpieczeństwa – kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych przez Radę Ministrów i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT i procesów ICT;
28) krajowy poziom uzasadnienia zaufania – potwierdzenie, że dany produkt ICT, dana usługa ICT lub dany proces ICT spełnia wymogi wskazanego poziomu bezpieczeństwa określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
29) obsługa incydentu lub incydentu telekomunikacyjnego – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu lub incydentu telekomunikacyjnego;
30) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;
31) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez cyberzagrożenia;
32) poważny incydent telekomunikacyjny – incydent telekomunikacyjny o znaczącym wpływie na bezpieczeństwo sieci lub usług komunikacji elektronicznej;
33) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;
34) produkt ICT – element lub grupę elementów systemu informacyjnego;

35) przedsiębiorca komunikacji elektronicznej – przedsiębiorca telekomunikacyjny lub podmiot świadczący publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów;
36) przedsiębiorca telekomunikacyjny – przedsiębiorcę, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
37) ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;
38) SOC wewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa utworzony w ramach struktury operatora usługi kluczowej;
39) SOC zewnętrzny – zespół pełniący funkcję operacyjnego centrum bezpieczeństwa świadczący usługi na rzecz operatora usługi kluczowej;
40) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;
41) 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 2021 r. poz. 2070 oraz z 2022 r. poz. 1087), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
42) sytuacja szczególnego zagrożenia – sytuacja:
    a) wymagająca współpracy przedsiębiorców komunikacji elektronicznej z organami administracji publicznej i innymi podmiotami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy, zarządzania kryzysowego, utrzymania porządku publicznego oraz obronności i bezpieczeństwa państwa:
        – w przypadku wystąpienia sytuacji kryzysowej, w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. 2022 r. poz. 261 i 583),
        – w czasie obowiązywania stanów nadzwyczajnych,
        – w warunkach zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny,
    b) stanowiąca bezpośrednie zagrożenie dla bezpieczeństwa sieci lub usług komunikacji elektronicznej;
43) telekomunikacyjne urządzenia końcowe – urządzenia telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończenia sieci;

44) 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;

45) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;

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

47) usługi komunikacji elektronicznej – usługi świadczone za pośrednictwem sieci telekomunikacyjnej, zwykle za wynagrodzeniem, z wyłączeniem usług związanych z zapewnianiem albo wykonywaniem kontroli treści przekazywanych przy wykorzystaniu sieci telekomunikacyjnych lub usług komunikacji elektronicznej, obejmującą:

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

b) usługi komunikacji interpersonalnej,

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

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

49) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.”;

4) po art. 2 dodaje się dział II oraz rozdział 1 w brzmieniu:

„DZIAŁ II.

Krajowy system cyberbezpieczeństwa i krajowy system certyfikacji cyberbezpieczeństwa

Rozdział 1

Krajowy system cyberbezpieczeństwa”;

5) po art. 3 dodaje się art. 3a w brzmieniu:

„Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu:

1) identyfikacji źródła i analizy ruchu sieciowego powodującego wystąpienie incydentu zakłócającego świadczenie przez ten podmiot usługi kluczowej, usługi cyfrowej lub realizację zadań publicznych;
2) czasowego ograniczenia ruchu sieciowego z adresów IP lub adresów URL, zidentyfikowanego jako przyczyna incydentu, wchodzącego do infrastruktury tego podmiotu.”;

6) użyte w art. 4 w pkt 6, w art. 7 w ust. 7, w art. 9 w ust. 2, w art. 11 w ust. 3 we wprowadzeniu do wyliczenia, w art. 12 w ust. 3 i 4, w art. 13 w ust. 3, w art. 14 ust. 3, w art. 15 w ust. 2 w pkt 3, w art. 26 w ust. 3 w pkt 10, w art. 42 w ust. 1 w pkt 5 dwukrotnie, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 48 w pkt 1, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 66 w ust. 7 oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „CSIRT sektorowy”;

7) w art. 4:

a) po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) przedsiębiorców komunikacji elektronicznej;”,

b) po pkt 5 dodaje się pkt 5a w brzmieniu:

„5a) CSIRT Telco;”,

c) po pkt 6 dodaje się pkt 6a i 6b w brzmieniu:

„6a) CSIRT INT;

6b) ISAC, o którym mowa w art. 25a;”,

d) w pkt 7 wyrazy „w art. 9 pkt 1–6, 8, 9, 11 i 12” zastępuje się wyrazami „w art. 9 pkt 1–6 i 8–10”,

e) po pkt 7 dodaje się pkt 7a w brzmieniu:

„7a) Urząd Komisji Nadzoru Finansowego;”,

f) pkt 8 otrzymuje brzmienie:

„8) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2022 r. poz. 574, z późn. zm. [4)]);”,

g) po pkt 14 dodaje się pkt 14a i14b w brzmieniu:

„14a) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2021 r. poz. 2233, 2368, oraz z 2022 r. poz. 88, 258, 855, 1079 i 1549);

14b) Polski Fundusz Rozwoju oraz inne instytucje rozwoju, o których mowa w ustawie z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2022 r. poz. 760 i 1079);”,

h) pkt 16 otrzymuje brzmienie:

„16) SOC zewnętrzne”;

i) po pkt 17 dodaje się punkt 17a w brzmieniu:

„17a) Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE”;

8) w art. 7:

a) po ust 3 dodaje się ust. 3a w brzmieniu:

„3a. W przypadku podmiotów, dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, wpisanie do wykazu operatorów usług kluczowych albo zmiana danych tych podmiotów dokonywana jest z urzędu.”,

b) w ust. 4 wyrazy „nie później niż w terminie 6 miesięcy” zastępuje się wyrazami „niezwłocznie, nie później niż w terminie 1 miesiąca”,

c) ust. 5 otrzymuje brzmienie:

„5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.”;

9) użyte w art. 8 w pkt 3, w pkt 5 w lit. d, w art. 9 w ust. 1 w pkt 2, w art. 13 w ust. 1 w pkt 2, w art. 22 w ust. 1 w pkt 4, w art. 26 w ust. 1, w ust. 3 w pkt 1, 2, 4 i 10, w pkt 14 w lit.

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2022 r. poz. 583, 655, 682, 807, 1010, 1079, 1117 i 1459.

b i c i w ust. 6 w pkt 2, w art. 33 w ust. 4a, w art. 35 w ust. 4 i 5, w art. 37 w ust. 1, w art. 39 w ust. 1, w ust. 3 we wprowadzeniu do wyliczenia i w ust. 4, w art. 46 w ust. 1 w pkt 5, w art. 51 w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 53 w ust. 1 w pkt 2 w lit. a, w art. 62 w ust. 2 w pkt 3, w art. 65 w ust. 1 w pkt 1 i 2, w art. 73 w ust. 5 w pkt 1, w art. 83, w różnej liczbie i różnym przypadku, wyrazy „zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i przypadku wyrazem „cyberzagrożenie”;

10) w art. 8 w pkt 5 lit. b otrzymuje brzmienie:

„b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi kluczowej oraz poziomu krytyczności poszczególnych aktualizacji,”;

11) w art. 9:

a) w ust. 1 w pkt 1 wyrazy „osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”,

b) ust. 2 otrzymuje brzmienie:

„2. Operator usługi kluczowej przekazuje do organu właściwego do spraw cyberbezpieczeństwa dane osób, o których mowa w ust. 1 pkt 1, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych – w terminie 14 dni od dnia ich zmiany. Organ właściwy do spraw cyberbezpieczeństwa przekazuje te dane do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.”;

12) w art. 10:

a) w ust. 1, w ust. 2 we wprowadzeniu do wyliczenia oraz w ust. 3 i 4 wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”,

b) w ust. 2 pkt 2 otrzymuje brzmienie:

„2) ochronę dokumentów przed przypadkowym uszkodzeniem, zniszczeniem, utratą, nieuprawnionym dostępem, niewłaściwym użyciem lub utratą integralności;”,

c) w ust. 5 wyraz „cyberbezpieczeństwa” zastępuje się wyrazami „bezpieczeństwa systemów informacyjnych”;

13) w art. 11:

a) w ust. 1 w pkt 4 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”,

b) w ust. 2 po wyrazach „przekazywane jest w postaci elektronicznej” dodaje się wyrazy „za pomocą systemu, o którym mowa w art. 46 ust. 1”,

c) w ust. 3:

– pkt 1 i 2 otrzymują brzmienie:

„1) współdziała z właściwym CSIRT sektorowym na poziomie sektora lub podsektora podczas obsługi incydentu poważnego lub incydentu krytycznego, koordynowanej przez CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe;

2) zapewnia właściwemu CSIRT sektorowemu dostęp do informacji o rejestrowanych incydentach.”,

– uchyla się pkt 3;

d) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu:

„3a. W przypadku gdy:

1) operator usługi kluczowej jest przedsiębiorcą komunikacji elektronicznej oraz

2) zgłasza incydent poważny, będący również poważnym incydentem telekomunikacyjnym zgłoszenie jest przekazywane tylko do CSIRT sektorowego. Zgłoszenie zawiera elementy wskazane w art. 12 i art. 20e.

3b. Operator usługi kluczowej współdziała również z CSIRT Telco w sytuacji, o której mowa w ust. 3a.”;

14) w art. 13:

a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT sektorowego”,

b) uchyla się ust. 3,

c) dodaje się ust. 5 w brzmieniu:

„5. W uzasadnionym przypadku, CSIRT sektorowy przekazuje do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV informacje o których mowa w ust. 1, niezwłocznie po stwierdzeniu zasadności przekazania danej informacji, nie później jednak niż w ciągu 8 godzin od takiego stwierdzenia.”;

15) art. 14 otrzymuje brzmienie:

„Art. 14. 1. Zadania operatora usługi kluczowej, o których mowa w art. 8, art. 9, art. 10 ust. 1–3, art. 11 ust. 1–3, art. 12 i art. 13, w zakresie bezpieczeństwa systemów informacyjnych realizowane są w ramach SOC wewnętrznego lub SOC zewnętrznego.

2. Operator usługi kluczowej powołuje SOC wewnętrzny lub zawiera umowę o prowadzenie SOC zewnętrznego, zwaną dalej „umową o świadczenie usług SOC”.

3. Organ tworzący lub nadzorujący operatora usługi kluczowej może utworzyć na rzecz tego operatora SOC zewnętrzny.

4. SOC wewnętrzny może realizować zadania, o których mowa w ust. 1, także na rzecz innych podmiotów.

5. SOC wewnętrzny lub SOC zewnętrzny, na podstawie przeprowadzonego szacowania ryzyka, prowadzi działania zapewniające cyberbezpieczeństwo, w szczególności wprowadza zabezpieczenia, zapewniające poufność integralność, dostępność i autentyczność przetwarzanych danych, z uwzględnieniem określenia zasad dostępu do pomieszczeń oraz systemów, a także eksploatacji i architektury systemów, w celu:

1) monitorowania i wykrywania incydentów;
2) reagowania na incydenty;
3) zapobiegania incydentom;
4) zarządzania jakością zabezpieczeń systemów, informacji i aktywów;
5) aktualizowania analizy ryzyka w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na działania, o których mowa w pkt 1–3.

6. Operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o sposobie realizacji obowiązku, o którym mowa w ust. 2, polegającego na powołaniu SOC wewnętrzny lub zawarciu umowy o świadczenie usług SOC, albo realizowaniu zadania poprzez SOC zewnętrzny utworzony na jego rzecz przez organ tworzący lub nadzorujący, lub o zmianie sposobu realizacji tego obowiązku.

7. W przypadku zawarcia umowy o prowadzenie SOC operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o:

1) zawarciu takiej umowy oraz dacie jej zawarcia,
2) danych kontaktowych, o których mowa w ust. 10 pkt 4, podmiotu, z którym zawarta została umowa,
3) zakresie świadczonej usługi,

4) terminie obowiązywania umowy,

5) rozwiązaniu umowy

– w terminie 14 dni od dnia zawarcia lub rozwiązania umowy.

8. W przypadku, gdy jest to niezbędne dla zapewnienia bezpieczeństwa systemów informacyjnych, podmiot prowadzący SOC zapewnia bezpieczny i zdalny dostęp do swoich systemów obsługiwanemu operatorowi usługi kluczowej przez co najmniej:

1) ustalenie zasad dostępu do systemu;

2) stosowanie środków zapewniających bezpieczne przetwarzanie danych i komunikację;

3) minimalizację zakresu danych przechowywanych poza bezpiecznym środowiskiem.

9. Przy zawieraniu umowy o prowadzenie SOC zawiera się zastrzeżenie, że świadczenie tych usług podlega prawu polskiemu.

10. SOC zewnętrzny, udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:

1) nazwa SOC zewnętrznego;

2) zakres obszaru działania, w tym:

   a) oferowany rodzaj wsparcia,

   b) zasady współpracy i wymiany informacji,

   c) politykę komunikacji i uwierzytelniania informacji;

3) oferowane usługi oraz politykę obsługi incydentów i koordynacji incydentów;

4) dane kontaktowe, w tym:

   a) adres ze wskazaniem strefy czasowej,

   b) numer telefonu, adres poczty elektronicznej oraz wskazanie innych dostępnych środków komunikacji z SOC,

   c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z SOC zewnętrznym,

   d) sposoby kontaktu z SOC zewnętrznym, w tym sposób zgłaszania incydentów.”;

16) po art. 14 dodaje się art. 14a w brzmieniu:

„14a. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz SOC wewnętrznych i SOC zewnętrznych, zwany dalej „wykazem SOC”.

2. Wykaz SOC zawiera:

1) nazwę (firmę) podmiotu prowadzącego SOC wewnętrzny lub SOC zewnętrzny;

2) nazwę (firmę) podmiotów, na rzecz których SOC wewnętrzny lub SOC zewnętrzny jest prowadzony;
3) siedzibę i adres SOC wewnętrzny lub SOC zewnętrzny;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) datę wpisania do wykazu SOC;
7) datę wykreślenia z wykazu SOC.

3. Wpisanie do wykazu SOC i wykreślenie z tego wykazu następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa złożony niezwłocznie, nie później niż w terminie 14 dni, po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6. Wniosek zawiera dane, o których mowa w ust. 2 pkt 1–5.

4. W przypadku podmiotów dla których organem właściwym do spraw cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji wpisanie do wykazu SOC dokonuje się z urzędu po uzyskaniu od operatora usługi kluczowej informacji, o której mowa w art. 14 ust. 6.

5. Zmiana danych w wykazie SOC następuje na wniosek organu właściwego do spraw cyberbezpieczeństwa, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych. Ust. 4 stosuje się odpowiednio.

6. Wnioski, o których mowa w ust. 3 i 5, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

7. Wpisanie do wykazu SOC i wykreślenie z tego wykazu oraz zmiana danych w wykazie SOC są czynnościami materialno–technicznymi.

8. Minister właściwy do spraw informatyzacji może, z urzędu, wpisać do wykazu, o którym mowa w ust. 1, inny podmiot niż SOC wewnętrzny lub SOC zewnętrzny, jeżeli co najmniej:

1) świadczy usługi z zakresu cyberbezpieczeństwa, w szczególności związane z:
   a) monitorowaniem, wykrywaniem, reagowaniem i zapobieganiem incydentów,
   b) zarządzaniem jakością zabezpieczeń systemów, informacji i powierzonych aktywów,
   c) aktualizowaniem ryzyk w przypadku zmiany struktury organizacyjnej, procesów i technologii, które mogą wpływać na reakcję na incydent;

2) przedstawi dokument potwierdzający zdolność do ochrony informacji niejawnych zgodnie z ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 oraz z 2022 r. poz. 655 i 1933);
3) zawrze z ministrem właściwym do spraw informatyzacji porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46 ust. 1.

9. Minister właściwy do spraw informatyzacji wykreśla z wykazu wpisany z urzędu podmiot, który przestał spełniać warunki, o których mowa w ust. 8.

10. Dane z wykazu SOC minister właściwy do spraw informatyzacji udostępnia CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, a także operatorowi usługi kluczowej w zakresie go dotyczącym.

11. Minister właściwy do spraw informatyzacji udostępnia dane z wykazu SOC, na wniosek, następującym podmiotom:

1) organowi właściwemu 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

– w zakresie niezbędnym do realizacji ich ustawowych zadań.”;

17) użyty w art. 17 w ust. 2, art. 69 w ust. 1, w ust. 2 w pkt 1, 6 i 7, w różnej liczbie i przypadku, wyraz „cyberbezpieczeństwo” zastępuje się użytymi w odpowiedniej liczbie i przypadku wyrazami „bezpieczeństwo systemów informacyjnych”;
18) w art. 17 w ust. 2 pkt 1 skreśla się wyrazy „systemów informacyjnych i”;
19) po rozdziale 4 dodaje się rozdział 4a w brzmieniu:

„Rozdział 4a

Zadania i obowiązki przedsiębiorców komunikacji elektronicznej w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów

Art. 20a. 1. Przedsiębiorca komunikacji elektronicznej, w celu zapewnienia ciągłości świadczenia usług komunikacji elektronicznej lub dostarczania sieci telekomunikacyjnej, jest obowiązany uwzględniać możliwość wystąpienia sytuacji szczególnego zagrożenia.

2. Przedsiębiorca komunikacji elektronicznej:

1) przeprowadza systematyczne szacowanie ryzyka wystąpienia sytuacji szczególnego zagrożenia co najmniej raz w roku;
2) podejmuje środki techniczne i organizacyjne zapewniające poufność, integralność, dostępność i autentyczność przetwarzanych danych, a także poziom bezpieczeństwa adekwatny do poziomu zidentyfikowanego ryzyka, minimalizujące w szczególności wpływ, jaki na sieci telekomunikacyjne, usługi komunikacji elektronicznej lub podmioty korzystające z tych sieci lub usług może mieć wystąpienie sytuacji szczególnego zagrożenia, dotyczące następujących obszarów:
   a) zapewnienia bezpieczeństwa infrastruktury telekomunikacyjnej,
   b) postępowania w przypadku wystąpienia sytuacji szczególnego zagrożenia,
   c) odtwarzania dostarczania sieci telekomunikacyjnych lub przywracania świadczenia usług komunikacji elektronicznej,
   d) monitorowania, kontroli i testowania sieci telekomunikacyjnych lub usług komunikacji elektronicznej

   – przy uwzględnieniu aktualnego stanu wiedzy technicznej oraz kosztów wprowadzenia tych środków;
3) dokumentuje czynności, o których mowa w pkt 1 i 2.

3. Przedsiębiorca telekomunikacyjny sporządzający plan działań w sytuacji szczególnego zagrożenia, dokumentuje w tym planie czynności, o których mowa w ust. 2 pkt 1 i 2.

4. Przedsiębiorca komunikacji elektronicznej:

a) wyznacza dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa,
b) przekazuje do Prezesa UKE dane osób, o których mowa w lit. a, 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. Prezes UKE przekazuje te dane do CSIRT Telco oraz do właściwego CSIRTMON, CSIRT NASK lub CSIRT GOV.

5. Przepisu ust. 4 nie stosuje się do przedsiębiorcy komunikacji elektronicznej, który jest mikroprzedsiębiorcą, małym przedsiębiorcą lub średnim przedsiębiorcą.

6. Minister właściwy do spraw informatyzacji może, w drodze rozporządzenia, określić dla danego rodzaju działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej minimalny zakres środków, o których mowa w ust. 2 pkt 2, lub sposób ich dokumentowania, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA”, skalę działalności wykonywanej przez przedsiębiorcę komunikacji elektronicznej oraz mając na uwadze potrzebę podejmowania przez tego przedsiębiorcę działań zapewniających bezpieczeństwo sieci lub usług komunikacji elektronicznej.

Art. 20b. 1. Prezes UKE, może dokonywać oceny zastosowanych przez przedsiębiorcę komunikacji elektronicznej środków technicznych i organizacyjnych, o których mowa w art. 20a ust. 2 pkt 2, kierując się rekomendacjami ENISA.

