Dz. U. 2018 poz. 1560

Opracowano na podstawie: t.j. Dz. U. z 2026 r. poz. 20, 252.

U S T A W A

z dnia 5 lipca 2018 r.

o krajowym systemie cyberbezpieczeństwa[1)2)]

Rozdział 1

Przepisy ogólne

Art. 1. 1. Ustawa określa:

1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej;
4) zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwanego dalej „Krajowym planem".

2. Ustawy nie stosuje się do:

1) (uchylony)
2) (uchylony)
3) podmiotów wykonujących działalność leczniczą, tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego lub Szefa Agencji Wywiadu.

---

1) Niniejsza ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80).

2) Niniejsza ustawa służy częściowemu stosowaniu rozporządzenia delegowanego Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024).

Art. 2. Użyte w ustawie określenia oznaczają:

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

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

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

3a) 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;

3b) abonent nazwy domeny – podmiot będący stroną umowy o utrzymywanie nazwy domeny zawartej z rejestrem nazw domen najwyższego poziomu (TLD), za pośrednictwem podmiotu świadczącego usługi rejestracji nazw domen;

3c) adres do doręczeń elektronicznych – adres, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3);

3d) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych, przy danym poziomie pewności, na zdarzenia naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;

4) cyberbezpieczeństwo – cyberbezpieczeństwo w rozumieniu art. 2 pkt 1 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, z późn. zm.[3)]), zwanego dalej „rozporządzeniem 2019/881”;

4a) cyberzagrożenie – cyberzagrożenie w rozumieniu art. 2 pkt 8 rozporządzenia 2019/881;

4b) dostawca sieci dostarczania treści – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza treści i usługi cyfrowe do sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności tych treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników Internetu w imieniu dostawców treści i usług, z wyłączeniem przedsiębiorców komunikacji elektronicznej;

4c) dostawca sprzętu lub oprogramowania – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, w rozumieniu odpowiednio art. 2 pkt 3–6 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.[4)]), produktu ICT, usługi ICT lub procesu ICT;

4d) dostawca internetowej platformy handlowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która dostarcza internetową platformę handlową, o której mowa w art. 2 pkt 8 ustawy z dnia 30 maja 2014 r. o prawach konsumenta (Dz. U. z 2024 r. poz. 1796 oraz z 2025 r. poz. 1172);

4e) dostawca chmury obliczeniowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników;

4f) dostawca platformy sieci usług społecznościowych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą

---

3) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2025/37 z 15.01.2025.

4) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 169 z 25.06.2019, str. 1.

elektroniczną (Dz. U. z 2024 r. poz. 1513), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń;

4g) dostawca usług DNS – podmiot, który świadczy dostępne publicznie rekurencyjne usługi rozpoznawania nazw domen na rzecz ogółu użytkowników końcowych Internetu lub autorytatywne usługi rozpoznawania nazw domen do użytku ogółu użytkowników końcowych Internetu, z wyjątkiem głównych serwerów nazw;

4h) dostawca usługi centrum przetwarzania danych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę obejmującą struktury lub grupy struktur przeznaczone do scentralizowanego hostingu, zapewniania wzajemnego połączenia i eksploatacji produktów ICT, usług ICT lub procesów ICT służącego do świadczenia usług przechowywania, przetwarzania i transportu danych wraz ze wszystkimi obiektami i całą infrastrukturą, zapewniającymi dystrybucję energii elektrycznej i kontrolę środowiskową;

4i) dostawca usług zarządzanych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi związane z instalacją, eksploatacją lub konserwacją produktów ICT, usług ICT, procesów ICT lub systemów informacyjnych przez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy na miejscu lub zdalnie;

4j) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi polegające na realizacji lub wsparciu dla realizacji działań związanych z zarządzaniem ryzykiem w cyberbezpieczeństwie, w tym obsługę incydentów, testów bezpieczeństwa, audytów systemów informacyjnych, doradztwo;

4k) dostawca usług zaufania – dostawcę usług zaufania w rozumieniu 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 (Dz. Urz. UE L 257 z 28.08.2014, str. 73), zwanego dalej „rozporządzeniem 910/2014”;

4l) dostawca wyszukiwarki internetowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługę wyszukiwarki internetowej, o której mowa w art. 2 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/1150 z dnia 20 czerwca 2019 r. w sprawie propagowania sprawiedliwości i przejrzystości dla użytkowników biznesowych korzystających z usług pośrednictwa internetowego (Dz. Urz. UE L 186 z 11.07.2019, str. 57);

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

6) incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;

7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej;

8) incydent w cyberbezpieczeństwie na dużą skalę – incydent, którego skutki przekraczają możliwości reagowania państwa lub który ma poważny wpływ na inne państwo członkowskie Unii Europejskiej;

8a) kierownik podmiotu kluczowego lub podmiotu ważnego – kierownik jednostki w rozumieniu art. 3 ust. 1 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, z późn. zm.[5)]) kierujący podmiotem kluczowym lub podmiotem ważnym, a w przypadku podmiotu kluczowego lub podmiotu ważnego będącego jednostką sektora finansów publicznych – kierownik jednostki sektora finansów publicznych, o którym mowa w art. 53

[5)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 295 i 1598, z 2024 r. poz. 619, 1685 i 1863 oraz z 2025 r. poz. 1218.

ust. 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2025 r. poz. 1483, 1844 i 1846);

9) (uchylony)

10) obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu;

10a) organizacja badawcza – niebędącą podmiotem kluczowym osobę prawną, albo jednostkę organizacyjną nieposiadającą osobowości prawnej, której podstawową działalnością jest działalność, o której mowa w art. 4 ust. 2 pkt 2 lub ust. 3 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2024 r. poz. 1571, z późn. zm.[6)]), w zakresie, w jakim prowadzi ją z wykorzystaniem systemów informacyjnych;

11) podatność – właściwości produktu ICT lub usługi ICT, które mogą być wykorzystane przez cyberzagrożenie;

11a) podmiot finansowy – podmiot, o którym mowa w art. 2 ust. 1 lit. a–t rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniającego rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Dz. Urz. UE L 333 z 27.12.2022, str. 1, z późn. zm.[7)]), zwanego dalej „rozporządzeniem 2022/2554”;

11b) podmiot publiczny – podmiot wskazany w załączniku nr 1 lub 2 do ustawy w sektorze podmioty publiczne;

11c) podmiot krytyczny – podmiot krytyczny w rozumieniu art. 2 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylającej dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164), zwanej dalej „dyrektywą 2022/2557”;

---

6) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1871 i 1897, z 2025 r. poz. 619, 620, 621, 622, 1162, 1794, 1837 i 1864 oraz z 2026 r. poz. 187 i 203.

7) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90177 z 12.03.2024.

11d) podmiot świadczący usługi rejestracji nazw domen – rejestratora lub agenta działającego w imieniu rejestratorów, w tym dostawcę lub odsprzedawcę usług w zakresie prywatnej rejestracji lub pośrednictwa w rejestracji;

11e) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które mogło mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych, które jednak nie wystąpiło lub któremu udało się zapobiec;

11f) poważne cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych lub użytkowników tych systemów przez wywołanie poważnej szkody materialnej lub niematerialnej;

11g) projekt – przedsięwzięcie realizowane w ramach programu, o którym mowa w art. 45a ust. 1, na podstawie umowy o dofinansowanie, zawieranej między beneficjentem a podmiotem udzielającym pomocy;

11h) poważny incydent związany z ICT – poważny incydent związany z technologiami informacyjno-komunikacyjnymi w rozumieniu art. 3 pkt 10 rozporządzenia 2022/2554;

11i) przedsiębiorca komunikacji elektronicznej – przedsiębiorcę komunikacji elektronicznej w rozumieniu art. 2 pkt 39 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej (Dz. U. poz. 1221 oraz z 2025 r. poz. 637 i 820);

11j) przedsiębiorca telekomunikacyjny – przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 40 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej;

11k) proces ICT – proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881;

11l) produkt ICT – produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;

11m) usługa ICT – usługę ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881;

11n) rejestr nazw domen najwyższego poziomu (TLD) – podmiot, któremu powierzono konkretną domenę najwyższego poziomu (TLD) i który odpowiada za zarządzanie nią, w tym za rejestrację nazw domen w ramach TLD oraz za jej techniczne funkcjonowanie, w tym za obsługę jej serwerów nazw, utrzymanie jej baz danych oraz dystrybucję plików strefowych TLD we wszystkich serwerach nazw, bez względu na to, czy którekolwiek z tych działań jest wykonywane przez sam podmiot czy zlecane na zewnątrz, ale z

wyłączeniem sytuacji, w których rejestr wykorzystuje nazwy TLD wyłącznie do własnego użytku;

12) ryzyko – kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji;

13) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka;

14) system informacyjny:

a) 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 2025 r. poz. 1703 oraz z 2026 r. poz. 160), lub

b) urządzenie lub grupę połączonych urządzeń i oprogramowania zaprogramowanych w celu przetwarzania danych

– wraz z danymi przetwarzanymi w postaci elektronicznej;

14a) właściwy organ w rozumieniu rozporządzenia 2022/2554 – Komisję Nadzoru Finansowego w zakresie nadzoru przewidzianego rozporządzeniem 2022/2554;

15) (uchylony)

16) (uchylony)

17) (uchylony)

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

19) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka.

Art. 2a. W przypadku podmiotu publicznego pod pojęciem usługi rozumie się także zadanie publiczne realizowane przez ten podmiot.

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

Art. 3a. W ramach obsługi incydentów podmiot krajowego systemu cyberbezpieczeństwa może w szczególności podejmować działania w celu wykrywania źródła lub dokonywania analizy aktywności, w tym ruchu sieciowego, powodujących wystąpienie incydentu zakłócającego świadczenie usług przez ten podmiot.

Art. 4. Krajowy system cyberbezpieczeństwa obejmuje:

1) podmioty kluczowe;
2) podmioty ważne;
3) CSIRT MON;
4) CSIRT NASK;
5) CSIRT GOV;
6) CSIRT sektorowe;
7) (uchylony)
8) (uchylony)
9) (uchylony)
10) (uchylony)
11) (uchylony)
12) (uchylony)
13) (uchylony)
14) (uchylony)
15) (uchylony)
16) (uchylony)
17) organy właściwe do spraw cyberbezpieczeństwa;
17a) Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC”;
18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym”;
19) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, zwanego dalej „Pełnomocnikiem”;
20) Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium”.

Rozdział 2

Identyfikacja i rejestracja podmiotów kluczowych lub podmiotów ważnych

Art. 5. 1. Podmiotem kluczowym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.[8)]), zwanego dalej „rozporządzeniem 651/2014/UE”;
2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub je przewyższa;
3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub je przewyższa;
4) niezależnie od wielkości podmiotu:
   a) dostawca usług DNS,
   b) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014,
   c) podmiot krytyczny,
   d) podmiot publiczny wskazany w załączniku nr 1 do ustawy w sektorze podmioty publiczne,
   e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7l ust. 2 pkt 1,
   f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy na podstawie art. 7m,
   g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo przez określenie jego rodzaju,
   h) podmiot będący operatorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i

[8)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2015, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159, Dz. Urz. UE L 167 z 30.06.2023, str. 1 oraz Dz. Urz. UE L 2025/90138 z 13.02.2025.

realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2025 r. poz. 1156),

i) rejestr nazw domen najwyższego poziomu (TLD),

j) podmiot świadczący usługi rejestracji nazw domen.

2. Podmiotem ważnym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE oraz która nie jest podmiotem kluczowym;

2) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 2 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE lub przewyższa te wymogi oraz która nie jest podmiotem kluczowym;

3) niekwalifikowany dostawca usług zaufania będący mikro-, małym lub średnim przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;

4) przedsiębiorca komunikacji elektronicznej będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 2 i 3 załącznika I do rozporządzenia 651/2014/UE;

5) podmiot będący inwestorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy – niezależnie od jego wielkości;

6) podmiot zidentyfikowany jako podmiot ważny na podstawie art. 7l ust. 2 pkt 2;

7) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2 do ustawy z nazwy albo przez określenie jego rodzaju;

8) podmiot publiczny, który nie jest podmiotem kluczowym oraz jest samorządową jednostką budżetową, samorządowym zakładem budżetowym, samorządową instytucją kultury albo spółką wykonującą zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia

20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679), jeżeli realizuje zadanie publiczne z wykorzystaniem systemów informacyjnych.

3. Przy określaniu wymogów dla podmiotów, o których mowa w ust. 1 pkt 1–3, ust. 2 pkt 1–4, nie stosuje się przepisu art. 3 ust. 4 załącznika I do rozporządzenia 651/2014/UE.

4. Jeżeli podmiot, o którym mowa w ust. 1, spełnia wymogi zarówno dla podmiotu kluczowego, jak i dla podmiotu ważnego, to jest podmiotem kluczowym.

5. Jeżeli status podmiotu kluczowego lub podmiotu ważnego zależy od wielkości podmiotu, to przesłanki uznania za podmiot kluczowy lub podmiot ważny bada się według stanu na dzień sporządzenia sprawozdania finansowego.