2. Przedsiębiorca komunikacji elektronicznej jest obowiązany do przekazania Prezesowi UKE, na jego żądanie, informacji niezbędnych do dokonania oceny.

3. Żądanie, o którym mowa w ust. 2, zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę;
3) wskazanie zakresu żądanych informacji oraz okresu, którego dotyczą;
4) wskazanie celu, jakiemu informacje mają służyć;
5) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
6) pouczenie o zagrożeniu karą, o której mowa w art. 76a ust. 1 pkt 4.

4. Prezes UKE może, w drodze decyzji, w przypadku powstania w wyniku dokonanej oceny, o której mowa w ust. 1, uzasadnionych wątpliwości co do stosowania właściwych środków technicznych i organizacyjnych, nałożyć na przedsiębiorcę komunikacji elektronicznej obowiązek:

1) uzupełnienia lub właściwego zastosowania środków technicznych lub organizacyjnych lub

2) poddania się, na własny koszt, audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany, wybrany przez przedsiębiorcę, niezależny podmiot i udostępnienia Prezesowi UKE wyników tego audytu.

5. W decyzji, o której mowa w ust. 4:

1) w pkt 1, Prezes UKE wskazuje termin uzupełnienia lub właściwego zastosowania środków technicznych lub organizacyjnych;
2) w pkt 2, Prezes UKE określa termin udostępnienia wyników audytu bezpieczeństwa.

6. Do audytu bezpieczeństwa, o którym mowa w ust. 5 pkt 2, stosuje się odpowiednio art. 15 ust. 2 pkt 1 i 2 oraz ust. 3–5. Audytorzy, o których mowa w art. 15 ust. 2 pkt 2, wykonujący audyt bezpieczeństwa muszą być niezależni od przedsiębiorcy komunikacji elektronicznej, u którego prowadzony jest audyt bezpieczeństwa.

Art. 20c. Przedsiębiorca komunikacji elektronicznej:

1) zapewnia obsługę incydentu telekomunikacyjnego;
2) może przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco informacje:
   a) o cyberzagrożeniach, podatnościach i incydentach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci lub usług komunikacji elektronicznej,
   b) o wykorzystywanych technologiach;
3) zapewnia dostęp do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań.

Art. 20d. 1. Przedsiębiorca komunikacji elektronicznej:

1) uznaje incydent telekomunikacyjny za poważny incydent telekomunikacyjny, o którym mowa w art. 20d ust. 3;
2) zgłasza poważny incydent telekomunikacyjny, niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do CSIRT Telco;
3) współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco oraz z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe.

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.

3. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, biorąc pod uwagę rekomendacje ENISA, progi uznania incydentu telekomunikacyjnego za poważny incydent telekomunikacyjny, uwzględniając:

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

Art. 20e. 1. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, jeśli został nadany;
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 telekomunikacyjnego na sieci i usługi, w tym:
   a) sieci telekomunikacyjne, na które poważny incydent telekomunikacyjny miał wpływ,
   b) usługi komunikacji elektronicznej zgłaszającego, na które poważny incydent telekomunikacyjny miał wpływ,
   c) liczbę użytkowników usługi komunikacji elektronicznej, na których poważny incydent telekomunikacyjny miał wpływ,
   d) moment wystąpienia i wykrycia poważnego incydentu telekomunikacyjnego oraz czas jego trwania,
   e) zasięg geograficzny obszaru, którego dotyczy poważny incydent telekomunikacyjny,

f) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi kluczowej przez operatorów usług kluczowych, jeżeli jest znany,

g) wpływ poważnego incydentu telekomunikacyjnego na świadczenie usługi cyfrowej przez dostawców usług cyfrowych, jeżeli jest znany,

h) przyczynę zaistnienia poważnego incydentu telekomunikacyjnego i sposób jego przebiegu oraz skutki jego oddziaływania na sieci telekomunikacyjne lub świadczone usługi komunikacji elektronicznej,

i) wpływ poważnego incydentu telekomunikacyjnego na połączenia z numerami alarmowymi,

j) wpływ poważnego incydentu telekomunikacyjnego na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;

5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie czy poważny incydent telekomunikacyjny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej;

6) informacje o podjętych działaniach zapobiegawczych;

7) informacje o podjętych działaniach naprawczych.

2. Zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2, może zawierać inne istotne informacje.

3. Przedsiębiorca komunikacji elektronicznej przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu telekomunikacyjnego.

4. Przedsiębiorca komunikacji elektronicznej może przekazać, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 20d ust. 1 pkt 2, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do obsługi incydentu telekomunikacyjnego przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco.

5. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco może zwrócić się do przedsiębiorcy komunikacji elektronicznej o uzupełnienie zgłoszenia o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do obsługi incydentu telekomunikacyjnego.

6. W zgłoszeniu przedsiębiorca komunikacji elektronicznej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 20f. 1. Przedsiębiorca komunikacji elektronicznej publikuje na swojej stronie internetowej informacje o:

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

2. Przedsiębiorca komunikacji elektronicznej, w przypadku szczególnego i znacznego zagrożenia wystąpienia incydentu telekomunikacyjnego, informuje swoich użytkowników, na których takie zagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć, oraz związanych z tym kosztach. Przedsiębiorca komunikacji elektronicznej informuje tych użytkowników o samym zagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa sieci lub usług komunikacji elektronicznej.

3. Przedsiębiorca komunikacji elektronicznej, informuje, w tym na swojej stronie internetowej, o incydencie telekomunikacyjnym i jego wpływie na dostępność świadczonych usług, jeżeli w jego ocenie ten wpływ jest istotny.

Art. 20g. W przypadku stwierdzenia przesyłania komunikatów elektronicznych zagrażających bezpieczeństwu sieci lub usług komunikacji elektronicznej, przedsiębiorca komunikacji elektronicznej, może zastosować środki polegające na:

1) zablokowaniu przesłania takiego komunikatu,
2) ograniczeniu albo przerwaniu świadczenia usługi komunikacji elektronicznej

– w zakresie niezbędnym dla zapobiegnięcia zagrożeniu i nie dłużej niż do czasu ustania przyczyny stwierdzenia zagrożenia.

Art. 20h. 1. Prezes UKE kierując się rekomendacjami ENISA dotyczącymi raportowania incydentów telekomunikacyjnych:

1) informuje o wystąpieniu poważnego incydentu telekomunikacyjnego organy regulacyjne innych państw członkowskich oraz ENISA, jeżeli uzna charakter tego incydentu za istotny;
2) przekazuje Komisji Europejskiej oraz ENISA sprawozdanie za rok poprzedni zawierające informacje o poważnych incydentach telekomunikacyjnych.

2. Prezes UKE może publikować na stronie podmiotowej Biuletynu Informacji Publicznej Urzędu Komunikacji Elektronicznej, w przypadkach uzasadnionych interesem publicznym, informację o wystąpieniu poważnego incydentu telekomunikacyjnego.

3. Prezes UKE informuje niezwłocznie, w terminie nie dłuższym niż 3 dni, przedsiębiorcę komunikacji elektronicznej, u którego wystąpił poważny incydent telekomunikacyjny, o opublikowaniu informacji, o której mowa w ust. 2, wraz ze wskazaniem adresu elektronicznego, pod którym udostępniona jest ta informacja.

4. Przedsiębiorca komunikacji elektronicznej, o którym mowa w ust. 3, jest obowiązany opublikować na swojej stronie internetowej informację o wystąpieniu poważnego incydentu telekomunikacyjnego oraz umieścić adres elektroniczny, o którym mowa w ust. 3, niezwłocznie, nie później niż w terminie 3 dni od otrzymania informacji, o której mowa w ust. 3.

5. Prezes UKE może, w drodze decyzji, nałożyć na przedsiębiorcę komunikacji elektronicznej, o którym mowa w ust. 3, obowiązek podania do publicznej wiadomości informacji o wystąpieniu poważnego incydentu telekomunikacyjnego, wskazując sposób jej publikacji, jeżeli sposoby opublikowania informacji, o których mowa w ust. 2 i 3, w niewystarczającym stopniu służą ochronie interesu publicznego.”;

20) w art. 21:

a) w ust. 1 wyrazy „osoby odpowiedzialnej” zastępuje się wyrazami „dwóch osób odpowiedzialnych”,

b) w ust. 2 i 3 wyrazy „jedną osobę odpowiedzialną” zastępuje się wyrazami „dwie osoby odpowiedzialne”;

21) w art. 22:

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

„1a. Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zgłaszają incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do CSIRT INT.”,

b) w ust. 2 po wyrazach „w ust. 1 pkt 2” dodaje się wyrazy „oraz ust. 1a”,

c) dodaje się ust. 3–5 w brzmieniu:

„3. Niezależnie od zadań, określonych w ust. 1, Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, przekazuje jednocześnie CSIRT INT w postaci elektronicznej, a w przypadku braku możliwości przekazania go w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji, zgłoszenie, o którym mowa w ust. 1 pkt 2.

4. Jednostki, o których mowa w ust. 3:

1) współdziałają z CSIRT INT podczas obsługi incydentu w podmiocie publicznym, przekazując niezbędne dane, w tym dane osobowe;

2) zapewniają CSIRT INT dostęp do informacji o rejestrowanych incydentach w zakresie niezbędnym do realizacji jego zadań;

3) przekazują do CSIRT INT dane osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, w terminie 14 dni od dnia ich wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia ich zmiany.

5. CSIRT INT niezwłocznie przekazuje informacje, o których mowa w ust. 4, do CSIRT GOV.”;

22) w art. 23 w ust. 3 i 4 oraz w art. 24 w zdaniu pierwszym wyrazy „CSIRT MON, CSIRT NASK lub CSIRT GOV” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”;

23) po art. 25 dodaje się rozdział 5a w brzmieniu:

„Rozdział 5a

Obowiązki ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa

Art. 25a 1. ISAC oraz minister właściwy do spraw informatyzacji mogą zawrzeć porozumienie w sprawie korzystania z systemu, o którym mowa w art. 46, jeżeli ISAC w szczególności:

1) wspiera podmioty krajowego systemu cyberbezpieczeństwa w:

a) rozpoznawaniu cyberzagrożeń i obsługi incydentów,

b) podnoszeniu świadomości cyfrowej;

2) gromadzi i analizuje informacje o podatnościach, cyberzagrożeniach i incydentach oraz zapewnia podmiotom krajowego systemy cyberbezpieczeństwa dostęp do tych informacji i wyników analiz.

2. Jeżeli ISAC jest jednostką organizacyjną nieposiadającą osobowości prawnej, strony tworzące ISAC wyznaczają przedstawiciela w celu zawarcia porozumienia, o którym mowa w ust. 1.

3. Minister właściwy do spraw informatyzacji prowadzi wykaz ISAC, które zawarły porozumienie, o którym mowa w ust. 1, zwany dalej „wykazem ISAC”.

4. Wykaz ISAC zawiera:

1) nazwę ISAC;
2) imię i nazwisko osoby reprezentującej ISAC wraz z numerem telefonu oraz adresem poczty elektronicznej;
3) siedzibę i adres ISAC, jeżeli posiada;
4) numer identyfikacji podatkowej (NIP), jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) adres poczty elektronicznej ISAC;
7) adres strony internetowej ISAC, jeżeli posiada;
8) adres do doręczeń elektronicznych ISAC, jeżeli posiada;
9) datę zawarcia porozumienia;
10) datę wpisania do wykazu ISAC;
11) datę wykreślenia z wykazu ISAC.

5. Wpisanie do wykazu ISAC następuje niezwłocznie, najpóźniej w ciągu 7 dni od zawarcia porozumienia, o którym mowa w ust. 1.

6. Wykreślenie ISAC z wykazu ISAC następuje w przypadku:

1) rozwiązania porozumienia, o którym mowa w ust. 1;
2) rozwiązania ISAC.

7. Zmiana danych w wykazie ISAC następuje na wniosek podmiotu prowadzącego ISAC, złożony niezwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych, lub z urzędu. Wniosek sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

8. Wpisanie do wykazu ISAC i wykreślenie z tego wykazu oraz zmiana danych w wykazie ISAC są czynnościami materialno–technicznymi.

9. Wykaz ISAC jest publikowany w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. W publikowanym wykazie nie umieszcza się informacji wskazanych w ust. 4 pkt 2.

10. ISAC wpisany do wykazu ISAC współpracuje z CSIRT MON, CSIRT NASK lub CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa, w szczególności w zakresie wymiany informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów.

11. ISAC wpisany do wykazu ISAC przedkłada ministrowi właściwemu do spraw informatyzacji w terminie do dnia 31 marca każdego roku sprawozdanie z realizacji zadań za poprzedni rok kalendarzowy.

12. Minister właściwy do spraw informatyzacji, na wniosek organu właściwego albo z urzędu, może przeprowadzić kontrolę:

1) zgodności z prawem działania ISAC wpisanego do wykazu ISAC;
2) przestrzegania przez ISAC wpisany do wykazu ISAC, zasad współpracy w ramach krajowego systemu cyberbezpieczeństwa.

13. Do kontroli, o której mowa w ust. 12, przepis art. 54 ust. 2 stosuje się odpowiednio.

14. W razie stwierdzenia, że działalność ISAC wpisanego do wykazu ISAC jest niezgodna z prawem lub narusza zasady współpracy w ramach krajowego systemu cyberbezpieczeństwa, minister właściwy do spraw informatyzacji, w zależności od rodzaju i stopnia stwierdzonych nieprawidłowości, może:

1) wystąpić do ISAC o usunięcie stwierdzonych nieprawidłowości w określonym terminie lub
2) wypowiedzieć porozumienie, o którym mowa w ust. 1.”;

24) w art. 26:

a) ust. 2 otrzymuje brzmienie:

„2. CSIRTMON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek podmiotów krajowego systemu 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 i incydentów telekomunikacyjnych.”,

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

„2a. Pełnomocnik może zlecić zapewnienie wsparcia w obsłudze incydentów i incydentów telekomunikacyjnych, o których mowa w ust. 2:

a) CSIRT NASK za zgodą ministra właściwego do spraw informatyzacji,

b) CSIRT GOV za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego, lub

c) CSIRT MON za zgodą Ministra Obrony Narodowej.

2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków porozumiewania się na odległość.”,

c) w ust. 3:

– w pkt 1 po wyrazie „incydentów” dodaje się wyrazy: „i incydentów telekomunikacyjnych”,

– w pkt 2 po wyrazie „incydentami” dodaje się wyrazy: „i incydentami telekomunikacyjnymi”,

– w pkt 3 wyrazy „incydentów i ryzyk” zastępuje się wyrazami „incydentów, incydentów telekomunikacyjnych i ryzyk”,

– pkt 5 otrzymuje brzmienie:

„5) reagowanie oraz koordynacja reagowania na zgłoszone incydenty i incydenty telekomunikacyjne;”,

– w pkt 6 wyrazy „w tym incydentów poważnych oraz incydentów istotnych” zastępuje się wyrazami „w tym incydentów poważnych, incydentów istotnych oraz incydentów telekomunikacyjnych”,

– w pkt 10 po wyrazie „oraz” dodaje się wyrazy „z CSIRT INT”,

– w pkt 12 wyrazy „30 maja” zastępuje się wyrazami „31 stycznia”,

– pkt 16 otrzymuje brzmienie:

„16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz ENISA;”,

– w pkt 16 kropkę zastępuje się średnikiem i dodaje się pkt 17–22 w brzmieniu:

„17) gromadzenie oraz przetwarzanie informacji dotyczących cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych;

18) przygotowywanie na zlecenie Pełnomocnika lub przewodniczącego Kolegium analiz w zakresie cyberzagrożeń, podatności, incydentów i incydentów telekomunikacyjnych;

19) przygotowywanie na zlecenie Pełnomocnika analiz skutków incydentów i incydentów telekomunikacyjnych oraz przebiegu obsługi incydentów i incydentów telekomunikacyjnych;

20) przygotowywanie rekomendacji w zakresie usprawniania krajowego systemu cyberbezpieczeństwa;

21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa, poprzez:

a) wykonywanie oceny bezpieczeństwa,

b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach;

22) udział w przedsięwzięciach mających na celu rozwój kompetencji CSIRTMON, CSIRT NASK lub CSIRT GOV, w szczególności w ćwiczeniach oraz szkoleniach specjalistycznych.”,

d) ust. 4 otrzymuje brzmienie:

„4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu lub incydentu telekomunikacyjnego, którego koordynacja obsługi wymaga współpracy CSIRT, oraz określą we współpracy z CSIRT sektorowymi, CSIRT Telco i CSIRT INT sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu lub incydentu telekomunikacyjnego.”,

e) w ust. 5 wprowadzenie do wyliczenia otrzymuje brzmienie:

„Do zadań CSIRT MON należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”,

f) w ust. 6:

– w pkt 1:

– – lit. a otrzymuje brzmienie:

„a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2–6 i 10 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,”,

– – lit. c otrzymuje brzmienie:

„c) podmioty wskazane w art. 7 ust. 1 pkt 1 i 3–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce,”,

– po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) koordynacja obsługi incydentów telekomunikacyjnych zgłaszanych przez przedsiębiorców komunikacji elektronicznej, z wyjątkiem incydentów telekomunikacyjnych zgłaszanych przez podmioty wskazane w ust. 5 i 7,

g) w ust. 7:

- wprowadzenie do wyliczenia otrzymuje brzmienie:

„Do zadań CSIRT GOV należy koordynacja obsługi incydentów i incydentów telekomunikacyjnych zgłaszanych przez:”;

- po pkt 4 dodaje się pkt 4a–4c w brzmieniu:

„4a) Państwowe Gospodarstwo Wodne Wody Polskie;

4b) Polski Fundusz Rozwoju i inne instytucje rozwoju;

4c) Urząd Komisji Nadzoru Finansowego;”,

h) w ust. 8 wyrazy „zgłoszenie incydentu” zastępuje się wyrazami „zgłoszenie incydentu lub incydentu telekomunikacyjnego”,

i) ust. 9 otrzymuje brzmienie:

„9. Działalność bieżąca CSIRT NASK jest finansowana w formie dotacji podmiotowej ze środków, których dysponentem jest minister właściwy do spraw informatyzacji.”,

j) po ust. 9 dodaje się ust. 9a w brzmieniu:

„9a. Rozbudowa i modernizacja infrastruktury teleinformatycznej CSIRT NASK służącej realizacji jego zadań może być dofinansowana w formie dotacji celowej ze środków budżetu państwa, których dysponentem jest minister właściwy do spraw informatyzacji.

k) w ust. 11 wyrazy „Ministra Cyfryzacji” zastępuje się wyrazami „ministra właściwego do spraw informatyzacji”,

l) dodaje się ust. 12 w brzmieniu:

„12. Minister Obrony Narodowej, Szef Agencji Bezpieczeństwa Wewnętrznego lub minister właściwy do spraw informatyzacji informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w ust. 10. Pełnomocnik

publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”;

25) użyte w art. 26 w ust. 3 w pkt 16 oraz w art. 49 w ust. 3 w pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”;

26) w art. 31:

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

„1a. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w 20d ust. 1 pkt 2, a także uzgodnią sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji – w przypadku braku możliwości dokonania zgłoszenia albo przekazania tych informacji w postaci elektronicznej.”,

b) ust. 2 otrzymuje brzmienie:

„2. Komunikat zawierający informacje, o których mowa w ust. 1i 1a, 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. Komunikat podlega również publikacji w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.”;

27) w art. 32 ust. 4 otrzymuje brzmienie:

„4. CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy lub CSIRT Telco na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotów krajowego systemu cyberbezpieczeństwa mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.”;

28) w art. 33:

a) po ust. 1 dodaje się ust. 1a–1e w brzmieniu:

„1a. Badanie, o którym mowa w ust. 1, przeprowadza się także na pisemny wniosek Pełnomocnika lub przewodniczącego Kolegium, skierowany do organu prowadzącego lub nadzorującego właściwy zespół CSIRT.

1b. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, jest uprawniony do stosowania technik mających na celu: obserwację

i analizę pracy, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez urządzenie informatyczne lub oprogramowanie.

1c. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, badanych urządzeń i oprogramowania, które ograniczyłyby możliwość przeprowadzenia badania.

1d. Badanie, o którym mowa w ust. 1:

1) nie narusza autorskich praw osobistych oraz majątkowych, oraz

2) nie wymaga zgody licencjodawcy lub dysponenta urządzenia informatycznego, oprogramowania lub usługi cyfrowej.

1e. Postanowienia umów sprzeczne z art. 33 ust. 1–1d są nieważne.”,

b) ust. 2 otrzymuje brzmienie:

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

c) po ust. 4b dodaje się ust. 4c w brzmieniu:

„4c. Rekomendacje, o których mowa w ust. 4, a także informację o ich zmianie lub odwołaniu, Pełnomocnik publikuje w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.”;

d) w ust. 5 wyrazy „od dnia otrzymania rekomendacji” zastępuje się wyrazami „od dnia opublikowania rekomendacji w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika”

29) w art. 34 ust. 1 otrzymuje brzmienie:

„1. CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy, CSIRT Telco oraz SOC zewnętrzne współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.”;

30) po art. 34 dodaje się art. 34a i art. 34b w brzmieniu:

„Art. 34a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco przekazują informacje o incydentach telekomunikacyjnych Prezesowi UKE w celu realizacji obowiązków, o których mowa w art. 20h ust. 1 pkt 1.

2. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco raz na pół roku przygotowują sprawozdania dotyczące liczby i rodzajów poważnych incydentów telekomunikacyjnych Prezesowi UKE oraz Pełnomocnikowi.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT Telco uzgadniają z Prezesem UKE sposób i tryb przekazywania informacji, o których mowa w ust. 1.

Art. 34b. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują z Prezesem UKE oraz CSIRT Telco przy wykonywaniu ustawowych zadań.”;

31) w art. 35 ust. 5 otrzymuje brzmienie:

„5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać Pełnomocnikowi do publikacji na stronie podmiotowej Pełnomocnika w Biuletynie Informacji Publicznej informacje o podatnościach, incydentach krytycznych oraz o cyberzagrożeniach:

1) jeżeli przekazywanie tych informacji przyczyni się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów;
2) wyłącznie w zakresie niezbędnym do realizacji tych celów, oraz
3) jeżeli publikacja informacji nie będzie naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.”;

32) w art. 36:

a) ust. 2 otrzymuje brzmienie:

„2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, Pełnomocnika, ministra właściwego do spraw informatyzacji oraz Rządowego Centrum Bezpieczeństwa.”,

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

„2a. W posiedzeniach Zespołu może uczestniczyć Pełnomocnik.”,

c) w ust. 6 zdanie pierwsze otrzymuje brzmienie:

„Dyrektor Rządowego Centrum Bezpieczeństwa na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1,

zawiadamia niezwłocznie członków Zespołu i Pełnomocnika o terminie i miejscu posiedzenia Zespołu.”;

33) po art. 36 dodaje się art. 36a w brzmieniu:

„Art. 36a. W wypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie opinii Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.”;

34) po art. 36a dodaje się rozdział 6a i 6b w brzmieniu:

„Rozdział 6a

Zadania CSIRT INT

Art. 36b. 1. Do zadań CSIRT INT należy zapewnianie wsparcia w obsłudze incydentów zgłaszanych przez:

1) jednostki organizacyjne podległe Ministrowi Spraw Zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
2) Agencję Wywiadu.

2. W zakresie określonym w ust. 1 CSIRT INT współpracuje z CSIRT GOV.

3. Do zadań CSIRT INT w ramach wspierania podmiotów określonych w ust. 1 należy:

1) przyjmowanie zgłoszeń o incydentach w podmiotach publicznych;
2) reagowanie na incydenty w podmiotach publicznych;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo w podmiotach publicznych;
4) współpraca z podmiotami publicznymi w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;

5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty w podmiotach publicznych oraz wymiany informacji o cyberzagrożeniach;
6) zapewnianie dynamicznej analizy ryzyka i incydentów oraz wspomaganie podnoszenia świadomości o cyberzagrożeniach;
7) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych, podmiotów o których mowa w ust. 1, w szczególności przez:
   a) wykonywanie testów bezpieczeństwa w porozumieniu z podmiotami, o których mowa w ust. 1,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

Art. 36c. CSIRT INT niezwłocznie, nie później niż w ciągu 8 godzin, przekazuje zgłoszenie, o którym mowa w art. 22 ust. 1a, do CSIRT GOV.

Rozdział 6b

Ocena bezpieczeństwa

Art. 36d. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy albo CSIRT Telco mogą przeprowadzić ocenę bezpieczeństwa systemów informacyjnych wykorzystywanych przez podmioty krajowego systemu cyberbezpieczeństwa.

2. Ocena bezpieczeństwa polega na przeprowadzeniu testów bezpieczeństwa systemu informacyjnego w celu identyfikacji podatności tego systemu.

3. Przepisów niniejszego rozdziału nie stosuje się do ocen bezpieczeństwa systemów teleinformatycznych:

1) podmiotów krajowego systemu cyberbezpieczeństwa, które znajdują się w zbiorze organów i podmiotów wymienionych w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. 2022 r. poz. 557 i 1488);

2) akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742 oraz z 2022 r. poz. 655 i 1933).

4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest:

1) w przypadku podmiotów określonych w art. 26 ust. 5 – CSIRT MON;

2) w przypadku podmiotów określonych w art. 26 ust. 6 pkt 1 lit. a–k i pkt 1a – CSIRT NASK;

3) w przypadku podmiotów określonych w art. 26 ust. 7 pkt 1–4 – CSIRT GOV.

5. CSIRTMON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa.

6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego operatora usługi kluczowej za zgodą właściwego CSIRT GOV, CSIRT MON lub CSIRT NASK. O zamiarze przeprowadzenia oceny bezpieczeństwa CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora.

7. CSIRT INT może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu, o którym mowa w art. 36b ust. 1, za zgodą CSIRT GOV.

8. CSIRT Telco może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego przedsiębiorcy komunikacji elektronicznej za zgodą właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. O zamiarze przeprowadzenia oceny bezpieczeństwa CSIRT Telco informuje Prezesa UKE.

Art. 36e. 1. Ocena bezpieczeństwa może być przeprowadzona za zgodą podmiotu krajowego systemu cyberbezpieczeństwa wyrażoną w formie pisemnej lub elektronicznej pod rygorem nieważności.

2. Ocena bezpieczeństwa powinna być prowadzona z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie.

3. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa.

4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodek karny (Dz. U. z

2022 r. poz. 1138, 1726 i 1855), oraz ich używać w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, o których mowa w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a Kodeksu karnego.

5. Używając urządzeń lub programów komputerowych, o których mowa w ust. 4, CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco może uzyskać dostęp do informacji dla niej nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, lub może uzyskać dostęp do całości lub części systemu informacyjnego.

6. Informacje uzyskane przez CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco w wyniku przeprowadzania oceny bezpieczeństwa stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRTMON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe i CSIRT Telco oraz podlegają one niezwłocznemu, komisyjnemu i protokolarnemu zniszczeniu.

7. Po przeprowadzeniu oceny bezpieczeństwa CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe albo CSIRT Telco sporządza i przekazuje podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa czynności oraz wskazanie wykrytych podatności systemu informacyjnego.

Art. 36f. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy albo CSIRT Telco informuje niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych.

Art. 36g. Rada Ministrów może określić, w drodze rozporządzenia sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36e ust. 6, a także wzory niezbędnych druków, mając na uwadze rodzaj materiałów podlegających zniszczeniu.”;

35) w art. 37 ust. 1–3 otrzymują brzmienie:

„1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz.

902) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. poz. 1641 oraz z 2022 r. poz. 1700).

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent operatorem usługi kluczowej, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, 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, przekazać Pełnomocnikowi do udostępnienia na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika, 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.”;

36) w art. 39:

a) w ust. 1 wyrazy „CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco przetwarzają dane pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami”,

b) użyte w ust. 2 oraz w ust. 5–9, w różnej liczbie wyrazy „i sektorowe zespoły cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie wyrazami „CSIRT sektorowy i CSIRT Telco”,

c) w ust. 3:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT, CSIRT sektorowe i CSIRT Telco przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami:”,

– pkt 2 otrzymuje brzmienie:

„2) dotyczące telekomunikacyjnych urządzeń końcowych;”,

– po w pkt 4 kropkę zastępuje się średnikiem i dodaje się pkt 5 w brzmieniu:

„5) gromadzone przez przedsiębiorców komunikacji elektronicznej w związku ze świadczeniem usług komunikacji elektronicznej.”,

d) w ust. 4:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes UKE przetwarzają dane osobowe pozyskane w związku z incydentami, incydentami telekomunikacyjnymi i cyberzagrożeniami:”,

– w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) gromadzone przez przedsiębiorców komunikacji elektronicznej.”,

e) ust. 5 i 6 otrzymują brzmienie:

„5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco 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, art. 36b–36c, art. 44 ust. 1–3 oraz art. 44a ust. 3–5.

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, art. 44 ust. 1–3 oraz art. 44a ust. 3–5, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK, CSIRT INT, CSIRT sektorowy, CSIRT Telco w terminie 5 lat od zakończenia obsługi incydentu lub incydentu telekomunikacyjnego, którego dotyczą.”,

f) w ust. 7 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT, CSIRT Telco”,

g) w ust. 8 i 9 po wyrazach „CSIRT MON, CSIRT NASK” dodaje się wyrazy „CSIRT Telco”,

h) po ust. 9 dodaje się ust. 10 w brzmieniu:

„10. Dane, o których mowa w ust. 4, są usuwane lub anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika, organy właściwe do spraw cyberbezpieczeństwa oraz Prezesa UKE

niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z niniejszej ustawy.”;

37) w art. 40:

a) w ust. 1 wyrazy „CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco”,

b) w ust. 2 i 3 wyrazy „CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT GOV, CSIRT INT, CSIRT sektorowy i CSIRT Telco”;

38) w art. 42:

a) w ust. 1:

– pkt 4 otrzymuje brzmienie:

„4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych bezzwłocznie, nie później niż w terminie 1 miesiąca od zmiany tych danych;”,

– w pkt 5 wyrazy „CSIRT NASK, CSIRT GOV, CSIRT MON” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT INT”,

– w pkt 7 wyrazy „CSIRT NASK, CSIRT GOV lub CSIRT MON” zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT”,

b) w ust. 8 wyrazy „Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”;

39) po art. 43 dodaje się oznaczenie rozdziału 8a w brzmieniu:

„Rozdział 8a

CSIRT sektorowy i CSIRT Telco”;

40) w art. 44:

a) ust. 1 otrzymuje brzmienie:

„1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla operatorów usług kluczowych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 do ustawy, do którego zadań należy:

1) przyjmowanie zgłoszeń o incydentach;

2) reagowanie na incydenty;

3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo systemów informacyjnych;

4) współpraca z operatorami usług kluczowych w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;
6) współpraca z innymi CSIRT sektorowymi oraz CSIRT INT w zakresie wymiany informacji o podatnościach i cyberzagrożeniach;
7) współpraca z CSIRT Telco w reagowaniu na incydenty poważne, będącymi również poważnymi incydentami telekomunikacyjnymi.”,

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

„1a. CSIRT sektorowy niezwłocznie, nie później niż 8 godzin od jego otrzymania, przekazuje zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4 do właściwego CSIRTMON, CSIRT NASK albo CSIRT GOV.

1b. CSIRT sektorowy może, w szczególności:

1) zapewniać we współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV dynamiczną analizę ryzyka i analizę incydentów oraz wspomagać w podnoszeniu świadomości cyberzagrożeń wśród operatorów usług kluczowych danego sektora lub podsektora;
2) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z operatorami usług kluczowych obsługę incydentów, które ich dotyczą;
3) wspierać, w uzgodnieniu z operatorem usługi kluczowej, wykonywanie przez niego obowiązków określonych w art. 11 ust. 1–3, art. 12 i art. 13;
4) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie operatora usługi kluczowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRTMON, CSIRT NASK albo CSIRT GOV;
5) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w danym sektorze lub podsektorze, w szczególności przez:

a) wykonywanie oceny bezpieczeństwa,

b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach,

c) uchyla się ust. 2,

d) ust. 4 otrzymuje brzmienie:

„4. Organ właściwy do spraw cyberbezpieczeństwa informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań.”,

e) dodaje się ust. 5–11 w brzmieniu:

„5. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego jednostkom jemu podległym albo przez niego nadzorowanym albo organowi przez niego nadzorowanemu.

6. Organ właściwy do spraw cyberbezpieczeństwa może, w drodze porozumienia, wyznaczyć spośród jednostek jemu podległych albo przez niego nadzorowanych jednostkę, która będzie wykonywała zadania CSIRT sektorowego dla kilku sektorów lub podsektorów. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu zasady odpowiedzialności za zadania oraz sprawowania nadzoru nad CSIRT sektorowym.

7. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT MON, CSIRT NASK albo CSIRT GOV realizację zadania lub zadań CSIRT sektorowego.

8. Powierzenie, o którym mowa w ust. 7, następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa:

1) w przypadku powierzenia zadań CSIRT NASK – za zgodą ministra właściwego do spraw informatyzacji – z Dyrektorem Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytutem Badawczym;

2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego;

3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.

9. W porozumieniu, o którym mowa w ust. 8, określa się zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym

wykonywaniem powierzonych zadań, zasady odpowiedzialności oraz zasady finansowania.

10. Komunikat o zawarciu porozumienia, o którym mowa w ust. 6 i 8, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa. W komunikacie wskazuje się:

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

11. Organ właściwy do spraw cyberbezpieczeństwa, informuje Pełnomocnika, o zawarciu porozumienia, o którym mowa w ust. 6 i 8. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.”;

41) po art. 44 dodaje się art. 44a i art. 44b w brzmieniu:

„Art. 44a. 1. Prezes UKE zapewnia funkcjonowanie CSIRT Telco.

2. Prezes UKE może powierzyć jednostce podległej lub nadzorowanej przez ministra właściwego do spraw informatyzacji prowadzenie CSIRT Telco – za zgodą tego ministra. Powierzenie następuje na podstawie porozumienia, w którym określa się zasady sprawowania przez Prezesa UKE kontroli nad prawidłowym wykonywaniem powierzonych zadań oraz zasady finansowania. Art. 44 ust. 10 i 11 stosuje się odpowiednio.

3. Do zadań CSIRT Telco w ramach wspierania przedsiębiorców komunikacji elektronicznej należy:

1) przyjmowanie zgłoszeń o incydentach telekomunikacyjnych;
2) reagowanie na incydenty telekomunikacyjne;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach, które mogą mieć negatywny wpływ na bezpieczeństwo sieci i usług komunikacji elektronicznej;
4) współpraca z przedsiębiorcami komunikacji elektronicznej w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach , organizacja i uczestnictwo w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie wymiany informacji i reagowania na incydenty telekomunikacyjne i krytyczne oraz wymiany informacji o cyberzagrożeniach;

6) współpraca z CSIRT sektorowymi w reagowaniu na poważne incydenty telekomunikacyjne, będącymi również incydentami poważnymi;
7) współpraca z organem właściwym do spraw ochrony danych osobowych podczas reagowania na incydent telekomunikacyjny, który doprowadził do naruszenia ochrony danych osobowych.

4. CSIRT Telco może, w szczególności:
1) zapewniać dynamiczną analizę ryzyka i incydentów telekomunikacyjnych oraz wspomagać podnoszenie świadomości cyberzagrożeń;
2) koordynować w uzgodnieniu z przedsiębiorcami komunikacji elektronicznej obsługę incydentów telekomunikacyjnych, które dotyczą różnych przedsiębiorców komunikacji elektronicznej;
3) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa sieci lub usług komunikacji elektronicznej przez:
   a) wykonywanie oceny bezpieczeństwa,
   b) identyfikowanie podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamianie właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach.

5. CSIRT Telco niezwłocznie, nie później niż 8 godzin od jego otrzymania, przekazuje zgłoszenie, o którym mowa w art. 20d ust. 1 pkt 2 do właściwego CSIRTMON, CSIRT NASK albo CSIRT GOV.
6. CSIRT Telco może zwrócić się do Prezesa UKE o wezwanie przedsiębiorcy komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego.
7. CSIRT Telco publikuje na swojej stronie internetowej i na stronie podmiotowej Biuletynu Informacji Publicznej CSIRT Telco komunikat zawierający informacje, o których mowa w art. 31 ust. 1a.

Art. 44b 1. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego. W sprawozdaniu za rok, w którym utworzony został CSIRT sektorowy, zawiera się informacje dotyczące jego utworzenia oraz funkcjonowania.

2. Prezes UKE raz w roku, do dnia 31 stycznia roku następującego po roku sprawozdawczym, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania

CSIRT Telco. W sprawozdaniu za rok, w którym utworzony został CSIRT Telco, zawiera się informacje dotyczące jego utworzenia oraz funkcjonowania.”;

42) w art. 45 w ust. 1 w pkt 6 w lit. c kropkę zastępuje się średnikiem i dodaje się pkt 7 i 8 w brzmieniu:

„7) wydawanie poleceń zabezpieczających;

8) prowadzenie postępowań w sprawie uznania dostawcy za dostawcę wysokiego ryzyka.”;

43) w art. 46:

a) ust. 2 otrzymuje brzmienie:

„2. Pełnomocnik, CSIRTMON, CSIRT NASK i CSIRT GOV korzystają z systemu teleinformatycznego, o którym mowa w ust. 1.”,

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

„2a. CSIRT sektorowe, CSIRT INT, CSIRT Telco, Prezes UKE korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie swojej właściwości.

2b. Operatorzy usług kluczowych korzystają z systemu teleinformatycznego, o którym mowa w ust. 1, w zakresie niezbędnym do realizowania obowiązków, o których mowa w rozdziale 3.

2c. Szczegółowe zasady korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, określa porozumienie zawarte pomiędzy ministrem właściwym do spraw informatyzacji a podmiotem, o którym mowa w ust. 2–2b.