6. Jeżeli podmiot spełnia wymogi do uznania za podmiot kluczowy, ponieważ przewyższa kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem kluczowym.

7. Jeżeli podmiot spełnia wymogi do uznania za podmiot ważny, ponieważ spełnia kryteria dla średniego przedsiębiorstwa zgodnie z art. 6 ust. 2–4 załącznika I do rozporządzenia 651/2014/UE, ale jego system informacyjny jest niezależny od systemów informacyjnych jego przedsiębiorstw powiązanych lub przedsiębiorstw partnerskich lub nie świadczy on usług wspólnie z jego przedsiębiorstwami powiązanymi lub przedsiębiorstwami partnerskimi, to nie jest podmiotem ważnym.

8. Podmiot leczniczy, który nie jest przedsiębiorcą:

1) jest podmiotem ważnym, jeżeli zatrudnia od 50 do 249 osób;
2) jest podmiotem kluczowym, jeżeli zatrudnia co najmniej 250 osób.

9. Podmiot, o którym mowa w ust. 1 pkt 4 lit. h, staje się podmiotem kluczowym z dniem:

1) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 3 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe (Dz. U. z 2026 r. poz. 1) – w przypadku operatora składowiska odpadów promieniotwórczych;
2) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji

na wytwarzanie energii elektrycznej lub ciepła, o których mowa w art. 32 ust. 1 pkt 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2026 r. poz. 43), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora elektrowni jądrowej;

3) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe, lub uzyskania koncesji na wydobywanie kopalin, o której mowa w art. 22 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2026 r. poz. 69), w zależności od tego, które zostanie uzyskane pierwsze – w przypadku operatora zakładu do wydobywania rud uranu i toru ze złóż i do ich wstępnego przetwarzania;

4) uzyskania zezwolenia na eksploatację, o której mowa w art. 4 ust. 1 pkt 2 ustawy z dnia 29 listopada 2000 r. – Prawo atomowe – w przypadku operatorów pozostałych obiektów energetyki jądrowej.

10. Do podmiotów kluczowych lub podmiotów ważnych nie zalicza się służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2025 r. poz. 902 i 1366 oraz z 2026 r. poz. 26), a także podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej.

11. Minister Obrony Narodowej wskaże, w drodze decyzji niepodlegającej ogłoszeniu, jednostki jemu podległe lub przez niego nadzorowane, które uznaje się za podmioty kluczowe lub podmioty ważne, oraz określi sektor lub sektory, a także w razie potrzeby podsektor, do jakiego przypisuje dany podmiot.

Art. 5a. 1. Podmiot kluczowy lub podmiot ważny podlegają obowiązkom wynikającym z ustawy, jeżeli mają miejsce zamieszkania na terytorium Rzeczypospolitej Polskiej lub prowadzą działalność na terytorium Rzeczypospolitej Polskiej przez swoje siedziby, oddziały lub w ramach działalności transgranicznej.

2. Przedsiębiorca komunikacji elektronicznej podlega obowiązkom wynikającym z ustawy, jeżeli świadczy usługi na terytorium Rzeczypospolitej Polskiej.

3. Dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury

obliczeniowej, dostawca usługi centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej podlega obowiązkom wynikającym z ustawy, jeżeli Rzeczpospolita Polska jest głównym miejscem prowadzenia działalności przez ten podmiot.

4. Głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym ma siedzibę kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1.

5. W przypadku gdy nie można ustalić, czy kierownik podmiotu podejmujący decyzje w sprawie systemu zarządzania bezpieczeństwem informacji ma siedzibę w państwie członkowskim Unii Europejskiej, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym są realizowane zadania związane z systemem zarządzania bezpieczeństwem informacji, o których mowa w art. 8 ust. 1.

6. W przypadku gdy informacji, o której mowa w ust. 5, również nie można ustalić, to głównym miejscem prowadzenia działalności jest państwo członkowskie Unii Europejskiej, w którym podmiot, o którym mowa w ust. 3, ma największą liczbę osób zatrudnionych w odniesieniu do innych państw członkowskich Unii Europejskiej.

7. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, wyznacza przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej.

8. Przedstawicielem, o którym mowa w ust. 7, może być osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona na terytorium Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu podmiotu wskazanego w ust. 1, który nie posiada jednostki organizacyjnej w

jednym z państw członkowskich Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może się zwrócić w związku z obowiązkami podmiotu wynikającymi z ustawy.

9. Podmiot, o którym mowa w ust. 3, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje swoje usługi na terytorium Rzeczypospolitej Polskiej, podlega właściwości polskiego organu właściwego do spraw cyberbezpieczeństwa, jeżeli wyznaczył przedstawiciela posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.

10. Ustawę stosuje się do podmiotów publicznych niezależnie od miejsca ich siedziby.

Art. 6. (uchylony)

Art. 7. 1. Wykaz podmiotów kluczowych i podmiotów ważnych, zwany dalej „wykazem”, jest prowadzony w celu:

1) identyfikacji podmiotów kluczowych i podmiotów ważnych;
2) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi i podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa;
3) umożliwienia prowadzenia czynności nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi.

2. Wykaz zawiera:

1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;
2) sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do ustawy;
3) adres siedziby i adres do korespondencji;
4) adres do doręczeń elektronicznych, jeżeli został wpisany do bazy adresów elektronicznych;
5) adres poczty elektronicznej;
6) numer identyfikacji podatkowej (NIP), jeżeli został nadany;

7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON), jeżeli został nadany;
8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany;
9) zakres publicznych adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny w sposób ciągły;
10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny w sposób ciągły;
11) dane osób do kontaktu z podmiotami z krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej, a w przypadku osoby, która będzie pełnić rolę administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, dodatkowo numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014;
12) numer telefonu przyporządkowany do wykonywanej działalności;
13) deklarację podmiotu kluczowego lub podmiotu ważnego, czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, albo przekracza te kryteria, a w przypadku podmiotu leczniczego, który nie jest przedsiębiorcą, oraz urzędu gminy – deklarację wskazującą liczbę osób zatrudnionych według stanu na dzień sporządzenia sprawozdania finansowego;
14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność, wraz z określeniem rodzaju wykonywanej działalności;
15) w przypadku dostawcy usług DNS, rejestru nazw domen najwyższego poziomu (TLD), podmiotu świadczącego usługi rejestracji nazw domen, dostawcy chmury obliczeniowej, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowej platformy handlowej, dostawcy wyszukiwarki internetowej oraz

dostawcy platformy usług sieci społecznościowych – główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6;

16) informację o zawarciu umowy z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa na realizację zadań, o których mowa w art. 8 i art. 11, wraz z danymi tego dostawcy zawierającymi nazwę (firmę) dostawcy, adres siedziby, adres do korespondencji, numer telefonu, adres poczty elektronicznej;
17) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5a ust. 7, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:
    a) w przypadku osób fizycznych: imię i nazwisko, adres do korespondencji, numer telefonu służbowego oraz adres służbowej poczty elektronicznej,
    b) w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, adres siedziby, adres do korespondencji, numer telefonu oraz adres poczty elektronicznej;
18) informację o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 6;
19) informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny;
20) wskazanie organu właściwego do spraw cyberbezpieczeństwa dla podmiotu kluczowego lub podmiotu ważnego;
21) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego;
22) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu ważnego;
23) numer w wykazie;
24) datę wpisu do wykazu;
25) podstawę prawną wpisania do wykazu;
26) datę wykreślenia z wykazu.