2d. Podmioty krajowego systemu cyberbezpieczeństwa, inne niż wskazane w ust. 2–2b, mogą korzystać z systemu teleinformatycznego, o którym mowa w ust. 1, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji.”,

c) uchyla się ust. 3;

44) w art. 48 w pkt 1 po wyrazach „CSIRT GOV” dodaje się wyrazy „CSIRT INT”;

45) w art. 51:

a) pkt 5 otrzymuje brzmienie:

„5) kierowanie, za pośrednictwem CSIRT MON, działaniami związanymi z obsługą incydentów w czasie stanu wojennego oraz w czasie wojny;”,

b) pkt 7 otrzymuje brzmienie:

„7) ocenę cyberzagrożeń oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;”;

46) po art. 52 dodaje się art. 52a w brzmieniu:

„Art. 52a. W celu zabezpieczenia realizacji przewidzianych w ustawie zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, o których mowa w art. 36a, art. 42 w zw. z art. 41 pkt 6, 9 i 11, art. 44 ust. 8 pkt 3, art. 51, art. 52 i art. 67e ust. 1, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.”;

47) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych, SOC zewnętrznych i przedsiębiorców komunikacji elektronicznej”;

48) w art. 53:

a) w ust. 1:

– pkt 1 otrzymuje brzmienie:

„1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi SOC zewnętrznego, o którym mowa w art. 2 pkt 37, wymogów, o których mowa w art. 14 ust. 3–7 oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b;”,

– w pkt 2 lit. a i b otrzymują brzmienie:

„a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania cyberzagrożeniom i zgłaszania incydentów poważnych oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b,

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 oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b;”,

– dodaje się pkt 3 w brzmieniu:

„3) Prezes UKE w zakresie wypełniania przez przedsiębiorców komunikacji elektronicznej obowiązków określonych w art. 20a ust. 2 i 3, art. 20b ust. 2 i 4, art. 20d ust. 1 i art. 20f oraz wykonywania obowiązków, o których mowa w art. 66b, art. 66c i art. 67b.”,

b) w ust. 2 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3 w brzmieniu:

„3) Prezes UKE prowadzi kontrole w zakresie, o którym mowa w ust. 1 w pkt 3, oraz nakłada kary pieniężne na przedsiębiorców komunikacji elektronicznej.”;

49) w art. 54 dodaje się ust. 3 w brzmieniu:

„3. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 3, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.”;

50) po art. 54 dodaje się art. 54a w brzmieniu:

„Art. 54a. Prezes UKE może, po otrzymaniu wniosku od CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT Telco wezwać przedsiębiorcę komunikacji elektronicznej do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu telekomunikacyjnego lub krytycznego.”;

51) w art. 56 dodaje się ust. 3 w brzmieniu:

„3. Organ przeprowadzający kontrolę może żądać od podmiotu kontrolowanego przedstawienia tłumaczenia na język polski sporządzonej w języku obcym dokumentacji przedłożonej przez podmiot kontrolowany. Tłumaczenie dokumentacji podmiot kontrolowany jest obowiązany wykonać na własny koszt.”;

5) art. 59 otrzymuje brzmienie:

„Art. 59 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy do spraw cyberbezpieczeństwa, minister właściwy do spraw informatyzacji lub Prezes UKE 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, ministra właściwego do spraw informatyzacji lub Prezesa UKE o sposobie wykonania zaleceń.”;

53) po rozdziale 11 dodaje się rozdział 11a w brzmieniu:

„Rozdział 11a

Krajowy system certyfikacji cyberbezpieczeństwa

Art. 59a. 1. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:

1) ministra właściwego do spraw informatyzacji;
2) Polskie Centrum Akredytacji;
3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;
4) dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje wyroby procesowi oceny zgodności zgodnie z ustawą.

2. Nadzór nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa sprawuje minister właściwy do spraw informatyzacji.

Art. 59b. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:

1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z certyfikacją cyberbezpieczeństwa;
2) monitorowanie stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;
3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59a ust. 1 pkt 3 i 4;
4) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;
5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;
6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”;
7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania „wysoki”;
8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;

9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonymi europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym programie certyfikacji cyberbezpieczeństwa;
10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez nie działań związanych z certyfikacją cyberbezpieczeństwa;
11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;
12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG", corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b–d oraz ust. 8 rozporządzenia 2019/881;
13) uczestniczenie w pracach ECCG;
14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;
15) nadzorowanie i egzekwowanie zawartych w europejskim programie certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;
16) przeprowadzanie badań certyfikownych produktów ICT, usług ICT lub procesów ICT.

Art. 59c. 1. Polskie Centrum Akredytacji sprawuje nadzór w zakresie udzielonej akredytacji nad akredytowanymi jednostkami prowadzącymi ocenę zgodności produktów ICT, usług ICT lub procesów ICT w obszarze cyberbezpieczeństwa, przy uwzględnieniu wymagań, o których mowa w art. 22 ust. 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854) oraz specyficznych wymagań podanych w:

1) załączniku do rozporządzenia 2019/881;
2) poszczególnych europejskich programach certyfikacji cyberbezpieczeństwa i krajowych programach certyfikacji cyberbezpieczeństwa.

Art. 59d. 1. Minister właściwy do spraw informatyzacji przygotowuje projekt krajowego programu certyfikacji cyberbezpieczeństwa lub zleca jego przygotowanie jednostkom jemu podległym lub przez niego nadzorowanym.

2. Rada Ministrów może określić, w drodze rozporządzenia, krajowy program certyfikacji cyberbezpieczeństwa dla danego produktu ICT, usługi ICT lub procesu ICT, uwzględniając konieczność opracowania wymagań dla produktów ICT, usług ICT lub procesów ICT zgodnie z aktualną wiedzą naukowo–techniczną oraz mając na celu zwiększenie cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

Art. 59e. 1. Podmiot ubiegający się o certyfikat lub posiadający certyfikat wydany na podstawie krajowego programu certyfikacji cyberbezpieczeństwa jest obowiązany wykonywać obowiązki określone w tym programie.

2. Obowiązki, o których mowa w ust. 1, mogą obejmować w szczególności:

1) udostępnianie informacji niezbędnych do przeprowadzenia certyfikacji;
2) przeprowadzanie okresowych badań produktów ICT, usług ICT, procesów ICT;
3) przeprowadzanie aktualizacji oprogramowania;
4) przeprowadzanie okresowych testów cyberbezpieczeństwa;
5) określony sposób przechowywania dokumentacji związanej z produktem ICT, usługą ICT lub procesem ICT;
6) określony sposób postępowania z wykrytymi podatnościami, w szczególności ich eliminację.

Art. 59f. 1. Tryb postępowań certyfikacyjnych produktów ICT, usług ICT lub procesów ICT może zostać określony w krajowym programie certyfikacji cyberbezpieczeństwa opracowanych odpowiednio dla produktów ICT, usług ICT albo procesów ICT.

2. Krajowy program certyfikacji cyberbezpieczeństwa zawiera:

1) przedmiot i zakres programu certyfikacji, w tym rodzaj lub kategorie objętych danym programem produktów ICT, usług ICT lub procesów ICT, określenie przedmiotu i zakresu programu certyfikacji;
2) opis celu programu oraz wpływu wybranych norm, metod oceny i krajowych poziomów uzasadnienia zaufania na realizację potrzeb przewidywanych użytkowników programu;
3) wskazanie, czy w ramach programu dozwolone jest wydanie deklaracji zgodności;

4) szczegółowe lub dodatkowe wymogi, którym podlegają jednostki oceniające zgodność w celu zagwarantowania ich kwalifikacji technicznych odnośnie do oceny wymogów cyberbezpieczeństwa;
5) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte cele w zakresie cyberbezpieczeństwa;
6) zakres informacji niezbędnych do uzyskania certyfikatu, które wnioskodawca ma dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność;
7) w przypadku gdy program przewiduje stosowanie znaków lub etykiet poświadczających zgodność z programem – określenie warunków, na jakich takie znaki lub etykiety mogą być stosowane;
8) sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymogami krajowych certyfikatów cyberbezpieczeństwa lub deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;
9) szczegółowe warunki wydawania, utrzymywania, przedłużania i odnawiania ważności krajowych certyfikatów cyberbezpieczeństwa;
10) skutki dla produktów ICT, usług ICT lub procesów ICT, które uzyskały krajowy certyfikat cyberbezpieczeństwa lub w przypadku których wydana została deklaracja zgodności, które nie spełniają wymogów programu;
11) szczegółowy sposób zgłaszania uprzednio niewykrytych, a wpływających na cyberbezpieczeństwo podatności produktów ICT, usług ICT lub procesów ICT, do jego dostawcy oraz sposobu postępowania z nimi;
12) instrukcje dotyczące przechowywania dokumentów przez jednostki oceniające zgodność;
13) treść i wzór graficzny krajowych certyfikatów cyberbezpieczeństwa i krajowych deklaracji zgodności okres dostępności krajowych deklaracji zgodności, dokumentacji technicznej oraz innych istotnych informacji;
14) okres ważności krajowych certyfikatów cyberbezpieczeństwa;
15) sposób dostarczania i aktualizowania dodatkowych informacji na temat cyberbezpieczeństwa przez dostawców sprzętu lub oprogramowania zgodnie z art. 59u.

3. Dostawca certyfikowanych produktów ICT, usług ICT lub procesów ICT lub ubiegający się o uzyskanie certyfikatu jest obowiązany dostarczyć lub udostępnić w inny sposób jednostkom oceniającym zgodność informacje, o których mowa w ust. 2 pkt 6 i 15.

Art. 59g. 1. Krajowy program certyfikacji cyberbezpieczeństwa wskazuje jeden lub więcej krajowych poziomów uzasadnienia zaufania produktów ICT, usług ICT lub procesów ICT. Wyróżnia się następujące poziomy uzasadnienia zaufania:

1) podstawowy;
2) istotny;
3) wysoki.

2. Krajowy poziom uzasadnienia zaufania:

1) podstawowy – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa lub wydana została krajowa deklaracja zgodności, spełniają odpowiadające im wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków;
2) istotny – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk wystąpienia incydentów i cyberataków przeprowadzanych przez osoby dysponujące niezaawansowanym sprzętem oraz podstawowymi umiejętnościami w zakresie przełamywania zabezpieczeń systemów informacyjnych;
3) wysoki – potwierdza, że produkty ICT, usługi ICT lub procesy ICT, dla których wydany został krajowy certyfikat cyberbezpieczeństwa, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach w zakresie przełamywania zabezpieczeń systemów informacyjnych lub dysponujące zawansowanym sprzętem.

3. Minimalne działania w zakresie oceny danego produktu ICT, usługi ICT czy procesu ICT obejmują:

1) w przypadku krajowego poziomu uzasadnienia zaufania „podstawowy” – przegląd dokumentacji technicznej lub działania o równoważnym skutku;
2) w przypadku krajowego poziomu uzasadnienia zaufania „istotny” – sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności oraz testowanie w celu wykazania, że w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa lub działania o równoważnym skutku;
3) w przypadku krajowego poziomu uzasadnienia zaufania „wysoki” – sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, testowanie, czy w produktach ICT, usługach ICT lub procesach ICT prawidłowo zaimplementowane zostały niezbędne, nowoczesne funkcjonalności bezpieczeństwa oraz ocenę sprawdzającą za pomocą testów penetracyjnych ich odporność na zaawansowane atak lub działania o równoważnym skutku.

Art. 59h. 1. Oceny zgodności w obszarze cyberbezpieczeństwa dokonuje jednostka oceniająca zgodność akredytowana z uwzględnieniem specyficznych wymagań określonych w art. 59c, posiadająca zakres akredytacji obejmujący ocenę zgodności produktów ICT, usług ICT lub procesów ICT, właściwą dla tego obszaru.

2. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji. 3. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.

4. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji niezwłocznie o udzielonej akredytacji z zakresu krajowych programów certyfikacji cyberbezpieczeństwa i europejskich programów certyfikacji cyberbezpieczeństwa.

5. Informacja o udzielonej akredytacji, o której mowa w ust. 2, zawiera:

1) oznaczenie podmiotu, któremu udzielono akredytacji;
2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.

6. Akredytacji udziela się na okres nie dłuższy niż 5 lat.

7. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji niezwłocznie o cofnięciu akredytacji jednostce oceniającej zgodność.

8. Informacja o cofnięciu akredytacji jednostce oceniającej zgodność zawiera:

1) oznaczenie podmiotu, któremu cofnięto akredytację;
2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;

3) wskazanie daty cofnięcia akredytacji.

Art. 59i. 1. W przypadku, gdy:

1) europejski program certyfikacji cyberbezpieczeństwa określa szczegółowe lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881,
2) krajowy program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 59f ust. 2 pkt 4

– czynności w ramach oceny zgodności dokonywanej na ich podstawie dokonuje tylko jednostka oceniająca zgodność posiadająca zezwolenie ministra do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji, w drodze decyzji, zezwala na wykonywanie przez jednostkę oceniającą zgodność zadań w ramach programów certyfikacji cyberbezpieczeństwa, o których mowa w ust. 1, na wniosek jednostki oceniającej zgodność, która spełniła wymogi określone w tych programach.

3. Minister właściwy do spraw informatyzacji może z urzędu cofnąć, ograniczyć albo zawiesić zezwolenie, o którym mowa w ust. 1, jeśli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego programu certyfikacji cyberbezpieczeństwa. Cofnięcie, ograniczenie albo zawieszenie zezwolenia następuje w drodze decyzji.

4. Do postępowań, o których mowa w ust. 2, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 59j. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności.

2. Ocena zgodności jest dobrowolna.

3. Warunki techniczne przeprowadzania oceny zgodności określają europejskie programy certyfikacji cyberbezpieczeństwa lub krajowe programy certyfikacji cyberbezpieczeństwa.

Art. 59k. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem:

1) deklaracji zgodności – badaniom przez dostawcę sprzętu lub oprogramowania, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy;
2) certyfikatu – ocenie zgodności przez jednostkę oceniającą zgodność, w zakresie właściwym do danego programu certyfikacji cyberbezpieczeństwa.

Art. 59l. 1. Wniosek o certyfikację produktu ICT, usługi ICT lub procesu ICT składa jego dostawca do jednostki oceniającej zgodność.

2. Wniosek o certyfikację zawiera co najmniej:

1) nazwę albo imię i nazwisko wnioskującego oraz wskazanie adresu jego siedziby, adresu miejsca prowadzenia działalności gospodarczej albo adresu zamieszkania;
2) informacje potwierdzające spełnianie kryteriów certyfikacji;
3) wskazanie zakresu wnioskowanej certyfikacji.

3. Do wniosku dołącza się dokumenty potwierdzające spełnianie wymagań określonych we właściwym programie certyfikacyjnym.

4. Wniosek składa się na piśmie w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.

Art. 59m. Jednostka oceniająca zgodność niezwłocznie przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, dane podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia albo dane podmiotu, któremu odmówiono wydania certyfikatu wraz ze wskazaniem przyczyn odmowy.

Art. 59n. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji przesyła, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 2 ustawy z dnia 7 października 2020 r. o doręczeniach elektronicznych (Dz. U. z 2022 r. poz. 569 i 1002) do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:

1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania „wysoki”;
2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania „wysoki”.

2. Minister właściwy do spraw informatyzacji:

1) zatwierdza certyfikat, o którym mowa w ust. 1;
2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z ustawą, rozporządzeniem 2019/881 lub programami, o których mowa w ust. 1.

3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego

europejskiego programu certyfikacji cyberbezpieczeństwa lub krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.

4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg procesu oceny zgodności.

5. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy może zasięgnąć opinii nadzorowanego instytutu badawczego w zakresie zgodności certyfikacji z programem. Instytut badawczy przekazuje opinię w terminie 1 miesiąca od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

6. Minister właściwy do spraw informatyzacji cofa certyfikat, jeśli jest on niezgodny z ustawą, rozporządzeniem 2019/881, europejskim programem certyfikacji cyberbezpieczeństwa lub krajowym programem certyfikacji cyberbezpieczeństwa.

7. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

Art. 59o. W przypadku stwierdzenia, że podmiot ubiegający się o uzyskanie certyfikatu nie spełnia kryteriów oceny zgodności, jednostka oceniająca zgodność odmawia jej dokonania, wskazując brak spełnienia kryteriów certyfikacji.

Art. 59p. 1. Dokumentem potwierdzającym certyfikację jest certyfikat.

2. Certyfikat zawiera co najmniej:

1) oznaczenie podmiotu, który otrzymał certyfikat;
2) nazwę podmiotu dokonującego certyfikacji oraz wskazanie adresu jego siedziby;
3) oznaczenie produktu ICT, usługi ICT lub procesu ICT podlegającego certyfikacji;
4) numer lub oznaczenie certyfikatu;
5) zakres certyfikacji;
6) okres, na jaki została dokonana certyfikacja;
7) wskazanie poziomu uzasadnienia zaufania określonego w europejskim programie certyfikacji cyberbezpieczeństwa lub krajowego poziomu uzasadnienia zaufania określonego w krajowym programie certyfikacji cyberbezpieczeństwa;
8) datę wydania i podpis podmiotu dokonującego certyfikacji lub osoby przez niego upoważnionej.

3. Certyfikat, wydany w ramach krajowego programu certyfikacji cyberbezpieczeństwa, odwołuje się do związanych z produktem ICT, usługą ICT lub

procesem ICT specyfikacji technicznych, norm i procedur, w tym kontroli mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

4. Okres ważności krajowych certyfikatów cyberbezpieczeństwa określany jest na podstawie charakterystyki specyfikacji technicznej dla konkretnych produktów ICT, usług ICT lub procesów ICT.

Art. 59q. 1. W okresie, na jaki został wydany certyfikat, podmiot, któremu go wydano, jest obowiązany spełniać kryteria obowiązujące na dzień jego wydania.

2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji.

3. Jednostka oceniająca zgodność informuje niezwłocznie ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Art. 59r. 1. Dostawcy, który poddał produkt ICT, usługę ICT lub proces ICT ocenie zgodności z wymaganiami określonymi w krajowym programie certyfikacji cyberbezpieczeństwa i potwierdził ich zgodność, wydaje się krajową deklarację zgodności.

2. Krajowa deklaracja zgodności, odwołuje się do określonych w krajowym programie certyfikacji cyberbezpieczeństwa specyfikacji technicznych, norm i procedur, w tym kontroli mających na celu zmniejszenie ryzyka wystąpienia incydentów cyberbezpieczeństwa lub zapobieganie takim incydentom.

3. Produkt ICT, usługa ICT lub proces ICT spełniają wymagania określone w programie certyfikacji przez cały okres na jaki została wydana deklaracja zgodności.

4. Krajowa deklaracja zgodności wydawana jest wyłącznie dla produktów ICT, usług ICT lub procesów ICT odpowiadających wymaganiom dla krajowego poziomu uzasadnienia zaufania „podstawowy”.

Art. 59s. Po wydaniu deklaracji zgodności dostawca przesyła jej kopię ministrowi właściwemu do spraw informatyzacji, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych.

Art. 59t. Domniemywa się, że wyrób, dla którego wydano deklarację zgodności, jest zgodny z wymaganiami określonymi w obowiązujących krajowych programach

certyfikacji cyberbezpieczeństwa lub europejskich programach certyfikacji cyberbezpieczeństwa.

Art. 59u. 1. Dostawca produktów ICT, usług ICT lub procesów ICT, posiadających krajowy certyfikat cyberbezpieczeństwa produktów ICT, usług ICT lub procesów IT, dla których została wydana krajowa deklaracja zgodności, udostępnia publicznie informacje zawierające:

1) porady i zalecenia mające pomóc użytkownikom końcowym w bezpiecznej: konfiguracji, instalacji i obsłudze oraz w bezpiecznym uruchomieniu i utrzymaniu produktów ICT, usług ICT lub procesów ICT;
2) okres, w którym użytkownikom końcowym oferowane jest wsparcie w zakresie bezpieczeństwa, w szczególności pod względem dostępności aktualizacji związanych z cyberbezpieczeństwem;
3) informacje kontaktowe wytwórcy lub dostawcy oraz akceptowane sposoby otrzymywania informacji o podatnościach pochodzących od użytkowników końcowych i ekspertów w obszarze bezpieczeństwa;
4) odesłanie do repozytoriów internetowych zawierających wykaz podanych do wiadomości publicznej podatnościach związanych z produktami ICT, usługami ICT lub procesami ICT oraz innych poradników dotyczących cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, są aktualizowane co najmniej do czasu wygaśnięcia certyfikatu lub deklaracji zgodności.

Art. 59v. Podmiot, o którym mowa w art. 59a ust. 1 pkt 3 i 4, na wniosek ministra właściwego do spraw informatyzacji, przedstawia informacje dotyczące:

1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;
2) wszelkich kwestii związanych z funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa;
3) liczby wydanych certyfikatów, w tym programów, w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;
4) liczby wydanych deklaracji zgodności, w tym programów, w ramach których zostały wydane;
5) liczby i sposobu rozpatrzenia skarg, o których mowa w art. 59y.

Art. 59w. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59a ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.

2. Do kontroli, o której mowa w ust. 1, 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. 59x. Do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa przepisy art. 55–art. 59 stosuje się.

Art. 59y Minister właściwy do spraw informatyzacji, w ramach przeprowadzanej kontroli, może poddać produkt ICT, usługę ICT lub proces ICT, dla których został wydany certyfikat lub deklaracja zgodności, badaniom lub zlecić ich przeprowadzenie, w celu ustalenia, czy spełniają one wymagania określone w ustawie, rozporządzeniu 2019/881, europejskim programie certyfikacji cyberbezpieczeństwa lub krajowym programie certyfikacji cyberbezpieczeństwa.

Art. 59z. 1. Badanie, o którym mowa w art. 59y, może zostać przeprowadzone na próbkach produktu ICT.

2. Podmiot kontrolowany jest obowiązany do przekazania kontrolerom wskazanej przez nich próbki produktu ICT. Z przekazania próbki sporządza się protokół.

3. Jeżeli przeprowadzone badania wykazały, że produkt ICT nie spełnia wymagań określonych w programie certyfikacji, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości informację o niespełnianiu przez produkt ICT wymagań określonych w programie certyfikacji.

4. W przypadku certyfikatów zatwierdzanych przez ministra właściwego do spraw informatyzacji, minister właściwy do spraw informatyzacji uchyla decyzję o zatwierdzeniu certyfikatu.

5. Koszty badań, o których mowa w art. 59y, ponosi podmiot kontrolowany.

6. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, wzór protokołu, o którym mowa w ust. 2, uwzględniając w szczególności nazwę produktu ICT, oznaczenie certyfikatu wydanego dla tego produktu ICT, wielkość próbki przekazanej

do badania, dane identyfikujące produkt ICT, takie jak numer seryjny przekazanego jako próbka egzemplarza produktu ICT, datę przekazania próbki.

Art. 59za. 1. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że produkt ICT nie spełnia wymagań określonych w ustawie, rozporządzeniu 2019/881, europejskim programie certyfikacji cyberbezpieczeństwa lub krajowym programie certyfikacji cyberbezpieczeństwa informuje o tym podmiot, który wydał dany certyfikat.

2. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że produkt ICT, dla którego wydany został certyfikat odwołujący się do poziomu zaufania wysoki określony w europejskim programie certyfikacji cyberbezpieczeństwa lub krajowym programie certyfikacji cyberbezpieczeństwa może cofnąć certyfikat.

Art. 59zb. 1. Jednostki oceniające zgodność rozpatrują skargi w sposób i na zasadach określonych programie certyfikacji cyberbezpieczeństwa.

2. Skargę składa się do jednostki oceniającej zgodność w terminie 14 dni od dnia doręczenia rozstrzygnięcia. Jednostka oceniająca zgodność może określić dłuższy termin na złożenie skargi.

3. Jednostka oceniająca zgodność rozpatruje skargę w terminie nie dłuższym niż 2 miesiące.

4. Skargę rozpatrują osoby, które nie brały udziału w podejmowaniu rozstrzygnięcia, którego dotyczy skarga.

5. Jednostka oceniająca zgodność informuje skarżącego o stanie postępowania oraz o prawie skierowania sprawy do sądu na jego wniosek.

6. Jednostki oceniające zgodność publikują na swojej stronie internetowej informacje o procedurze postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881. Procedura rozpatrywania skarg określa termin załatwienia skargi oraz przebieg procesu jej rozpatrywania.

Art. 59zc. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:

1) podmiot, który wydał unijną lub krajową deklarację zgodności, jeśli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja dotyczy nie spełnia wymogów określonych w programie certyfikacji cyberbezpieczeństwa;
2) jednostkę oceniającą zgodność.

2. Minister rozpatruje skargi, o których mowa w ust. 1, w sposób i na zasadach określonych w programie certyfikacji cyberbezpieczeństwa, a w przypadku jeżeli program nie określa sposobu i zasad rozpatrywania skarg stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.”;

54) w art. 62 w ust. 1:

a) w pkt 1 i 2 wyrazy „CSIRT MON, CSIRT NASK i CSIRT GOV”" zastępuje się wyrazami „CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT INT i CSIRT sektorowy”,

b) w pkt 6 kropkę zastępuje się średnikiem i dodaje się pkt 7–8 w brzmieniu:

„7) wydawanie ostrzeżeń;

8) zwracanie się ze zleceniem, o którym mowa w art. 26 ust. 2a.”;

55) po art. 62 dodaje się art. 62a w brzmieniu:

„Art. 62a. 1. Pełnomocnik może wydawać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

2. Rekomendacje Pełnomocnika są udostępniane w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. Podmiot krajowego systemu cyberbezpieczeństwa uwzględnia rekomendacje w zarządzaniu ryzykiem, jeżeli zostały do niego skierowane.”;

56) art. 64 otrzymuje brzmienie:

„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, CSIRT sektorowych, CSIRT Telco, CSIRT INT, Prezesa UKE i organów właściwych do spraw cyberbezpieczeństwa.”;

57) po art. 64 dodaje się art. 64a w brzmieniu:

„Art. 64a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone

w art. 66a ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRTMON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 66a ust. 2, sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT.

3. Zadania, o których mowa w ust. 1 i 2, są wykonywane w ramach ustawowych zadań odpowiednio CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT INT.”;

58) w art. 65:

a) w ust. 1:

– pkt 2 otrzymuje brzmienie:

„2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, CSIRT sektorowe, CSIRT Telco, CSIRT INT, i organy właściwe do spraw cyberbezpieczeństwa powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania cyberzagrożeniom;”,

– pkt 4 otrzymuje brzmienie:

„4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego, Szefa Agencji Wywiadu oraz ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, CSIRT Telco, CSIRT INT i organów właściwych do spraw cyberbezpieczeństwa;”,

– w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8 w brzmieniu:

„8) decyzji o w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.”,

b) w ust. 2 przed wyrazami „Rady Ministrów” dodaje się wyraz „Prezesa”,

c) dodaje się ust. 3 w brzmieniu:

„3. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).”;

59) w art. 66:

a) w ust. 1 pkt 4 otrzymuje brzmienie:

„4) członkowie Kolegium:

a) minister właściwy do spraw wewnętrznych,

b) minister właściwy do spraw informatyzacji,

c) minister właściwy do spraw energii,

d) Minister Obrony Narodowej,

e) minister właściwy do spraw zagranicznych,

f) Szef Kancelarii Prezesa Rady Ministrów,

g) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,

h) 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,

i) Przewodniczący Komisji Nadzoru Finansowego,

j) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni,

k) Prokurator Generalny.”,

b) ust. 4 otrzymuje brzmienie:

„4. W posiedzeniach Kolegium uczestniczą również:

1) Dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;

2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;

3) Szef Agencji Wywiadu albo jego zastępca;

4) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;

5) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;

6) Szef Służby Wywiadu Wojskowego albo jego zastępca;

7) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego albo jego zastępca.”,

c) w ust. 5 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3–8 w brzmieniu:

„3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;

4) może zlecić CSIRTMON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT,

usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 64a ust. 1;

5) może zlecić CSIRTMON, CSIRT NASK, CSIRT GOV lub CSIRT INT, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprawuje nadzór nad procesem wytwarzania i dostarczania produktów ICT, usług ICT lub procesów ICT, o której mowa w art. 64a ust. 2;

6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 66a ust. 1;

7) powołuje zespół opiniujący, o którym mowa w art. 66a ust. 10 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład;

8) rozstrzyga spór, o którym mowa w art. 66a ust. 12 pkt 2, wskazując właściwego członka zespołu opiniującego.”,

d) w ust. 7 po wyrazach „CSIRT NASK,” dodaje się wyrazy „CSIRT INT,”;

60) po art. 66 dodaje się art. 66a–66e w brzmieniu:

„Art. 66a. 1. Minister właściwy do spraw informatyzacji, w celu ochrony bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, może wszcząć z urzędu albo na wniosek przewodniczącego Kolegium, postępowanie w sprawie uznania za dostawcę wysokiego ryzyka dostawcy sprzętu lub oprogramowania, które jest wykorzystywane przez:

1) podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 1–2, 3–20,

2) przedsiębiorców telekomunikacyjnych obowiązanych posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń,

3) właścicieli lub posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

– zwane dalej „postępowaniem w sprawie uznania za dostawcę wysokiego ryzyka”.

2. Dostawcą sprzętu lub oprogramowania, o którym mowa w ust. 1, jest dostawca produktów ICT, usług ICT lub procesów ICT.

3. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka stosuje się, jeżeli ustawa nie stanowi inaczej, przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks

postępowania administracyjnego, z wyłączeniem art. 28, art. 31, art. 51, art. 66a i art. 79 tej ustawy.

4. Stroną postępowania jest każdy wobec kogo zostało wszczęte postępowanie w sprawie uznania za dostawcę wysokiego ryzyka;

5. Do postępowania może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny, który w poprzednim roku obrotowym, uzyskał przychód z tytułu prowadzenia działalności telekomunikacyjnej w wysokości co najmniej dwudziestotysięcznej krotności przeciętnego wynagrodzenia w gospodarce narodowej, wskazanego w ostatnim komunikacie Prezesa Głównego Urzędu Statystycznego, o którym mowa w art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2022 r. poz. 504 i 1504). Przepisy art. 31 § 2 i § 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.

6. Za poprzedni rok obrotowy uznaje się rok, przed którym postępowanie zostało wszczęte. Za ostatni komunikat Prezesa Głównego Urzędu Statystycznego uznaje się ostatni komunikat Prezesa Głównego Urzędu Statystycznego przed wszczęciem postępowania.

7. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie, o którym mowa w zdaniu poprzedzającym, udostępnia się także w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji niezwłocznie po wpłynięciu do ministra właściwego do spraw informatyzacji potwierdzenia doręczenia tego zawiadomienia.

8. Zawiadomienie, o którym mowa w ust. 7, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, jeżeli dostawcą sprzętu lub oprogramowania jest strona niemająca siedziby na terytorium państwa członkowskiego Unii Europejskiej, Konfederacji Szwajcarskiej albo państwa członkowskiego Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania.

9. Minister właściwy do spraw informatyzacji przed rozstrzygnięciem sprawy zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Terminu od dnia wystąpienia o opinię do dnia otrzymania opinii nie

wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

10. Opinia, o której mowa w ust. 9 zdanie pierwsze, zawiera analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego;

2) prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego, z uwzględnieniem:

   a) przepisów prawa regulujących stosunki między dostawcą sprzętu lub oprogramowania, a tym państwem oraz praktyki stosowania prawa w tym zakresie,

   b) prawodawstwa oraz stosowania prawa w zakresie ochrony danych osobowych, w szczególności tam, gdzie nie ma porozumień w zakresie ochrony tych danych między Unią Europejską i tym państwem,

   c) struktury własnościowej dostawcy sprzętu lub oprogramowania,

   d) zdolności ingerencji tego państwa w swobodę działalności gospodarczej dostawcy sprzętu lub oprogramowania;

3) trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w załączniku do rozporządzenia Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz. Urz. UE L 129I z 17.5.2019, str. 1–12, z późn. zm.);

4) liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania;

5) tryb i zakres, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1 pkt 1–4, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;

6) treści wydanych wcześniej rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

11. Sporządzając opinię, o której mowa w ust. 7, Kolegium uwzględnia:

1) certyfikaty wydane dla produktów ICT, usług ICT lub procesów ICT, wydane lub uznawane w państwach członkowskich Unii Europejskiej lub Organizacji Traktatu Północnoatlantyckiego;
2) analizy, o których mowa w art. 64a ust. 1 i 2.

12. Procedura sporządzenia opinii, o której mowa w ust. 9, przebiega w następujący sposób:

1) przewodniczący Kolegium powołuje zespół w celu opracowania projektu opinii w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, zwany dalej „zespołem opiniującym”, w skład którego wchodzą przedstawiciele członków Kolegium wskazani przez przewodniczącego Kolegium;
2) każdy członek zespołu opiniującego przygotowuje stanowisko, w zakresie swojej właściwości, na podstawie analizy, o której mowa w ust. 10, które następnie przekazuje zespołowi, o którym mowa w pkt 1. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego;
3) jeżeli nie zostały wykonane analizy, o których mowa w art. 64a ust. 1 i 2, Przewodniczący Kolegium zleca ich wykonanie;
4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
5) uzgodnienie opinii następuje na posiedzeniu Kolegium;
6) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

13. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.

14. Decyzja, o której mowa w ust. 13, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.

15. Minister właściwy do spraw informatyzacji ogłasza decyzję, o której mowa w ust. 13, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” oraz udostępnia w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji, a także na stronie internetowej urzędu obsługującego tego ministra.

16. Decyzja, o której mowa w ust. 13, podlega natychmiastowemu wykonaniu.

17. Od decyzji, o której mowa w ust. 13, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 66b. 1. W przypadku wydania decyzji, o której mowa w art. 66a ust. 13, podmioty, o których mowa w art. 66a ust. 1:

1) nie wprowadzają do użytkowania typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka;

2) wycofują z użytkowania typy produktów ICT, rodzaje usług ICT i konkretne procesy ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13.

2. Przedsiębiorcy telekomunikacyjni obowiązani posiadać aktualne i uzgodnione plany działań w sytuacjach szczególnych zagrożeń, wycofują w ciągu 5 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 i 2, dopuszcza się użytkowanie dotychczas posiadanych typów produktów ICT, rodzajów usług ICT i konkretnych procesów ICT w zakresie objętym decyzją, dostarczanych przez dostawcę wysokiego ryzyka, w zakresie naprawy, modernizacji, wymiany elementu lub aktualizacji, jeśli jest to niezbędne dla zapewnienia odpowiedniej jakości i ciągłości świadczonych usług, w szczególności dokonywania niezbędnych napraw awarii lub uszkodzeń.

4. Podmioty, o których mowa w art. 66 ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, 1812 i 1933), nie mogą nabywać sprzętu, oprogramowania i usług określonych w decyzji, o której mowa w art. 66a ust. 13.

5. W przypadku gdy podmioty, o których mowa w art. 66 ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13, produkt, usługę lub proces określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 66a ust. 13, a w przypadku produktów, usług lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 5 lat.

Art. 66c. 1. Podmioty, o których mowa w art. 66 ust. 1, są obowiązane przekazać informacje na wniosek uprawnionych organów, o których mowa w ust. 2, o wycofywanych typach produktów ICT, rodzajach usług ICT i konkretnych procesach ICT w zakresie objętym decyzją, o której mowa w art. 66a ust. 13.

2. Uprawnionymi organami do żądania informacji, o których mowa w ust. 1, są wobec:

1) operatorów usług kluczowych i dostawców usług cyfrowych – organy właściwe do spraw cyberbezpieczeństwa;
2) SOC zewnętrznych – minister właściwy do spraw informatyzacji;
3) przedsiębiorców telekomunikacyjnych – Prezes UKE;
4) podmiotów publicznych – właściwe organy nadzorcze lub minister właściwy do spraw informatyzacji;
5) właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym – ministrowie kierujący działami administracji rządowej i kierownicy urzędów centralnych odpowiedzialnych za systemy, o których mowa w art. 3 pkt 2 tej ustawy

3. Wniosek zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę wydania;
3) wskazanie zakresu żądanych informacji;
4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, nie krótszego niż 7 dni;
5) uzasadnienie
6) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 2d.

4. Minister właściwy do spraw informatyzacji może zwrócić się do uprawnionych organów, o których mowa w ust. 2 pkt 1 lub ust. 2 pkt 3–6, o żądanie informacji, o których mowa w ust. 1.

Art. 66d. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 66a ust. 13, na posiedzeniu niejawnym w składzie trzech sędziów.

2. Odpis sentencji wyroku z uzasadnieniem doręcza się wyłącznie ministrowi właściwemu do spraw informatyzacji. Skarżącemu doręcza się odpis wyroku z tą częścią uzasadnienia, która nie zawiera informacji niejawnych w rozumieniu przepisów o ochronie informacji niejawnych.

Art. 66e. Minister właściwy do spraw informatyzacji prowadzi i udostępnia przy użyciu systemu teleinformatycznego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 66a ust. 13.”;

61) w art. 67 w ust. 1 po pkt 3 dodaje się pkt 3a w brzmieniu:

„3a) Szefa Agencji Wywiadu – w odniesieniu do działalności CSIRT INT;”;

62) po art. 67 dodaje się rozdział 12a w brzmieniu:

„Rozdział 12a.

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

Art. 67a. 1. Pełnomocnik w przypadku uzyskania informacji wskazującej na możliwość wystąpienia incydentu krytycznego, może wydać ostrzeżenie w celu poinformowania o cyberzagrożeniu:

1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) właścicieli oraz posiadaczy samoistnych i 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;
3) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2021 r. poz. 1907, 1814 i 2140 oraz z 2022 r. poz. 1488);
4) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 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.

2. Do ostrzeżenia nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Pełnomocnik, przed wydaniem ostrzeżenia, przeprowadza we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę obejmującą:

1) istotność cyberzagrożenia;
2) prawdopodobieństwo wystąpienia incydentu krytycznego;
3) rodzaje ryzyk;
4) skuteczność zalecenia określonego zachowania, które zmniejszy ryzyko wystąpienia incydentu krytycznego lub alternatywnych metod zapewnienia cyberbezpieczeństwa.

4. Ostrzeżenie zawiera:

1) określenie rodzaju lub rodzajów podmiotów wskazanych w ust. 1, będących jego adresatami;
2) zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego;
3) uzasadnienie zawierające wyniki analizy, o której mowa w ust. 3;
4) datę wejścia w życie ostrzeżenia.

5. Pełnomocnik odwołuje ostrzeżenie po:

1) uzyskaniu informacji o ustaniu zagrożenia wystąpienia incydentu krytycznego;
2) przeprowadzaniu przeglądu i ustaleniu, że nie jest zasadne jego utrzymanie.

6. Pełnomocnik przeprowadza przegląd ostrzeżenia nie rzadziej niż raz na rok od jego wydania. W ramach przeglądu ostrzeżeń Pełnomocnik może przeprowadzić analizę, o której mowa w ust. 3.

7. Pełnomocnik udostępnia:

1) informację o wydanym ostrzeżeniu, a także o odwołaniu ostrzeżenia,
2) listę wydanych i odwołanych ostrzeżeń

– w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika, a także na stronie internetowej urzędu obsługującego Pełnomocnika.

8. Informacja o wydaniu ostrzeżenia może być przekazana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

9. Zalecenie określonego zachowania zmniejszającego ryzyko wystąpienia incydentu krytycznego może polegać na:

1) przeprowadzeniu szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzeniu środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
2) dokonaniu przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu związanego z daną podatnością;
3) wdrożeniu określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;
4) dokonaniu określonej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;
5) prowadzeniu wzmożonego monitorowania zachowania systemu;
6) odstąpieniu od korzystania z określonego sprzętu lub oprogramowania;
7) wprowadzeniu reguły ruchu sieciowego zakazującego połączeń z określonymi adresami IP lub nazwami URL.

Art. 67b. 1. Minister właściwy do spraw informatyzacji w przypadku wystąpienia incydentu krytycznego może, w drodze decyzji, wydać polecenie zabezpieczające.

2. Polecenie zabezpieczające dotyczy nieokreślonej liczby:
1) podmiotów, o których mowa w art. 4 pkt 1–16;
2) właścicieli oraz posiadaczy samo istnych i 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;
3) krajowych instytucji płatniczych, o których mowa w art. 2 pkt 16 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych;
4) kwalifikowanych i niekwalifikowanych dostawców usług zaufania, o których mowa w art. 3 pkt 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 uchylające dyrektywę 1999/93/WE.

3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy stosuje się odpowiednio.

4. Stronę zawiadamia się o czynnościach w sprawie przez publiczne udostępnienie informacji w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji.

5. Minister właściwy do spraw informatyzacji, przed wydaniem polecenia zabezpieczającego przeprowadza, we współpracy z Zespołem, o którym mowa w art. 35 ust. 3, analizę, obejmującą:

1) istotność cyberzagrożenia;
2) rodzaje ryzyk;
3) przewidywane lub zaistniałe skutki incydentu krytycznego;
4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;
5) przewidywane finansowe, społeczne i prawne skutki wydania polecenia zabezpieczającego.