3. Do danych, o których mowa w ust. 2, nie stosuje się przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902 oraz z 2025 r. poz. 1844) oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych

danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

4. Organ właściwy do spraw cyberbezpieczeństwa prowadzi wykaz w zakresie nadzorowanego sektora i w tym zakresie jest administratorem danych zawartych w wykazie.

5. Organ właściwy do spraw cyberbezpieczeństwa:

1) może wpisać podmiot do wykazu zgodnie z art. 7j i art. 7l ust. 6;
2) wykreśla podmiot z wykazu zgodnie z art. 7f ust. 2;
3) może dokonać czynności sprawdzających, o których mowa w art. 7k.

6. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, za pomocą którego wykaz jest prowadzony.

7. Minister właściwy do spraw informatyzacji jest współadministratorem danych, w tym danych osobowych, gromadzonych w wykazie.

8. Minister właściwy do spraw informatyzacji podejmuje czynności, o których mowa w art. 7a, art. 7b ust. 1 i 2, art. 7d ust. 6, art. 7e, art. 7f ust. 1, art. 7g ust. 1 i 2, art. 7i oraz art. 7m.

Art. 7a. 1. Dane, o których mowa w art. 7 ust. 2 pkt 19–26, uzupełnia minister właściwy do spraw informatyzacji.

2. W przypadku:

1) przedsiębiorców telekomunikacyjnych,
2) dostawców usług zaufania,
3) podmiotów publicznych,
4) podmiotów krytycznych

– minister właściwy do spraw informatyzacji wpisuje do wykazu dane, o których mowa w art. 7 ust. 2 pkt 1–8 oraz pkt 19–26, dotyczące tych podmiotów – na podstawie danych zawartych w rejestrach publicznych, bazie adresów elektronicznych lub przekazanych przez właściwe organy nadzorcze.

Art. 7b. 1. Zawiadomienie o wpisie do wykazu z urzędu minister właściwy do spraw informatyzacji doręcza podmiotom kluczowym lub podmiotom ważnym.

2. Minister właściwy do spraw informatyzacji wzywa podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, do uzupełnienia brakujących

danych w wykazie, w terminie 6 miesięcy od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej.

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

1) podstawę prawną wpisu do wykazu;
2) numer podmiotu w wykazie;
3) dane podmiotu wpisane do wykazu oraz wskazanie źródła ich pochodzenia;
4) wskazanie brakujących danych, które podmiot musi uzupełnić.

4. Podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, uzupełniają dane w wykazie, składając wniosek o zmianę wpisu w tym wykazie, w tym również uzupełniają dane w wykazie w zakresie ich działalności, która nie została objęta wpisem z urzędu.

5. Zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2025 r. poz. 1691).

6. W przypadku przedsiębiorców telekomunikacyjnych zawiadomienie o wpisie do wykazu z urzędu oraz wezwanie, o którym mowa w ust. 2, może być doręczone za pomocą Platformy Usług Elektronicznych Urzędu Komunikacji Elektronicznej w ramach współpracy ministra właściwego do spraw informatyzacji z Prezesem Urzędu Komunikacji Elektronicznej.

7. Sprawy, o których mowa w ust. 1 i 2, mogą być załatwiane w sposób, o którym mowa w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 7c. 1. Podmiot kluczowy lub podmiot ważny składają wniosek o wpis do wykazu, w terminie 6 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

2. Wniosek o wpis do wykazu zawiera dane, o których mowa w art. 7 ust. 2 pkt 1–18.

3. Podmiot kluczowy lub podmiot ważny składają wniosek o zmianę wpisu w wykazie w zakresie danych, o których mowa w art. 7 ust. 2 pkt 1–18, w terminie 14 dni od dnia ich zmiany.

4. Wniosek o zmianę wpisu w wykazie zawiera wskazanie zmienianych danych oraz numer podmiotu w tym wykazie.

5. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu zawiera oświadczenie kierownika podmiotu kluczowego lub podmiotu ważnego o następującej treści: „Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny oświadczam, że dane zawarte we wniosku są zgodne z prawdą.”. Klauzula ta zastępuje pouczenie o odpowiedzialności karnej za złożenie fałszywego oświadczenia. Odpowiedzialność za złożenie fałszywego oświadczenia nie obejmuje podania zakresów adresów IP oraz zakresów nazw domenowych.

6. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym kierownika podmiotu kluczowego lub podmiotu ważnego lub osoby przez niego upoważnionej albo kwalifikowaną pieczęcią elektroniczną ze wskazaniem w treści pisma osoby opatrującej pismo pieczęcią. Wniosek składa się w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

7. W przypadku działania przez pełnomocnika do wniosku o wpis, zmianę wpisu albo o wykreślenie z wykazu dołącza się pełnomocnictwo w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. W przypadku pełnomocnika podmiotu ujawnionego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub prokurenta ujawnionego w Krajowym Rejestrze Sądowym nie dołącza się pełnomocnictwa.

Art. 7d. 1. Wpisu podmiotu do wykazu dokonuje się z chwilą złożenia wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

2. Podmiot kluczowy lub podmiot ważny prowadzący kilka rodzajów działalności wykazują odrębnie te działalności we wniosku.

3. Wpisu do wykazu nie dokonuje się, jeżeli wniosek:

1) nie zawiera danych podlegających wpisowi zgodnie z art. 7 ust. 2 pkt 1–18;
2) dotyczy podmiotu kluczowego lub podmiotu ważnego już wpisanego do wykazu;
3) nie zawiera oświadczenia, o którym mowa w art. 7c ust. 5;
4) nie został podpisany.

4. Zmiany wpisu do wykazu nie dokonuje się, jeżeli wniosek o zmianę wpisu:

1) nie zawiera nazwy podmiotu oraz numeru podmiotu w wykazie;
2) nie zawiera wskazania danych zmienianych;
3) nie zawiera oświadczenia, o którym mowa w art. 7c ust. 5;
4) nie został podpisany.

5. Wpis, zmiana wpisu oraz wykreślenie wpisu z wykazu jest czynnością materialno-techniczną i ma charakter deklaratoryjny.

6. Minister właściwy do spraw informatyzacji wydaje, na żądanie podmiotu wpisanego do wykazu, zaświadczenie o wpisie podmiotu do wykazu albo o zmianie tego wpisu wraz ze wskazaniem aktualnych danych zawartych w wykazie dotyczących podmiotu.

7. Zaświadczenie, o którym mowa w ust. 6, jest wydawane w postaci dokumentu elektronicznego, opatrzonego kwalifikowaną pieczęcią elektroniczną, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

Art. 7e. Minister właściwy do spraw informatyzacji co najmniej raz w roku aktualizuje dane zawarte we wpisach w wykazie w zakresie nazwy podmiotu na podstawie danych pozyskanych z publicznie dostępnych rejestrów publicznych.

Art. 7f. 1. Minister właściwy do spraw informatyzacji wykreśla podmiot z wykazu, po uzyskaniu informacji o wykreśleniu podmiotu z krajowego rejestru urzędowego podmiotów gospodarki narodowej (REGON), Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

2. Organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu, w zakresie nadzorowanego sektora, podsektora lub rodzaju działalności, jeżeli:

1) podmiot wpisany do wykazu nie jest podmiotem kluczowym albo podmiotem ważnym;
2) podmiot wpisany do wykazu utracił status podmiotu kluczowego albo podmiotu ważnego po wpisie do wykazu.

3. Podmiot kluczowy lub podmiot ważny składają za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wniosek o wykreślenie z wykazu w zakresie sektora, podsektora lub rodzaju działalności, jeżeli przestały spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny w tym

sektorze, podsektorze lub dla określonego rodzaju działalności. Wniosek o wykreślenie z wykazu zawiera uzasadnienie.

4. Organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek w terminie miesiąca od dnia złożenia wniosku i informuje o wykreśleniu albo odmowie wykreślenia z wykazu.

5. Organ właściwy do spraw cyberbezpieczeństwa odmawia wykreślenia podmiotu z wykazu, jeżeli podmiot nadal spełnia przesłanki uznania za podmiot kluczowy lub podmiot ważny.

6. Odmowa wykreślenia jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.

7. Brak odmowy wykreślenia podmiotu z wykazu w terminie, o którym mowa w ust. 4, skutkuje wykreśleniem podmiotu z wykazu.

8. Wykreślenie podmiotu z wykazu jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

Art. 7g. 1. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowemu w zakresie sektora lub podsektora, dla którego został ustanowiony, organowi właściwemu do spraw cyberbezpieczeństwa w zakresie nadzorowanego sektora lub podsektora, a także podmiotowi kluczowemu lub podmiotowi ważnemu w zakresie go dotyczącym.

2. Minister właściwy do spraw informatyzacji udostępnia dane, o których mowa w art. 7 ust. 2, na wniosek, następującym podmiotom:

1) Agencji Bezpieczeństwa Wewnętrznego,
2) Agencji Wywiadu,
3) dyrektorowi Rządowego Centrum Bezpieczeństwa,
4) organom Krajowej Administracji Skarbowej,
5) Najwyższej Izbie Kontroli,
6) Policji,
7) Prezesowi Urzędu Lotnictwa Cywilnego,
8) Prezesowi Urzędu Ochrony Danych Osobowych,
9) Prezesowi Urzędu Transportu Kolejowego,
10) Prokuratorii Generalnej Rzeczypospolitej Polskiej,

11) prokuratorowi,
12) sądom,
13) Służbie Kontrwywiadu Wojskowego,
14) Służbie Ochrony Państwa,
15) Służbie Wywiadu Wojskowego,
16) Straży Granicznej,
17) Żandarmerii Wojskowej

– w zakresie niezbędnym do realizacji ich ustawowych zadań.

3. Udostępnianie danych, o których mowa w art. 7 ust. 2, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

4. Informacja o zmianie wpisu w wykazie lub o wykreśleniu podmiotu z wykazu jest przechowywana w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, przez 5 lat od dokonania tej zmiany lub wykreślenia. W informacji wskazuje się datę i czas dokonania zmiany lub wykreślenia.

5. Dane administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, w tym numer PESEL lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, są dostępne wyłącznie dla ministra właściwego do spraw informatyzacji lub jednostki podległej temu ministrowi albo przez niego nadzorowanej, której powierzył realizację zadania rozwoju lub utrzymania systemu. Przepisu zdania pierwszego nie stosuje się do uprawnień sądu i prokuratora w ramach przeprowadzania dowodu w postępowaniu karnym, postępowaniu cywilnym, postępowaniu sądowoadministracyjnym.

Art. 7h. Informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny przekazuje ministrowi właściwemu do spraw informatyzacji dyrektor Rządowego Centrum Bezpieczeństwa.

Art. 7i. Minister właściwy do spraw informatyzacji udostępnia w portalu danych, o którym mowa w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, liczbę podmiotów kluczowych lub podmiotów ważnych w podziale na sektory, podsektory i rodzaj działalności. Dane te są aktualizowane nierzadziej niż raz na kwartał.

Art. 7j. 1. Organ właściwy do spraw cyberbezpieczeństwa może wpisać podmiot do wykazu, jeżeli podmiot ten spełnia przesłanki uznania go za podmiot kluczowy albo podmiot ważny, oraz podmiot ten nie złożył wniosku w terminie, o którym mowa w art. 7c ust. 1.

2. Dokonując wpisu podmiotu do wykazu, organ właściwy do spraw cyberbezpieczeństwa korzysta z danych zawartych w publicznie dostępnych rejestrach publicznych, danych dostępnych organowi na podstawie przepisów odrębnych oraz informacji uzyskanych od podmiotu na podstawie art. 43 ust. 1.

3. Organ właściwy do spraw cyberbezpieczeństwa zawiadamia podmiot o wpisie do wykazu na podstawie ust. 1 oraz wzywa ten podmiot do uzupełnienia brakujących danych w wykazie, w terminie 6 miesięcy od dnia otrzymania zawiadomienia, pod rygorem nałożenia kary pieniężnej.

4. Zawiadomienie o wpisie do wykazu na podstawie ust. 1 oraz wezwanie, o którym mowa w ust. 3, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

5. Wpis do wykazu na podstawie ust. 1 jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego, i wymaga uzasadnienia.

Art. 7k. 1. Organ właściwy do spraw cyberbezpieczeństwa może dokonywać czynności sprawdzających mających na celu weryfikację zgodności ze stanem faktycznym danych zawartych w wykazie.