6. Do analizy, o której mowa w ust. 5, nie stosuje się art. 106 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

7. Dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy.

8. Przedstawiciele podmiotów, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Dyrektora Rządowego Centrum Bezpieczeństwa do udziału w pracach Zespołu lub posiedzeniach Zespołu w związku z przygotowywaniem analizy, o której mowa w ust. 5.

9. Polecenie zabezpieczające zawiera:

1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy;
2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się, oraz
3) termin jego wdrożenia.

10. Przez zachowanie, o którym mowa w ust. 9 pkt 2, rozumie się:

1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego sprzętu lub oprogramowania i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;

2) nakaz przeglądu planów ciągłości działania i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
3) nakaz zastosowania określonej poprawki bezpieczeństwa w sprzęcie lub oprogramowaniu posiadającym daną podatność;
4) nakaz szczególnej konfiguracji sprzętu lub oprogramowania, zabezpieczającej przed wykorzystaniem określonej podatności;
5) nakaz wzmożonego monitorowania zachowania systemu;
6) zakaz korzystania z określonego sprzętu lub oprogramowania, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;
7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu określonego w art. 67b ust. 2, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRTMON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego;
8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;
9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych;
10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

11. Wskazanie obowiązku określonego zachowania, o którym mowa w ust. 9 pkt 2, następuje z uwzględnieniem środków adekwatnych, w szczególności w świetle analizy, o której mowa w ust. 5.

12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, nie dłużej niż na dwa lata.

13. Polecenie zabezpieczające wygasa:
1) z dniem wskazanym w ogłoszeniu o zakończeniu koordynacji obsługi incydentu w dzienniku urzędowym ministra właściwego do spraw informatyzacji, lub
2) po upływie czasu, na który zostało wydane.

14. Polecenie zabezpieczające podlega natychmiastowej wykonalności.

15. Minister właściwy do spraw informatyzacji ogłasza polecenie zabezpieczające w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Informacje o poleceniu zabezpieczającym udostępnia się również w Biuletynie Informacji Publicznej

na stronie podmiotowej ministra lub na stronie internetowej urzędu obsługującego ministra.

16. Polecenie zabezpieczające uznaje się za doręczone z chwilą ogłoszenia polecenia zabezpieczającego w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

17. Od polecenia zabezpieczającego nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

18. Nadzór nad wykonywaniem polecenia zabezpieczającego sprawują organy właściwe do sprawowania nadzoru nad danym podmiotem.

Art. 67c. 1. Skargę na decyzję, o której mowa w art. 67b ust. 1, wnosi się w terminie 2 miesięcy, od dnia, w którym decyzja została ogłoszona w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

2. Sąd administracyjny zarządza połączenie wszystkich oddzielnych spraw toczących się przed nim w celu ich łącznego rozpoznania i rozstrzygnięcia, jeżeli dotyczą tej samej decyzji.

3. Wniosek o przywrócenie terminu na złożenie skargi jest niedopuszczalny.

Art. 67d 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 66b, art. 66c oraz art. 67b.

2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o:

1) decyzjach wydanych na podstawie art. 66a ust. 13;
2) wydanych poleceniach zabezpieczających.

Art. 67e. 1. Prezes Rady Ministrów, działając na podstawie rekomendacji Kolegium, w uzgodnieniu z Ministrem Obrony Narodowej, może czasowo powierzyć temu ministrowi realizację wybranych zadań, o których mowa w art. 26 ustawy.

2. Decyzja, o której mowa w ust. 1, określa w szczególności:

1) zakres powierzonych zadań;
2) czas realizacji powierzonych zadań lub sposób ich odwołania;
3) w razie potrzeby – szczególne zasady współpracy z CSIRT MON, CSIRT NASK i CSIRT GOV;
4) zasady informowania Kolegium o stanie realizacji powierzonych zadań.

3. Realizacja zadań, o których mowa w ust. 1, dokonywana jest przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych.”;

63) w art. 73:

a) w ust. 1:

– w pkt 4 wyraz „osoby” zastępuje się wyrazem „osób”,

– w pkt 13 kropkę zastępuje się średnikiem i dodaje się pkt 14 i 15 w brzmieniu:

„14) z własnej winy nie korzysta z systemu, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11;

15) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 3.”,

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

„1a. Jednostka oceniająca zgodność, która:

1) nie przekazuje informacji, o których mowa w art. 59m i art. 59q ust. 3 lub przekazuje je nieprawdziwe lub niekompletne,

2) nie wykonuje obowiązku określonego w art. 59zb ust. 1

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski” na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”.

1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających, w chwili jego wydania, wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:

1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w,

2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59w,

3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,

4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji,

5) nie wykonuje obowiązku określonego w art. 59s

– podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.”,

c) po ust. 2 dodaje się ust. 2a–2d w brzmieniu:

„2a. Karze pieniężnej podlega podmiot określony w art. 66a ust. 1 pkt 1–4, który nie dostosował się do obowiązków określonych w art. 66b.

2b. Karze pieniężnej podlega podmiot, którego dotyczy polecenie zabezpieczające, który:

1) nie wdrożył w terminie zachowania określonego w poleceniu zabezpieczającym;

2) odstąpił od wykonywania zachowania, określonego w poleceniu zabezpieczającym, przed wygaśnięciem polecenia zabezpieczającego.

2c. Na podmiot publiczny, który nie wyznaczył osób, o których mowa w art. 21, może być nałożona kara pieniężna, jeżeli brak wyznaczenia tych osób uniemożliwia lub utrudnia wymianę informacji pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa a tym podmiotem.

2d. Na podmiot, który nie wypełnia obowiązków informacyjnych, o których mowa w art. 66c, może zostać nałożona kara pieniężna, jeżeli przemawia za tym charakter lub zakres naruszenia.”,

d) w ust. 3:

– pkt 9 otrzymuje brzmienie:

„9) ust. 1 pkt 10 i 15, wynosi do 100 000 zł;”,

– po pkt 11 dodaje się pkt 11a w brzmieniu:

„11a) ust. 1 pkt 14 wynosi do 100 000 zł;”,

– dodaje się pkt 14–17 w brzmieniu:

„14) ust. 2a, wynosi:

a) w przypadku podmiotów określonych w art. 66a ust. 1, z wyjątkiem podmiotów publicznych, do 3% jego całkowitego rocznego światowego obrotu podmiotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów publicznych do 100 000 zł;

15) ust. 2b, wynosi:

a) w przypadku podmiotów określonych w art. 67b ust. 2 z wyjątkiem podmiotów publicznych, do 3% całkowitego rocznego światowego obrotu podmiotu z poprzedniego roku obrotowego,

b) w przypadku podmiotów publicznych do 100 000 zł;

16) ust. 2c, wynosi do 10 000 zł;

17) ust. 2d wynosi do 50 000 zł.”,

e) dodaje się ust. 6 i 7 w brzmieniu:

„6. Niezależnie od kary pieniężnej, o której mowa w ust. 2c, minister właściwy do spraw informatyzacji może nałożyć, w drodze decyzji, na kierującego podmiotem publicznym, o którym mowa w art. 4 pkt 7–15, realizującym zadanie publiczne zależne od systemu informacyjnego, karę pieniężną w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek,

7. Niezależnie od kary pieniężnej, o której mowa w ust. 2d, można nałożyć na kierującego podmiotem, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego tego podmiotu lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.”;

64) w art. 74:

a) ust. 1 otrzymuje brzmienie:

„1. Karę pieniężną, o której mowa w art. 73 ust. 1 i 2, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.”,

b) dodaje się ust. 1a–1e w brzmieniu:

„1a. Karę pieniężną, o której mowa w art. 73 ust. 1a–1c, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

1b. Karę pieniężną, o której mowa w art. 73 ust. 2a nakłada, w drodze decyzji:

1) w przypadku przedsiębiorców komunikacji elektronicznej – Prezes UKE;

2) w przypadku operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej – organ właściwy do spraw cyberbezpieczeństwa;

3) w przypadku podmiotów określonych w art. 66a ust. 1, innych niż przedsiębiorcy komunikacji elektronicznej, operatorzy usług kluczowych, dostawcy usług cyfrowych – minister właściwy do spraw informatyzacji.

1c. Karę pieniężną, o której mowa w art. 73 ust. 2b, nakłada, w drodze decyzji:

1) w przypadku przedsiębiorców komunikacji elektronicznej, którzy nie są krajowymi instytucjami płatniczymi – Prezes UKE;

2) w przypadku operatorów usług kluczowych i dostawców usług cyfrowych, którzy nie są przedsiębiorcami komunikacji elektronicznej – organ właściwy do spraw cyberbezpieczeństwa;

3) w przypadku krajowych instytucji płatniczych – Komisja Nadzoru Finansowego;4) w przypadku podmiotów określonych w art. 67b ust. 1, innych niż przedsiębiorcy komunikacji elektronicznej, operatorzy usług kluczowych, dostawcy usług cyfrowych, krajowe instytucje płatnicze – minister właściwy do spraw informatyzacji.

1d. Karę pieniężną, o której mowa w art. 73 ust. 2c, nakłada w drodze decyzji minister właściwy do spraw informatyzacji.

1e. Karę pieniężną, o której mowa w art. 73 ust. 2d i 7, może nałożyć w drodze decyzji organ uprawniony do żądania informacji zgodnie z właściwością określoną w art. 66c ust. 2.”,

c) ust. 2 otrzymuje brzmienie:

„2. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.”;

65) po art. 74 dodaje się art. 74a w brzmieniu:

„Art. 74a 1. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ust. 2a lub 2b, podmiot, wobec którego wszczęto to postępowanie, jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru administracyjnej kary pieniężnej.

2. W przypadku gdy podmiot, wobec którego wszczęto postępowanie w sprawie nałożenia kary pieniężnej, o której mowa w art. 73 ust. 2a lub 2b:

1) nie dostarczył danych niezbędnych do określenia podstawy wymiaru kary pieniężnej lub
2) dostarczone przez ten podmiot dane uniemożliwiają ustalenie podstawy wymiaru kary pieniężnej

– organ uprawniony do nałożenia kary ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy uwzględniając wielkość podmiotu, specyfikę prowadzonej przez niego działalności lub ogólnie dostępne dane finansowe dotyczące podmiotu.”;

66) po art. 75 dodaje się art. 75a i art. 75b w brzmieniu:

„Art. 75a. 1. Organ właściwy do spraw cyberbezpieczeństwa nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT sektorowego, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44 ust. 1a.

2. Szef Agencji Wywiadu nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT INT, jeżeli nie został wykonany obowiązek, o którym mowa w art. 36c.

3. Minister właściwy do spraw informatyzacji nakłada, w drodze decyzji, karę pieniężną na kierownika CSIRT Telco, jeżeli nie został wykonany obowiązek, o którym mowa w art. 44a ust. 5.

4. Kara pieniężna, o której mowa w ust. 1–3, nakładana jest w wysokości do jednokrotności minimalnego wynagrodzenia za pracę w roku, w którym nie został wykonany obowiązek.

Art. 75b. Wpływy z tytułu kar pieniężnych, o których mowa w art. 75 i art. 75a, stanowią przychód Funduszu Cyberbezpieczeństwa.”;

67) po art. 76 dodaje się art. 76a–art. 76c w brzmieniu:

„Art. 76a. 1. Karze pieniężnej podlega przedsiębiorca komunikacji elektronicznej, który:

1) nie wypełnia obowiązku systematycznego szacowania ryzyka wystąpienia sytuacji szczególnego zagrożenia, o którym mowa w art. 20a ust. 2;
2) nie podejmuje środków, o których mowa w art 20a ust. 2 pkt 2;
3) nie dokumentuje czynności, o których mowa w art. 20a ust. 2 pkt 1 i 2;
4) nie przekazuje informacji, o których mowa w art. 20b ust. 2, w terminie wskazanym w żądaniu Prezesa UKE;
5) nie wykonuje obowiązku, o którym mowa w art. 20b ust. 4, w terminie wskazanym w decyzji Prezesa UKE;
6) nie obsługuje incydentu telekomunikacyjnego, o którym mowa w art. 20c pkt 1;

7) nie zgłasza poważnego incydentu telekomunikacyjnego, o którym mowa w art. 20d ust. 1 pkt 2;
8) nie współdziała podczas obsługi poważnego incydentu telekomunikacyjnego i incydentu krytycznego z CSIRT Telco lub z właściwym CSIRTMON, CSIRT NASK, CSIRT GOV i tym samym nie wykonuje obowiązku, o którym mowa w art. 20d ust. 1 pkt 3 i 4;
9) nie usuwa, w wyznaczonym przez Prezesa UKE terminie, podatności, która doprowadziła lub mogła doprowadzić do incydentu telekomunikacyjnego lub krytycznego, o której mowa w art. 54a;
10) nie wykonuje zaleceń pokontrolnych Prezesa UKE, o których mowa w art. 59.

2. Prezes UKE, jeżeli przemawia za tym charakter lub zakres naruszenia, może nałożyć karę pieniężną na przedsiębiorcę komunikacji elektronicznej, który:

1) nie wyznacza dwóch osób, o których mowa w art. 20a ust. 4;
2) nie zapewnia dostępu do informacji o rejestrowanych przez niego incydentach telekomunikacyjnych właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV oraz CSIRT Telco w zakresie niezbędnym do realizacji ich zadań;
3) nie wykonuje obowiązku, o którym mowa w art. 20f ust. 1 i 2;
4) nie wykonuje obowiązku, o którym mowa w art. 20h ust. 5.

3. Kara, o której mowa w ust. 1 i 2, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

4. Karę, o której mowa w ust. 1:

1) pkt 6 – nakłada się za każdy stwierdzony przypadek zaniechania obsługi incydentu telekomunikacyjnego;
2) pkt 7 – nakłada się za każdy stwierdzony przypadek niezgłoszenia poważnego incydentu telekomunikacyjnego.

5. Niezależnie od kar pieniężnych, o których mowa w ust. 1 i 2, Prezes UKE może nałożyć na osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy..

Art. 76b. 1. Kary pieniężne, o których mowa w art. 76a ust. 1 i 2, nakłada Prezes UKE, w drodze decyzji, w wysokości do 3% przychodu ukaranego podmiotu,

osiągniętego w poprzednim roku kalendarzowym. Decyzji o nałożeniu kary pieniężnej nie nadaje się rygoru natychmiastowej wykonalności.

2. W przypadku, gdy podmiot w roku kalendarzowym poprzedzającym rok nałożenia kary pieniężnej nie osiągnął przychodu lub osiągnął przychód w wysokości nieprzekraczającej 500 000 zł, Prezes UKE, nakładając karę pieniężną, uwzględnia średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających rok nałożenia kary pieniężnej.

3. W przypadku, gdy podmiot nie osiągnął przychodu w okresie, o którym mowa w ust. 2, lub gdy przychód podmiotu w tym okresie nie przekracza 500 000 zł, Prezes UKE może nałożyć na podmiot karę pieniężną w wysokości nieprzekraczającej 15 000 zł.

4. W przypadku, gdy przed wydaniem decyzji o nałożeniu kary pieniężnej podmiot nie dysponuje danymi finansowymi niezbędnymi do ustalenia przychodu za rok kalendarzowy poprzedzający rok nałożenia kary pieniężnej, Prezes UKE, nakładając karę pieniężną, uwzględnia:

1) przychód osiągnięty przez podmiot w roku kalendarzowym poprzedzającym ten rok;
2) w przypadku, o którym mowa w ust. 2 – średni przychód osiągnięty przez podmiot w trzech kolejnych latach kalendarzowych poprzedzających ten rok. Przepis ust. 3 stosuje się odpowiednio.

5. W przypadku, gdy podmiot powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu, o którym mowa w ust. 1, Prezes UKE uwzględnia przychód osiągnięty przez te podmioty w roku kalendarzowym poprzedzającym rok nałożenia kary. Przepisy ust. 2–4 stosuje się odpowiednio.

6. Ustalając wysokość kary pieniężnej, Prezes UKE uwzględnia charakter i zakres naruszenia, dotychczasową działalność podmiotu oraz jego możliwości finansowe.

7. Podmiot jest obowiązany do dostarczenia Prezesowi UKE, na każde jego żądanie, w terminie 1 miesiąca od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej. W przypadku niedostarczenia danych lub gdy dostarczone dane uniemożliwiają ustalenie podstawy wymiaru kary, Prezes UKE może ustalić podstawę wymiaru kary pieniężnej w sposób szacunkowy, nie mniejszą jednak niż kwota 500 000 złotych.

8. Kary, o których mowa w art. 76a ust. 1 i 2, stanowią przychód Funduszu Cyberbezpieczeństwa.

Art. 76c. Organy uprawnione do nałożenia kary przekazują środki pochodzące z kar, o których mowa w art. 73, art. 75, art. 75a i art. 76a, na rachunek Funduszu Cyberbezpieczeństwa w terminie 1 miesiąca od dnia ich pobrania.”;

68) przed art. 77 dodaje się oznaczenie i tytuł działu oraz oznaczenie i tytuł rozdziału w brzmieniu:

„DZIAŁ III. STRATEGICZNA SIEĆ BEZPIECZEŃSTWA

Rozdział 1

Operator strategicznej sieci bezpieczeństwa

Art. 76d. 1. W celu zapewnienia realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, w zakresie telekomunikacji, tworzy się strategiczną sieć bezpieczeństwa, będącą siecią telekomunikacyjną w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

2. Strategiczna sieć bezpieczeństwa jest uruchamiana oraz zarządzana przez Operatora strategicznej sieci bezpieczeństwa.

3. Prezes Rady Ministrów może określić, w drodze rozporządzenia, minimalne wymagania techniczne jakie musi spełniać strategiczna sieć bezpieczeństwa oraz minimalny poziom bezpieczeństwa usług transmisji danych, połączeń głosowych oraz wiadomości tekstowych, mając na względzie konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa komunikacji oraz aktualny poziom wiedzy naukowo–technicznej.

Art. 76e. 1.Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa, spośród podmiotów spełniających łącznie następujące warunki:

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

- pod warunkiem wyrażenia zgody na pełnienie funkcji Operatora strategicznej sieci bezpieczeństwa.

2. Operator strategicznej sieci bezpieczeństwa obowiązany jest do wyodrębnienia w ramach prowadzonej rachunkowości informacji dla zadań, o których mowa w art. 76d ust. 1.

Art. 76f. 1. Operator strategicznej sieci bezpieczeństwa w celu realizacji zadań, o których mowa w art. 76d ust. 1, świadczy usługi telekomunikacyjne oraz może świadczyć usługi związane z zapewnieniem udogodnień towarzyszących oraz usług z zakresu cyberbezpieczeństwa.

2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 111 ust. 2 pkt 2 i 3 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne. Wykorzystanie częstotliwości użytkowanych jako rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3.

3. Wykorzystanie częstotliwości, o których mowa w art. 76t ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 143 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się odpowiednio.

Art. 76g. 1. Operator strategicznej sieci bezpieczeństwa świadczy usługi, na potrzeby realizacji zadań określonych w art. 76d ust.1, na rzecz:

1) Kancelarii Prezydenta RP,
2) Kancelarii Sejmu,
3) Kancelarii Senatu,
4) Kancelarii Prezesa Rady Ministrów,
5) Biura Bezpieczeństwa Narodowego,
6) urzędów obsługujących organy administracji rządowej, organy jednostek samorządu terytorialnego oraz podmiotów podległych tym organom albo przez nie nadzorowanych, wykonującym zadania z zakresu:
   a) ochrony bezpieczeństwa i porządku publicznego,
   b) bezpieczeństwa i obronności państwa,
   c) bezpieczeństwa ekonomicznego,
   d) ochrony granicy państwa,
   e) ochrony ludności i obrony cywilnej,

f) zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej państwa,

g) dostaw energii,

h) ochrony interesów Rzeczypospolitej Polskiej,

i) ochrony zdrowia,

j) weterynaryjnej ochrony zdrowia publicznego,

k) nadzoru sanitarnego,

l) ochrony środowiska,

m) sprawiedliwości,

n) sądownictwa,

o) prokuratury,

p) systemu powiadamiania ratunkowego,

7) Sił Zbrojnych Rzeczypospolitej Polskiej oraz jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej,

8) podmiotów wykonujących na rzecz administracji rządowej zadania z zakresu ochrony ludności i obrony cywilnej, zarządzania kryzysowego, w tym związane z zapewnieniem ciągłości funkcjonowania i odtwarzania infrastruktury krytycznej Państwa

– na wniosek tych podmiotów.