2. W przypadku stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym, organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu, w terminie 7 dni od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Do doręczenia wezwania stosuje się przepisy działu I rozdziału 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Organ właściwy do spraw cyberbezpieczeństwa poprawia, z urzędu, oczywiste omyłki i błędy zawarte w wykazie.

Art. 7l. 1. Organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, może uznać osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub podmiot ważny,

która nie spełnia przesłanek określonych w art. 5 ust. 1 pkt 1–3, pkt 4 lit. a–d oraz g–j, ust. 2 pkt 1–5 oraz 7 i 8, ust. 3–11, jeżeli:

1) jest podmiotem określonym w załączniku nr 1 lub 2 do ustawy;
2) spełnia co najmniej jedną z poniższych przesłanek:
   a) jako jedyna świadczy usługę, za pomocą systemu informacyjnego, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
   b) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego,
   c) zakłócenie usługi świadczonej przez nią za pomocą systemu informacyjnego spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub
   d) świadczenie przez nią, za pomocą systemu informacyjnego, usługi ma istotne znaczenie na poziomie wojewódzkim lub krajowym lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

2. Podmiot uznaje się za:

1) podmiot kluczowy, jeżeli prowadzi działalność określoną w załączniku nr 1 do ustawy;
2) podmiot ważny, jeżeli prowadzi działalność określoną w załączniku nr 2 do ustawy.

3. W decyzji, o której mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa:

1) określa sektor i podsektor, do którego został przypisany podmiot;
2) wzywa podmiot do uzupełnienia brakujących danych w wykazie, w terminie 6 miesięcy od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania do uzupełnienia brakujących danych w wykazie stosuje się przepis art. 7b ust. 3.

5. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu.

6. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie wpisuje do wykazu podmiot, wobec którego wydano decyzję, o której mowa w ust. 1.

7. Podmiot, wobec którego wydano decyzję, o której mowa w ust. 1:

1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,
2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.

Art. 7m. 1. Minister właściwy do spraw informatyzacji może uznać, w drodze decyzji, państwową osobę prawną, o której mowa w art. 3 ust. 1 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125, 834, 1823, 1897 i 1940 oraz z 2026 r. poz. 160), za podmiot kluczowy w sektorze podmiotów publicznych, jeżeli realizuje, za pomocą systemu informacyjnego, zadanie publiczne:

1) którego zakłócenie spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego lub
2) które ma istotne znaczenie na poziomie krajowym.

2. Decyzja, o której mowa w ust. 1, podlega natychmiastowemu wykonaniu.

3. Minister właściwy do spraw informatyzacji wzywa państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1, do uzupełnienia brakujących danych w wykazie, w terminie 6 miesięcy od dnia doręczenia decyzji, o której mowa w ust. 1, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania do uzupełnienia brakujących danych w wykazie, o którym mowa w ust. 3, stosuje się przepis art. 7b ust. 3.

5. Minister właściwy do spraw informatyzacji niezwłocznie wpisuje do wykazu państwową osobę prawną, wobec której wydano decyzję, o której mowa w ust. 1.

6. Państwowa osoba prawna, wobec której wydano decyzję, o której mowa w ust. 1:

1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,
2) zapewnia przeprowadzenie po raz pierwszy audytu w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.

Rozdział 3

Obowiązki podmiotów kluczowych lub podmiotów ważnych

Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności:
   a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
   b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
   c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,
   d) bezpieczeństwo zasobów ludzkich,
   e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
   f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,

g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,
j) podstawowe zasady cyberhigieny,
k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,
m) zarządzanie aktywami,
n) polityki kontroli dostępu;

3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;
4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczność minimalizacji

skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

2. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. e, podmiot kluczowy lub podmiot ważny uwzględnia:

1) podatności związane z dostawcą sprzętu lub oprogramowania;
2) ogólną jakość produktów ICT, usług ICT i procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania;
3) wyniki skoordynowanej oceny bezpieczeństwa przeprowadzonej przez Grupę Współpracy, o której mowa w art. 22 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającej dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), zwanej dalej „dyrektywą 2022/2555”;
4) wyniki postępowania, o którym mowa w art. 67b.

3. Podmiot ważny będący podmiotem publicznym albo podmiotem, o którym mowa w art. 7 ust. 1 pkt 1–4 i 6–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, niebędącym organizacją badawczą w zakresie, w jakim realizuje zadania publiczne z wykorzystaniem systemów informacyjnych, nie stosuje przepisu ust. 1. Podmiot, o którym mowa w zdaniu pierwszym, opracowuje, wdraża, realizuje, monitoruje i utrzymuje w systemach informacyjnych kontrolowanych przez ten podmiot system zarządzania bezpieczeństwem informacji spełniający wymogi określone w załączniku nr 4 do ustawy.

4. Podmiot publiczny uwzględnia w systemie zarządzania bezpieczeństwem informacji system informacyjny dostarczany przez inny podmiot publiczny, w tym na podstawie przepisów ustawy, w szczególności system informacyjny zapewniający działanie rejestru publicznego w zakresie odpowiadającym zakresowi kompetencji tego podmiotu, wynikającym z polityki bezpieczeństwa danego systemu informacyjnego lub przepisów prawa regulujących sposób działania tego systemu.

Art. 8a. Rada Ministrów może określić, w drodze rozporządzenia, odrębnie dla danego rodzaju działalności wykonywanej przez podmioty kluczowe lub

podmioty ważne, szczegółowe wymagania dla systemu zarządzania bezpieczeństwem informacji, o którym mowa w art. 8 ust. 1, biorąc pod uwagę rekomendacje międzynarodowe o charakterze specjalistycznym, w tym rekomendacje Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa, zwanej dalej „ENISA", wielkość podmiotu, skalę działalności wykonywanej przez te podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.

Art. 8b. 1. Dostawcy usług DNS, rejestry nazw domen najwyższego poziomu (TLD), dostawcy usług chmurowych, dostawcy usługi centrum przetwarzania danych, dostawcy sieci dostarczania treści, dostawcy usług zarządzanych, dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa, dostawcy internetowych platform handlowych, dostawcy wyszukiwarek internetowych oraz dostawcy platform usług sieci społecznościowych stosują, w ramach systemu, o którym mowa w art. 8 ust. 1, środki zarządzania ryzykiem określone w rozporządzeniu wykonawczym Komisji (UE) 2024/2690 z dnia 17 października 2024 r. ustanawiającym zasady stosowania dyrektywy (UE) 2022/2555 w odniesieniu do wymogów technicznych i metodycznych dotyczących środków zarządzania ryzykiem w cyberbezpieczeństwie oraz doprecyzowujące przypadki, w których incydent uznaje się za poważny w odniesieniu do dostawców usług DNS, rejestrów nazw TLD, dostawców usług chmurowych, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie bezpieczeństwa, dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych oraz dostawców usług zaufania (Dz. Urz. UE L 2024/2690 z 18.10.2024, z późn. zm.[9)]).