2. Podmioty, o których mowa w ust. 1, korzystają z usług telekomunikacyjnych w ruchomej publicznej sieci telekomunikacyjnej świadczonych przez Operatora strategicznej sieci bezpieczeństwa, przy pomocy strategicznej sieci bezpieczeństwa, w zakresie niezbędnym do zapewnienia w tych podmiotach realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

3. Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego nie mają obowiązku korzystania z sieci, o której mowa w ust. 2.

4. Prezes Rady Ministrów może zobowiązać Operatora strategicznej sieci bezpieczeństwa do świadczenia usług, o których mowa w art. 76f ust. 1:

1) właścicielom i posiadaczom 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 - na wniosek organu, we właściwości którego znajduje się określony system infrastruktury krytycznej, lub

2) przedsiębiorcom realizującym zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny - na wniosek Ministra Obrony Narodowej.

5. Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, Straż Graniczna, Państwowa Straż Pożarna, Służba Ochrony Państwa oraz Policja mogą zlecić Operatorowi strategicznej sieci bezpieczeństwa świadczenie usługi wsparcia technicznego, z uwzględnieniem aktualnego poziomu wiedzy naukowo–technicznej dotyczącego nowoczesnych systemów łączności. Usługi wsparcia technicznego mogą polegać w szczególności na utrzymaniu, rozbudowie i modyfikacji sieci teleinformatycznych w zakresie sieci rozległych oraz zestawienia i utrzymania łączy dostępowych do takich sieci.

6. Świadczenie usług, o których mowa w ust. 1–5 oraz art. 76f ust. 1, przez Operatora strategicznej sieci bezpieczeństwa wymaga zawarcia umowy pomiędzy Operatorem strategicznej sieci bezpieczeństwa a właściwym podmiotem, o którym mowa w ust. 1 i 2.

7. Umowa, o której mowa w ust. 6, określa w szczególności obowiązek zapewnienia przez Operatora strategicznej sieci bezpieczeństwa usług telekomunikacyjnych o określonej jakości, dostępności, pojemności i wydajności, w tym w przypadkach zagrożenia dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, a w przypadku wydania rozporządzenia, o którym mowa w art. 76d ust. 3, także obowiązek zapewnienia określonego w rozporządzeniu poziomu bezpieczeństwa sieci i usług.

8. W przypadku uporczywego niewywiązywania się przez Operatora z obowiązków wynikających z umowy, o której mowa w ust. 6, podmiot na rzecz którego Operator świadczy usługi może rozwiązać taką umowę, informując Prezesa Rady Ministrów o przyczynach rozwiązania umowy.

9. W wypadku, o którym mowa w ust. 8, podmiot może zlecić świadczenie usług objętych umową, o której mowa w ust. 6, operatorowi telekomunikacyjnemu innemu niż Operator strategicznej sieci bezpieczeństwa, dającemu rękojmię zapewnienia bezpieczeństwa świadczonych usług na poziomie nie niższym niż określony w rozwiązanej umowie z Operatorem strategicznej sieci bezpieczeństwa lub w rozporządzeniu wydanym na podstawie art. 76d ust. 3.

Art. 76h. W związku z ochroną istotnych interesów bezpieczeństwa państwa, przy zawieraniu umów, o których mowa w art. 76g ust. 6, dotyczących realizacji zadań, o których mowa w art. 76d ust. 1, nie stosuje się przepisów ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych.

Art. 76i. 1. Prezes UKE może dokonywać analizy cen usług telekomunikacyjnych stosowanych przez Operatora strategicznej sieci bezpieczeństwa, o których mowa w art. 76g ust. 2.

2. Podmioty, o których mowa w art. 76g ust. 1, mogą wnioskować o dokonanie analizy, o której mowa w ust. 1.

3. Prezes UKE dokonuje analizy, o której mowa w ust. 1, w terminie 2 miesięcy, od złożenia wniosku, o którym mowa w ust. 2.

4. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę, których dotyczą, podmiot zobowiązany do zawarcia umowy z Operatora strategicznej sieci bezpieczeństwa może rozpocząć procedurę zawarcia umowy o świadczenie usług telekomunikacyjnych z innym dostawcą usług. Prezes UKE informuje Operatora strategicznej sieci bezpieczeństwa o wynikach analizy, o której mowa w ust. 1

5. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 1, przekraczają koszty oraz rozsądną marżę , których dotyczą, Operator strategicznej sieci bezpieczeństwa w terminie 7 dni, od dnia otrzymania informacji, o której mowa w ust. 4, jest obowiązany przedstawić nową ofertę podmiotowi zobowiązanemu do zawarcia umowy z Operatorem strategicznej sieci bezpieczeństwa. Prezes UKE, na wniosek operatora strategicznej sieci bezpieczeństwa, dokonuje analizy cen usług telekomunikacyjnych przedstawionych w nowej ofercie w terminie 21 dni, od otrzymania wniosku. O wyniku analizy informowany jest podmiot, do którego ta oferta została skierowana.

6. W przypadku stwierdzenia przez Prezesa UKE, że ceny, o których mowa w ust. 5, przekraczają koszty oraz rozsądną marżę, Prezes UKE wydaje decyzję zastępującą albo zmieniającą umowę, uwzględniając przedłożoną ofertę oraz określa cenę świadczonych usług na poziomie odpowiadającym kosztom oraz rozsądnej marży.

Art. 76j. 1. Operator strategicznej sieci bezpieczeństwa przekazuje Prezesowi UKE informacje o zawartej umowie na świadczenie usług za pośrednictwem strategicznej sieci

bezpieczeństwa, w szczególności cenę oraz zakres świadczonych usług, w terminie 14 dni od dnia zawarcia umowy.

2. Operator strategicznej sieci bezpieczeństwa jest obowiązany do przekazywania na żądanie Prezesa UKE informacji niezbędnych do wykonywania przez Prezesa UKE jego uprawnień i obowiązków, w terminie 21 dni od otrzymania żądania.

Art. 76k. 1. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (Dz. U. z 2022 r. poz. 884), zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do infrastruktury technicznej, w tym współkorzystanie z niej, w celu realizacji zadań, o których mowa w art. 76d ust. 1.

2. Dostęp do infrastruktury technicznej jest odpłatny, chyba że strony umowy postanowią inaczej.

3. Opłaty z tytułu dostępu do infrastruktury technicznej określa się w wysokości, która umożliwia zwrot części kosztów, które ponosi operator sieci w związku z utrzymaniem tej infrastruktury oraz z zapewnieniem dostępu.

4. Warunki dostępu, o którym mowa w ust. 1, w tym techniczne, eksploatacyjne i finansowe warunki współpracy, określa umowa zawarta w formie pisemnej lub elektronicznej pomiędzy Operatorem strategicznej sieci bezpieczeństwa a operatorem sieci. Przepisy art. 19 ust. 1–2a, 4 i 5, art. 20, art. 24 i art. 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio.

5. W przypadku odmowy udzielenia dostępu do infrastruktury technicznej przez operatora sieci lub niezawarcia umowy o dostępie do infrastruktury technicznej w terminie 2 miesięcy od dnia złożenia wniosku o taki dostęp, Operator strategicznej sieci bezpieczeństwa może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do infrastruktury technicznej.

6. Do wniosku do Prezesa UKE o wydanie decyzji w sprawie dostępu do infrastruktury technicznej dołącza się:

1) wniosek w sprawie zawarcia umowy o dostępie do infrastruktury technicznej;

2) potwierdzenie doręczenia drugiej stronie lub potwierdzenie nadania przesyłką poleconą wniosku, o którym mowa w pkt 1;

3) dokumenty z negocjacji prowadzonych z drugą stroną, o ile druga strona podjęła negocjacje;

4) projekt umowy o dostępie do infrastruktury technicznej, z zaznaczeniem tych części umowy, co do których strony nie doszły do porozumienia.

7. Strony są obowiązane przedłożyć Prezesowi UKE, na jego żądanie, w terminie 14 dni, swoje stanowiska wobec rozbieżności oraz dokumenty niezbędne do rozpatrzenia wniosku.

8. Prezes UKE wydaje decyzję w sprawie dostępu do infrastruktury technicznej, w celu realizacji przez Operatora strategicznej sieci bezpieczeństwa zadań, o których mowa w art. 76d ust. 1, w terminie 2 miesięcy od dnia złożenia wniosku o jej wydanie przez Operatora strategicznej sieci bezpieczeństwa, biorąc pod uwagę w szczególności konieczność zapewnienia niedyskryminacyjnych i proporcjonalnych warunków dostępu.

9. Operator sieci, o którym mowa w art. 2 ust. 1 pkt 8 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, w terminie 14 dni od dnia otrzymania zawiadomienia o wszczęciu postępowania o wydanie decyzji w sprawie dostępu do infrastruktury technicznej, przedstawia Prezesowi UKE uzasadnienie wysokości opłat z tytułu dostępu do infrastruktury technicznej, w którym uwzględnia kryteria, o których mowa w ust. 3.

10. Decyzja w sprawie dostępu do infrastruktury technicznej w zakresie nią objętym zastępuje umowę o tym dostępie.

11. W przypadku zawarcia przez zainteresowane strony umowy o dostępie do infrastruktury technicznej, decyzja o dostępie do infrastruktury technicznej wygasa z mocy prawa w części objętej umową.

12. Decyzja w sprawie dostępu do infrastruktury technicznej może zostać zmieniona przez Prezesa UKE na wniosek każdej ze stron, której ona dotyczy, lub z urzędu, w przypadkach uzasadnionych potrzebą zapewnienia ochrony interesów odbiorców usług świadczonych przez podmioty wykonujące zadania z zakresu użyteczności publicznej lub użytkowników końcowych lub zapewnienia ochrony skutecznej konkurencji.

13. W postępowaniu w sprawie zmiany decyzji w sprawie dostępu do infrastruktury technicznej przepisy ust. 3 oraz ust. 8–10 stosuje się odpowiednio.

Art. 76l. 1. Na potrzeby realizacji zadań, o których mowa w art. 76d ust. 1:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu Państwa,

2) jednostka samorządu terytorialnego, oraz

3) właściciel lub zarządca nieruchomości

– zapewnia Operatorowi strategicznej sieci bezpieczeństwa dostęp do nieruchomości, w tym do budynku, polegający na umożliwieniu umieszczenia na niej infrastruktury telekomunikacyjnej, a także eksploatacji i konserwacji tej infrastruktury telekomunikacyjnej, jeżeli nie uniemożliwia to racjonalnego korzystania z nieruchomości, w szczególności nie prowadzi do istotnego zmniejszenia jej wartości.

2. Warunki dostępu, o którym mowa w ust. 1, określa odpowiednio umowa zawarta pomiędzy Operatorem strategicznej sieci bezpieczeństwa a podmiotami, o których mowa w ust. 1. Przepisy art. 19 ust. 1-2a, 4 i 5, art. 20 i art. 24a ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych stosuje się odpowiednio.

3. Umowa, o której mowa w ust. 2, jest zawierana w formie pisemnej lub elektronicznej.

4. Dostęp, o którym mowa w ust. 1, jeżeli podmiotem zapewniającym dostęp jest:

1) użytkownik wieczysty lub zarządca nieruchomości stanowiącej własność Skarbu jest nieodpłatny;

2) jednostka samorządu terytorialnego, właściciel lub zarządca nieruchomości, jest nieodpłatny, przy czym Operator strategicznej sieci bezpieczeństwa ponosi:

a) proporcjonalną część kosztów administracyjnych, poniesionych przy zarządzaniu, sprawowaniu nadzoru lub zarządzaniu tą nieruchomością,

b) proporcjonalną część kosztów, które wystąpiły po stronie udostępniającego, jeżeli są konieczne i zaistniały bezpośrednio na skutek zapewnienia takiego dostępu,

c) koszty przywrócenia nieruchomości do stanu poprzedniego.

5. W przypadku odmowy udzielenia dostępu do nieruchomości przez podmioty, o których mowa w ust. 1, lub niezawarcia umowy o dostępie do nieruchomości w terminie miesiąca od dnia złożenia wniosku o taki dostęp każda ze stron może zwrócić się do Prezesa UKE z wnioskiem o wydanie decyzji w sprawie dostępu do nieruchomości.

6. Przepisy art. 76k ust. 6–8 oraz ust. 10–13 stosuje się odpowiednio.

Art. 76m. Od decyzji Prezesa UKE dotyczącej dostępu telekomunikacyjnego, o którym mowa w art. 76k ust. 5 oraz art. 76l ust. 5, przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

Art. 76n. 1. Operatorowi strategicznej sieci bezpieczeństwa przysługuje prawo pierwokupu sieci telekomunikacyjnych będących własnością:

1) Skarbu Państwa lub innych państwowych osób prawnych, w szczególności podmiotów, o którym mowa w art. 4 pkt 1, 2, 4, 5, 7 i 8 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;
2) jednostek samorządu terytorialnego.

2. Podmioty, o których mowa w ust. 1 pkt 1i 2, informują Operatora strategicznej sieci bezpieczeństwa o zamiarze zbycia sieci telekomunikacyjnych, określając termin na skorzystanie z prawa pierwokupu nie krótszy niż 2 tygodnie.

3. W przypadku braku odpowiedzi od Operatora strategicznej sieci bezpieczeństwa w wyznaczonym terminie, przyjmuje się, że Operator strategicznej sieci bezpieczeństwa zrezygnował ze skorzystania z prawa pierwokupu.

Art. 76o. 1. W sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 40 lit. a, w przypadku pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703-713 MHz i 758-768 MHz, Operator strategicznej sieci bezpieczeństwa może zażądać od podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz udostępnienia zasobów częstotliwości z tego zakresu.

2. Podmiot dysponujący rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz jest obowiązany udostępnić Operatorowi strategicznej sieci bezpieczeństwa zasoby częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz niezwłocznie, nie później niż w ciągu jednej godziny, z wyjątkiem częstotliwości, które zostały udostępnione Siłom Zbrojnym Rzeczypospolitej Polskiej.

3. Operator strategicznej sieci bezpieczeństwa, występując z żądaniem, o którym mowa w ust. 1, informuje podmiot dysponujący rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz o czasie i zasięgu terytorialnym tego udostępnienia.

4. Żądanie, o którym mowa w ust. 1, jest przekazywane za pośrednictwem kanału komunikacji, o którym mowa w art. 76o.

5. Okres udostępnienia zasobów częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz na rzecz Operatora strategicznej sieci bezpieczeństwa jest ograniczony do okresu występowania sytuacji szczególnego zagrożenia, o której mowa w ust. 1, oraz sytuacji pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703-713 MHz i 758-768 MHz przez Operatora strategicznej sieci bezpieczeństwa, przy czym nie może być dłuższy niż 72 godziny. W przypadku ustania okoliczności, o których mowa w ust. 1, Operator strategicznej sieci bezpieczeństwa niezwłocznie zwalnia udostępnione zasoby częstotliwości.

6. Operator strategicznej sieci bezpieczeństwa może ponawiać żądanie udostępnienia częstotliwości na kolejne 72 godziny, z zastrzeżeniem ust. 5 zdanie drugie.

7. Zasięg terytorialny udostępnienia zasobów częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz nie może przekraczać obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1.

8. Operator strategicznej sieci bezpieczeństwa przekazuje w postaci elektronicznej na elektroniczną skrzynkę podawczą Prezesa UKE uzasadnienie żądania, o którym mowa w ust. 1, w terminie 1 dnia od dnia wystąpienia z tym żądaniem do podmiotu dysponującego rezerwacją częstotliwości z zakresu 713-733 MHz oraz 768-788 MHz.

9. Przepis ust. 8 stosuje się odpowiednio w przypadku ponowienia żądania, o którym mowa w ust. 6.

10. Uzasadnienie, o którym mowa w ust. 8, zawiera:

1) opis sytuacji szczególnego zagrożenia, o której mowa w ust. 1;

2) wskazanie przyczyn pełnego wykorzystania możliwości świadczenia usług w zakresie częstotliwości 703–713 MHz i 758–768 MHz;

3) wskazanie obszaru, na którym wystąpiła sytuacja szczególnego zagrożenia, o której mowa w ust. 1.

11. Prezes UKE może w ciągu 1 dnia od dnia otrzymania uzasadnienia, o którym mowa w ust. 8, zażądać od Operatora strategicznej sieci bezpieczeństwa dodatkowych wyjaśnień względem tego uzasadnienia. Do czasu uzyskania wyjaśnień, uzasadnienie uważa się za niezłożone.

12. W przypadku niezłożenia uzasadnienia, w terminie, o którym mowa w ust. 8, lub nieprzedstawienia wyjaśnień, o których mowa w ust. 11, Operator strategicznej sieci bezpieczeństwa nie może, do czasu wykonania powyższych obowiązków, ponownie żądać od tego samego podmiotu dysponującego rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788 MHz udostępnienia zasobów częstotliwości z tego zakresu.

13. Prezes UKE udostępnia na wniosek podmiotu dysponującego rezerwacją częstotliwości z zakresu 713–733 MHz oraz 768–788, od którego Operator strategicznej sieci bezpieczeństwa zażądał udostępnienia tych częstotliwości, uzasadnienie, o którym mowa w ust. 8, lub uzasadnienie wydłużenia czasu udostępnienia zasobów częstotliwości.

14. W sytuacji szczególnego zagrożenia, o której mowa w art. 2 pkt 40 lit. a, Operator strategicznej sieci bezpieczeństwa jest obowiązany udostępnić Siłom Zbrojnym Rzeczypospolitej Polskiej udostępnione mu przez podmiot dysponujący rezerwacją

częstotliwości z zakresu 713–733 MHz oraz 768– 788 MHz zasoby częstotliwości z tego zakresu niezwłocznie, nie później niż w ciągu jednej godziny, na czas na jaki zostały mu udostępnione. Przepisy ust. 3, 5, 7-8 i 10 stosuje się odpowiednio.

Art. 76p. Podmiot posiadający rezerwację częstotliwości z zakresu 713 – 733 MHz oraz 768-788 MHz określa kanał komunikacji elektronicznej, umożliwiający niezwłoczną wymianę komunikatów z Operatorem strategicznej sieci bezpieczeństwa i przekazuje informację o tym kanale do Operatora strategicznej sieci bezpieczeństwa w terminie 14 dni od otrzymania decyzji w sprawie rezerwacji częstotliwości z zakresu 713– 733 MHz oraz 768– 788 MHz.

Art. 76q. W zakresie nieuregulowanym w ustawie do Operatora strategicznej sieci bezpieczeństwa stosuje się przepisy ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

Art. 76r. 1. W przypadku, w którym podmiot wyznaczony na Operatora strategicznej sieci bezpieczeństwa przestaje spełniać którąkolwiek z przesłanek, o których mowa w art. 76e ust. 1, Prezes Rady Ministrów może:

1) odwołać Operatora strategicznej sieci bezpieczeństwa, wskazując termin tego odwołania, oraz

2) wyznaczyć nowego Operatora strategicznej sieci bezpieczeństwa za jego zgodą, wskazując termin objęcia tej funkcji.

2. Prezes Rady Ministrów, po zasięgnięciu opinii dotychczasowego Operatora strategicznej sieci bezpieczeństwa wyznacza termin odwołania dotychczasowego operatora oraz wyznaczenia nowego.

3. Prezes Rady Ministrów, w drodze zarządzenia, określa sposób przekazania majątku trwałego nabytego z wykorzystaniem środków publicznych, w celu wykonywania zadań, o których mowa w art. 76d ust. 1, na rzecz nowego Operatora strategicznej sieci bezpieczeństwa.

Art. 76s. W przypadku, o którym mowa w art. 76r ust. 1:

1) podmiot wyznaczony na nowego Operatora strategicznej sieci bezpieczeństwa jest następcą prawnym i wstępuje w ogół praw i obowiązków dotychczasowego Operatora strategicznej sieci bezpieczeństwa w zakresie realizacji zadań, o których mowa w art. 76d ust. 1;

2) umowy, o których mowa w art. 76g ust. 6, wygasają z mocy prawa w terminie 3 miesięcy od wyznaczenia nowego Operatora strategicznej sieci bezpieczeństwa.

Rozdział 2

Przyznanie częstotliwości z zakresu 70 –713 MHz oraz 758–768 MHz

Art. 76t. 1. Prezes UKE, w drodze decyzji, przydziela Operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe w zakresie 703–713 MHz oraz 758–768 MHz.

2. Do decyzji, o której mowa w ust. 1, przepisy art. 114 oraz art. 115 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne stosuje się odpowiednio.

3. W decyzji, o której mowa w ust. 1, Prezes UKE określa wymogi pokrycia zasięgiem ruchomych sieci telekomunikacyjnych opartych o częstotliwości, o których mowa w ust. 1.

Art. 76u. 1. W przypadku zmiany operatora, nowy Operator strategicznej sieci bezpieczeństwa, obejmuje prawa i obowiązki wynikające z przydziału częstotliwości, o którym mowa w art. 76t ust. 1.

2. Prezes UKE potwierdza, w terminie 14 dni od wyznaczenia nowego Operatora strategicznej sieci bezpieczeństwa, o którym mowa w ust. 1, w drodze zaświadczenia, przejęcie przez nowego Operatora strategicznej sieci bezpieczeństwa, praw i obowiązków wynikających z przydziału częstotliwości, o którym mowa w art. 76t ust. 1.

3. Zaświadczenie, o którym mowa w ust. 2, wydaje się na wniosek nowego Operatora strategicznej sieci bezpieczeństwa.

Rozdział 3

Finansowanie strategicznej sieci bezpieczeństwa

Art. 76w. 1. Operator strategicznej sieci bezpieczeństwa otrzymuje dotację celową z części budżetu państwa, której dysponentem jest minister właściwy do spraw aktywów państwowych, na realizację zadań związanych z utrzymaniem, rozwojem i modernizacją infrastruktury strategicznej sieci bezpieczeństwa.

2. Podstawę obliczenia należnej operatorowi strategicznej sieci bezpieczeństwa dotacji, o której mowa w ust. 1, stanowi ustalony przez ministra właściwego do spraw aktywów państwowych koszt realizacji poszczególnych zadań.

3. Szczegółowe warunki wypłaty środków, o których mowa w ust. 1, kwoty należne z tytułu realizacji zadań, o których mowa w ust. 1, oraz sposób i zasady rozliczeń określa umowa zawarta między ministrem właściwym do spraw aktywów państwowych a operatorem strategicznej sieci bezpieczeństwa.

4. Umowa określa również zasady zwrotu niewykorzystanych środków publicznych przeznaczonych na wykonywanie zadań, o których mowa w art. 76d ust. 1, w przypadku, o którym mowa w art. 76r ust. 1 pkt 1.

5. Minister właściwy do spraw aktywów państwowych określi łączną kwotę dotacji, o której mowa w ust. 1, na podstawie danych dotyczących kosztu realizacji zadań, o których mowa w ust. 1, oraz liczby zrealizowanych zadań, przedstawionych przez operatora strategicznej sieci bezpieczeństwa.

6. Ze środków dotacji nie może być dofinansowana działalność gospodarcza operatora strategicznej sieci bezpieczeństwa.”;

69) po art. 76w dodaje się oznaczenie i tytuł działu oraz w brzmieniu:

„DZIAŁ IV

Przepisy końcowe.”;

70) w oznaczeniu rozdziału „15” zastępuje się „1”;

71) w art. 93 uchyla się ust. 8 i 23;

72) w załączniku nr 1 do ustawy:

a) w wierszu „Ochrona zdrowia” w kolumnie trzeciej „Rodzaj podmiotów:

– skreśla się wiersz czwarty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2021 r. poz. 1977 i 2120 oraz z 2022 r. poz. 830, 974, 1095, 1344 i 1733).”,

– skreśla się wiersz piąty „Podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.”,

– po wierszu dwunastym dodaje się wiersz trzynasty w brzmieniu: „Jednostka będąca administratorem Systemu Wspomagania Dowodzenia Państwowego Ratownictwa Medycznego, o którym mowa w art. 24a ust. 1 z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. 2022 r. poz. 1720 i 17)”

b) w wierszu „Infrastruktura cyfrowa” w kolumnie trzeciej „Rodzaj podmiotów” po wierszu „Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).” dodaje się wiersz w brzmieniu „Operator strategicznej sieci bezpieczeństwa”;

72) po załączniku nr 2 do ustawy dodaje się załącznik nr 3 w brzmieniu określonym w załączniku do niniejszej ustawy.

Art. 2. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648 i 1933) uchyla się dział VIIA.

Art. 3. W ustawie z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2021 r. poz. 1933 oraz z 2022 r. poz. 807, 872, 1459 i 1512) w art. 13 w ust. 1 w pkt 30 kropkę zastępuje się średnikiem i dodaje się pkt 31 w brzmieniu:

„31) podmiot wyznaczony na operatora strategicznej sieci bezpieczeństwa, o którym mowa w przepisach ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i …).”.

Art. 4 W ustawie z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2022 r. poz. 1710, 1812 i 1933), w art. 226 ust. 1 w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:

„19) obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 66a ust. 13 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1836 i poz. …) oraz usługę ICT lub proces ICT, określone w tej decyzji.”.

Art. 5. 1. Operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą systemu teleinformatycznego od 1 stycznia 2023 r.

2. Operator usługi kluczowej, któremu została doręczona decyzja o uznaniu za operatora usługi kluczowej po dniu 1 lipca 2022 r., w terminie 6 miesięcy rozpoczyna korzystanie z systemu, o którym mowa w art. 46 ustawy zmienianej w art. 1.

Art. 6. Do postępowań o udzielenie zamówienia publicznego, wszczętych przed dniem wejścia w życie niniejszej ustawy, stosuje się przepisy ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 7. 1. Do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy operatorzy usług kluczowych zgłaszają incydenty poważne do właściwego CSIRTMON, CSIRT NASK lub CSIRT GOV.

2. Agencja Wywiadu oraz jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy

teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym do czasu otrzymania informacji o osiągnięciu zdolności operacyjnej przez CSIRT INT, zgłaszają incydenty w podmiocie publicznym do CSIRT GOV.

Art. 8. 1. Narzędzie do uwierzytelnienia dwuskładnikowego zakupione w ramach realizacji przez NASK–PIB zadania, o którym mowa w art. 37 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych, z chwilą przekazania staje się własnością osoby, która je otrzymała.

2. Określone w ust. 1 nabycie narzędzia do uwierzytelnienia dwuskładnikowego nie rodzi zobowiązań podatkowych, z wyjątkiem ewentualnych zobowiązań z zakresu podatku od towarów i usług.

Art. 9. 1. Z dniem wejścia w życie ustawy:

1) wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo powołane w ramach operatora usługi kluczowej przed wejściem w życie niniejszej ustawy stają się SOC wewnętrznymi;
2) podmioty świadczące usługi z zakresu cyberbezpieczeństwa, z którym dotychczas operator usługi kluczowej zawarł umowę stają się SOC zewnętrznymi;
3) sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy w brzmieniu dotychczasowym staje się CSIRT sektorowym.

2. Podmioty publiczne oraz podmiot, o którym mowa w art. 7 ust. 1 pkt 7 ustawy – Prawo o szkolnictwie wyższym, wyznaczają osoby, o których mowa w art. 21 ustawy zmienianej w art. 1 w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy.

3. Organ właściwy ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

4. Organ właściwy do spraw cyberbezpieczeństwa publikuje komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

5. Minister właściwy do spraw informatyzacji powołuje CSIRT Telco w terminie 18 miesięcy od dnia wejścia w życie ustawy.

6. Minister właściwy do spraw informatyzacji publikuje komunikat o osiągnięciu przez CSIRT Telco zdolności operacyjnej w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

7. Szef Agencji Wywiadu informuje jednostki organizacyjne podległe ministrowi właściwemu do spraw zagranicznych lub przez niego nadzorowane, w tym jednostki, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, o osiągnięciu przez CSIRT INT zdolności operacyjnej.

8. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również publikowana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika,
2) zespołów CSIRTMON, CSIRT NASK, CSIRT GOV

– a także jest przekazywana za pomocą systemu informacyjnego, o którym mowa w art. 46 ustawy o krajowym systemie cyberbezpieczeństwa.

9. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT Telco jest również publikowana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika,
2) zespołów CSIRT MON, CSIRT NASK, CSIRT GOV,
3) Prezesa UKE, w tym na stronie podmiotowej Prezesa UKE w Biuletynie Informacji Publicznej

– a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

10. Przedsiębiorca komunikacji elektronicznej:

1) do dnia publikacji komunikatu, o którym mowa w ust. 6, zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, do CSIRTMON, CSIRT NASK albo CSIRT GOV zgodnie z właściwością określoną w art. 26 tej ustawy;
2) zgłasza incydenty telekomunikacyjne, o których mowa w art. 20d ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, do CSIRT Telco od dnia publikacji komunikatu, o którym mowa w ust. 7.

11. Do dnia publikacji komunikatu, o którym mowa w ust. 6, w uzgodnieniach, o których mowa w art. 34 ust. 1a oraz 34a ust. 3, nie bierze udziału CSIRT Telco.

12. Operator usługi kluczowej realizuje obowiązki, o których mowa w art. 11 ust. 3 pkt 1–3 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

13. Operator usługi kluczowej wykonuje po raz pierwszy obowiązek, o którym mowa w art. 9 ust. 2 ustawy zmienianej w art. 1, w terminie 14 dni od dnia wejścia w życie niniejszej ustawy.

14. CSIRTMON, CSIRT NASK lub CSIRT GOV dostosowują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1, do przepisów ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

15. Porozumienia w sprawie korzystania z systemu, o którym mowa w art. 46 ustawy zmienianej w art. 1, zawarte przed datą wejścia w życie niniejszej ustawy, zachowują ważność.

Art. 10. Prezes Rady Ministrów wyznacza Operatora strategicznej sieci bezpieczeństwa w terminie do 1 miesiąca od wejścia w życie ustawy.

Art. 11. Z dniem … w art. 76t ust. 1i 2 ustawy zmienianej w art. 1 otrzymują brzmienie:

„1. Prezes UKE, przydziela w drodze przydziału, o którym mowa w art. 72 ust. 1 ustawy z dnia … – Prawo komunikacji elektronicznej, Operatorowi strategicznej sieci bezpieczeństwa częstotliwości rządowe z zakresu 703–713 MHz oraz 758–768 MHz. Przepisy art. 73–79 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.

2. Do decyzji, o której mowa w ust. 1, przepisy art. 68, art 69 ust. 1, art. 80, art. 82, art. 84, art. 85 oraz art. 89 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.

Art. 12. Z dniem … w art. 76f ust. 2 i 3 otrzymują brzmienie:

„2. Operator strategicznej sieci bezpieczeństwa może świadczyć usługi telekomunikacyjne także w oparciu o zasoby częstotliwości użytkowane jako rządowe w użytkowaniu rządowym lub cywilno-rządowym w rozumieniu art. 62 ust. 2 pkt 2 i 3 ustawy z dnia … – Prawo komunikacji elektronicznej. Wykorzystanie częstotliwości użytkowanych jako rządowe przez Operatora strategicznej sieci bezpieczeństwa koordynuje Minister Obrony Narodowej, z wyjątkiem ust. 3.

3. Wykorzystanie częstotliwości, o których mowa w art. 76t ust. 1, przez Operatora strategicznej sieci bezpieczeństwa koordynuje Prezes UKE. Przepisy art. 138 ustawy z dnia … – Prawo komunikacji elektronicznej stosuje się odpowiednio.”.

Art. 13. W roku 2023 w budżecie państwa tworzy się rezerwę celową na utworzenie i funkcjonowanie CSIRT sektorowych i CSIRT Telco, o których mowa w art. 44 i art. 44a ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 14. 1.Maksymalny limit wydatków z budżetu państwa dla części budżetowej 21 – Gospodarka morska, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 r. - 0 zł;
2) w 2023 r. – 0 zł;
3) w 2024 r. - 5,417 mln zł;
4) w 2025 r. – 5,656 mln zł;
5) w 2026 r. – 5,692 mln zł;
6) w 2027 r. – 5,719 mln zł;
7) w 2028 r. – 5,747 mln zł;
8) w 2029 r. – 5,775 mln zł;
9) w 2030 r. – 5,804 mln zł;
10) w 2031 r. – 5,834 mln 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 2022 r. – 0 zł;
2) w 2023 r. – 0 zł;
3) w 2024 r. – 5,048 mln zł;
4) w 2025 r. – 5,287 mln zł;
5) w 2026 r. – 5,323 mln zł;
6) w 2027 r. – 5,35 mln zł;
7) w 2028 r. – 5,378 mln zł;
8) w 2029 r. – 5,406 mln zł;
9) w 2030 r. – 5,435 mln zł;
10) w 2031 r. – 5,465 mln zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 r. – 0 mln zł;
2) w 2023 r. – 0,912 mln zł;
3) w 2024 r. – 75,555 mln zł;
4) w 2025 r. – 74,259 mln zł;
5) w 2026 r. – 70,94 mln zł;
6) w 2027 r. – 70,292 mln zł;
7) w 2028 r. – 74,476 mln zł;
8) w 2029 r. – 78,496 mln zł;
9) w 2030 r. – 88,684 mln zł;
10) w 2031 r. – 88,973 mln zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 - Transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 r. - 0 zł;
2) w 2023 r. – 0 zł;
3) w 2024 r. - 5,417 mln zł;
4) w 2025 r. – 5,656 mln zł;
5) w 2026 r. – 5,692 mln zł;
6) w 2027 r. – 5,719 mln zł;
7) w 2028 r. – 5,747 mln zł;
8) w 2029 r. – 5,775 mln zł;
9) w 2030 r. – 5,804 mln zł;
10) w 2031 r. – 5,834 mln zł.

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 - Zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 r. – 0 zł;
2) w 2023 r. – 0 zł;
3) w 2024 r. – 5,773 mln zł;
4) w 2025 r. – 6,012 mln zł;
5) w 2026 r. – 6,048 mln zł;
6) w 2027 r. – 6,075 mln zł;
7) w 2028 r. – 6,103 mln zł;
8) w 2029 r. – 6,131 mln zł;
9) w 2030 r. – 6,160 mln zł;

10) w 2031 r. – 6,19 mln zł.

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 - Energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 r. – 0 zł;
2) w 2023 r. – 0 zł;
3) w 2024 r. – 5,773 mln zł;
4) w 2025 r. – 6,012 mln zł;
5) w 2026 r. – 6,048 mln zł;
6) w 2027 r. – 6,075 mln zł;
7) w 2028 r. – 6,103 mln zł;
8) w 2029 r. – 6,131 mln zł;
9) w 2030 r. – 6,160 mln zł;
10) w 2031 r. – 6,19 mln zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 55 – aktywa państwowe, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 – 0 zł;
2) w 2023 – 189,000 mln zł;
3) w 2024 – 748,000 mln zł;
4) w 2025 – 1 459,000 mln zł;
5) w 2026 – 544,000 mln zł;
6) w 2027 – 552,000 mln zł;
7) w 2028 – 569,000 mln zł;
8) w 2029 – 622,000 mln zł;
9) w 2030 – 650,000 mln zł;
10) w 2031 – 662,000 mln zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 59 – Agencja Wywiadu, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2022 – 0 zł;
2) w 2023 r. – 6,885 mln zł;
3) w 2024 r. – 5,773 mln zł;
4) w 2025 r. – 6,012 mln zł;
5) w 2026 r. – 6,048 mln zł;
6) w 2027 r. – 6,075 mln zł;

7) w 2028 r. – 6,103 mln zł;
8) w 2029 r. – 6,131 mln zł;
9) w 2030 r. – 6,160 mln zł;
10) w 2031 r. – 6,19 mln 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 2022 – 0 zł;
2) w 2023 r. – 0 mln zł;
3) w 2024 r. – 5,773 mln zł;
4) w 2025 r. – 6,012 mln zł;
5) w 2026 r. – 6,048 mln zł;
6) w 2027 r. – 6,075 mln zł;
7) w 2028 r. – 6,103 mln zł;
8) w 2029 r. – 6,131 mln zł;
9) w 2030 r. – 6,160 mln zł;
10) w 2031 r. – 6,19 mln zł.

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

1) ograniczeniu finansowania działalności CSIRT sektorowego;
2) ograniczeniu finansowania działalności CSIRT INT;
3) ograniczeniu finansowania działalności CSIRT Telco.

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

12. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw gospodarki wodnej.

13. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw informatyzacji.

14. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw transportu.

15. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw zdrowia.

16. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw energii.

17. Minister właściwy do spraw aktywów państwowych monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw aktywów państwowych.

18. Szef Agencji Wywiadu 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. 10 pkt 2, dokonuje Szef Agencji Wywiadu w uzgodnieniu ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych.

19. 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 mechanizmów korygujących, o których mowa w ust. 10 pkt 1, dokonuje minister właściwy do spraw aktywów państwowych.

Art. 15. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 10 ust. 5 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

2. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1.

3. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 175a ust. 2a ustawy zmienianej w art. 2, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 20d ust. 3ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

4. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 175d ustawy zmienianej w art. 2, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 20a ust. 6 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 16. Postanowienia umów, o których mowa w art. 33 ust. 1c ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, obowiązujących w dniu wejścia w życie ustawy, sprzeczne z art. 33 ust. 1–1d ustawy zmienianej w art. 1 niniejszej ustawy w brzmieniu nadanym tą ustawą, są nieważne.

Art. 17. 1. Do czasu osiągnięcia przez Operatora strategicznej sieci bezpieczeństwa pełnej zdolności operacyjnej do świadczenia usług, o których mowa w art. 76g ust. 2 ustawy zmienianej w art. 1 niniejszej ustawy, podmioty, o których mowa w tym przepisie, mogą zawierać umowy na świadczenie usług, o których mowa, także z innymi operatorami telekomunikacyjnymi.

2. Prezes Rady Ministrów podaje do publicznej wiadomości informacje o osiągnięciu pełnej zdolności operacyjnej do świadczenia usług przez Operatora strategicznej sieci bezpieczeństwa.

Art. 18. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Załącznik do ustawy z dnia …
Załącznik nr 3

KATEGORIE FUNKCJI KRYTYCZNYCH
DLA BEZPIECZEŃSTWA SIECI I USŁUG

LP.	**OPIS FUNKCJI**	**IDENTYFIKACJA POWIĄZANEJ FUNKCJI SIECIOWEJ WG STANDARDÓW 3GPP**
1.	Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.	AMF – Access & Mobility management Function AUSF – Authentication Server Function
2.	Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.	UDM – Unified Data Management
3.	Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych.	5G Radio Base Station Baseband Unit oraz inne funkcje
4.	Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.	UPF – User Plane Function
5.	Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.	SMF – Session Management Function
6.	Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.	PCF – Policy Control Function
7.	Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.	NSSF – Network Slice Selection Function
8.	Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.	NRF – Network Repository Function
9.	Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.	NEF – Network Exposure Function
10.	Zabezpieczenia połączeń z innymi sieciami.	SEPP – Security Edge

		Protection Proxy

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
LEGISLACYJNYM I REDAKCYJNYM
Anna Markowska
Zastępca Dyrektora Departamentu Regulacji Cyfrowych
Kancelarii Prezesa Rady Ministrów