2. W ramach systemu, o którym mowa w art. 8 ust. 1, podmioty kluczowe lub podmioty ważne, inne niż określone w ust. 1, stosują środki zarządzania ryzykiem dla danego rodzaju podmiotu określone w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 21 ust. 5 dyrektywy 2022/2555.

9) Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90225 z 12.03.2025.

3. Podmioty kluczowe lub podmioty ważne z podsektora energii elektrycznej, uznane za podmiot o dużym wpływie lub podmiot o krytycznym wpływie, o którym mowa w art. 52a ust. 2, dodatkowo stosują środki określone w rozporządzeniu delegowanym Komisji (UE) 2024/1366 z dnia 11 marca 2024 r. uzupełniającym rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/943 poprzez ustanowienie kodeksu sieci dotyczącego zasad sektorowych w zakresie aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej (Dz. Urz. UE L 2024/1366 z 24.05.2024, z późn. zm.[10)]), zwanym dalej „rozporządzeniem 2024/1366".

Art. 8c. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność za wykonywanie obowiązków w zakresie cyberbezpieczeństwa przez podmiot kluczowy lub podmiot ważny, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

2. W przypadku gdy kierownikiem podmiotu kluczowego lub podmiotu ważnego jest organ wieloosobowy i nie została wskazana osoba odpowiedzialna, odpowiedzialność ponoszą wszyscy członkowie tego organu.

3. Kierownik podmiotu kluczowego lub podmiotu ważnego ponosi odpowiedzialność także wtedy, gdy niektóre z obowiązków albo wszystkie obowiązki zostały powierzone innej osobie za jej zgodą.

Art. 8d. Kierownik podmiotu kluczowego lub podmiotu ważnego:

1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie;
2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa;
3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;
4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie;

[10)] Zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/90558 z 16.09.2024.

5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Art. 8e. 1. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa, raz w roku kalendarzowym przechodzi szkolenie.

2. Zakres szkolenia obejmuje wykonywanie obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8f ust. 1 i 2, art. 9–12b, art. 14 i art. 15.

3. Udział w szkoleniu jest udokumentowany.

Art. 8f. 1. Przed rozpoczęciem realizacji zadań, o których mowa w art. 8 lub art. 11, osoba, która ma te zadania realizować, przedstawia podmiotowi kluczowemu lub podmiotowi ważnemu informację o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji. Kierownik podmiotu kluczowego lub podmiotu ważnego dopuszcza osobę do realizacji zadań, o których mowa w art. 8 lub art. 11, po otrzymaniu informacji, o której mowa w zdaniu pierwszym.

2. Podmiot kluczowy lub podmiot ważny wzywa osobę realizującą zadania, o których mowa w art. 8 lub art. 11, do ponownego przedstawienia informacji o osobie z Krajowego Rejestru Karnego, jeżeli poważnie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji.

3. Wymagania, o których mowa w ust. 1 i 2, uznaje się za spełnione, jeżeli osoba realizująca zadania, o których mowa w art. 8 i art. 11, posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej.

4. Osoba skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie może realizować zadań, o których mowa w art. 8 lub art. 11.

Art. 8g. Podmiot kluczowy będący dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa świadczącym usługę obsługi incydentów udostępnia na swojej stronie internetowej co najmniej następujące informacje na temat swojej działalności:

1) nazwę (firmę);

2) zakres działania, w tym:
   a) oferowany rodzaj wsparcia,
   b) zasady współpracy i wymiany informacji,
   c) politykę komunikacji;
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 elektronicznej z dostawcą,
   c) dane o wykorzystywanych kluczach publicznych i sposobach szyfrowania komunikacji z dostawcą,
   d) sposoby kontaktu z dostawcą, w tym sposób zgłaszania incydentów.

Art. 8h. 1. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą wymieniać między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu informacyjnego, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki.

2. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, jest dopuszczalna, jeżeli:

1) ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach lub łagodzenie ich skutków lub
2) zwiększa poziom cyberbezpieczeństwa, w szczególności przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie ich rozprzestrzeniania się, eliminowanie i ujawnianie podatności, techniki wykrywania cyberzagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego

działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

3. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, odbywa się za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, systemów teleinformatycznych zapewnianych przez organy właściwe do spraw cyberbezpieczeństwa lub w drodze porozumień, o których mowa w ust. 6.

4. Wymieniając informacje, o których mowa w ust. 1, podmioty kluczowe lub podmioty ważne oznaczają zakres odbiorców tych informacji. Odbiorca informacji może ją udostępniać w zakresie określonym przez wytwórcę informacji.

5. Wymieniając informacje, o których mowa w ust. 1, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 w ust. 1, nie przekazuje się danych osobowych.

6. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, dostawcy sprzętu lub oprogramowania dla tych podmiotów lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne mogą zawierać porozumienia w sprawie wymiany informacji, o których mowa w ust. 1, w szczególności określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia.

7. Koszty wykonania porozumień, o których mowa w ust. 6, są ponoszone w równych częściach przez wszystkie strony, chyba że w danym porozumieniu postanowiono inaczej.

Art. 8i. 1. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych nie stosuje się przepisów ustawy dotyczących systemu zarządzania bezpieczeństwem informacji lub zgłaszania poważnych incydentów, z wyjątkiem art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d oraz art. 67g–67i.

2. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się odpowiednio przepisy art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.

3. Do podmiotów kluczowych lub podmiotów ważnych z sektora bankowości i infrastruktury rynków finansowych stosuje się przepisy rozdziałów 11 i 14 ustawy

w zakresie art. 3a, art. 5 ust. 1–3, art. 7–7m, art. 8 ust. 1 pkt 1 i pkt 2 lit. j, art. 8h, art. 9, art. 11 ust. 1 pkt 5 i 6, art. 13, art. 16, art. 26a ust. 2–4, art. 32, art. 33 ust. 5, 7 i 8, art. 36a, art. 36b, art. 37, art. 43, art. 45 ust. 3, art. 46 ust. 1 pkt 1, 2, 4–7 i ust. 4–6, art. 67a, art. 67c, art. 67d, art. 67g–67i oraz stosowanych odpowiednio przepisów art. 8c–8f, art. 12 ust. 7 oraz art. 31 ust. 1.

Art. 8j. Służby specjalne mogą stosować środki zapobiegające i ograniczające wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do realizacji zadań w tym niezwłocznie podejmować działania po dostrzeżeniu podatności lub cyberzagrożeń, w tym również dokonywać czasowego ograniczenia ruchu sieciowego przychodzącego do infrastruktury służb specjalnych, który może skutkować zakłóceniem realizacji zadań służb specjalnych, mając na uwadze konieczność minimalizacji skutków ograniczenia możliwości realizacji tych działań.

Art. 9. 1. Podmiot kluczowy lub podmiot ważny:

1) wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;
2) zapewnia użytkownikowi usługi dostępu do wiedzy pozwalającej na zrozumienie cyberzagrożeń i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczonymi usługami, w szczególności przez udostępnianie informacji na ten temat na swojej stronie internetowej;
3) zapewnia użytkownikowi usługi możliwość zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą;
4) po uzyskaniu wpisu podmiotu do wykazu rozpoczyna korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

2. Podmiot kluczowy lub podmiot ważny będący mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi.

3. Podmiot ważny będący podmiotem publicznym wyznacza co najmniej jedną osobę odpowiedzialną za utrzymywanie kontaktów z innymi podmiotami kluczowymi lub podmiotami ważnymi.

4. Obowiązek, o którym mowa w ust. 1 pkt 2, może być zrealizowany przez zamieszczenie na stronie internetowej podmiotu hiperłącza do stron internetowych organu właściwego do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

Art. 10. 1. Podmiot kluczowy lub podmiot ważny opracowuje, stosuje i aktualizuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

2. Do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, o której mowa w ust. 1, zalicza się:

1) dokumentację normatywną;
2) dokumentację operacyjną.

3. Dokumentację normatywną stanowią:

1) dokumentacja systemu zarządzania bezpieczeństwem informacji;
2) dokumentacja ochrony infrastruktury, z wykorzystaniem której jest świadczona usługa, obejmująca:
   a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa,
   b) ocenę aktualnego stanu ochrony infrastruktury,
   c) szacowanie ryzyka dla obiektów infrastruktury,
   d) plan postępowania z ryzykiem,
   e) opis zabezpieczeń technicznych obiektów infrastruktury,
   f) zasady organizacji i wykonywania ochrony fizycznej infrastruktury,
   g) dane o specjalistycznej uzbrojonej formacji ochronnej, o której mowa w art. 2 pkt 7 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2025 r. poz. 532), chroniącej infrastrukturę – jeżeli występuje;
3) dokumentacja systemu zarządzania ciągłością działania;
4) dokumentacja techniczna systemu informacyjnego wykorzystywanego w procesie świadczenia usługi;
5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze.

4. Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji

normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów informacyjnych.

5. Dokumentacja dotycząca bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi może być prowadzona w postaci papierowej lub w postaci elektronicznej.

6. Podmiot kluczowy lub podmiot ważny jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zapewniającego:

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

7. Podmiot kluczowy lub podmiot ważny przechowuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi przez okres co najmniej 2 lat od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od dnia 1 stycznia roku następującego po roku, w którym wygasa okres jej przechowywania. Przepisu nie stosuje się do podmiotów podlegających ustawie z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2020 r. poz. 164 oraz z 2025 r. poz. 1173).

8. Zniszczenie wycofanej z użytkowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, opis sposobu zniszczenia, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi są przechowywane w sposób trwały.

Art. 11. 1. Podmiot kluczowy lub podmiot ważny:

1) zapewnia obsługę incydentu;

2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu w zakresie niezbędnym do realizacji jego zadań;
3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny;
4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, niepóźniej niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;
4a) zgłasza incydent poważny niezwłocznie, niepóźniej niż w ciągu 72 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;
4b) przekazuje, na wniosek właściwego CSIRT sektorowego, sprawozdanie okresowe z obsługi incydentu poważnego;
4c) przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe z obsługi incydentu poważnego, niepóźniej niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a;
5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym, przekazując niezbędne dane, w tym dane osobowe;
6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

1a. Dostawca usług zaufania zgłasza incydent poważny niezwłocznie, niepóźniej niż w ciągu 24 godzin od momentu jego wykrycia do właściwego CSIRT sektorowego.

2. Wczesne ostrzeżenie, o którym mowa w ust. 1 pkt 4, zgłoszenie, o którym mowa w ust. 1 pkt 4a, sprawozdanie okresowe, o którym mowa w ust. 1 pkt 4b, sprawozdanie końcowe, o którym mowa w ust. 1 pkt 4c, oraz sprawozdanie z postępu obsługi incydentu poważnego, o którym mowa w art. 12b ust. 1, są przekazywane za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

2a. W przypadku zaistnienia poważnego cyberzagrożenia podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Podmiot kluczowy lub podmiot ważny

informuje tych użytkowników o samym poważnym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.

2b. Podmiot kluczowy lub podmiot ważny informuje użytkowników swoich usług o incydencie poważnym, jeżeli ma on niekorzystny wpływ na świadczenie tych usług.

3. (uchylony)

4. Rada Ministrów określi, w drodze rozporządzenia, progi uznania incydentu za poważny według rodzaju zdarzenia w poszczególnych sektorach i podsektorach określonych w załącznikach nr 1 i 2 do ustawy, z wyłączeniem progów uznania incydentu za poważny, dla podmiotów, dla których progi te określiła Komisja Europejska w akcie wykonawczym wydanym na podstawie art. 23 ust. 11 dyrektywy 2022/2555, wskazując w zależności od rodzaju zdarzenia, czy odnosi się ono do:

1) liczby użytkowników, których dotyczy zakłócenie świadczenia usługi,
2) czasu oddziaływania incydentu na świadczoną usługę,
3) zasięgu geograficznego obszaru, którego dotyczy incydent,
4) innych czynników charakterystycznych dla danego sektora lub podsektora, jeżeli występują

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

Art. 12. 1. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer z właściwego rejestru, siedzibę i adres;
2) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu służbowego oraz adres służbowej poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania;

5) wskazanie, czy incydent poważny został wywołany działaniem bezprawnym lub działaniem w złej wierze, jeżeli możliwe jest dokonanie takiej oceny;
6) określenie, czy incydent dotyczy innych państw członkowskich Unii Europejskiej.

2. Wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4, może zawierać wniosek o wskazanie wytycznych dotyczących możliwych do wdrożenia środków ograniczających skutki incydentu poważnego lub o dodatkowe wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy niepóźniej niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela dodatkowego wsparcia technicznego, a w przypadku incydentu poważnego wyczerpującego znamiona przestępstwa również informacje o sposobie zgłoszenia organom ścigania.

3. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, zawiera:

1) opis wpływu incydentu poważnego na świadczenie usługi, w tym:
   a) wskazanie usługi zgłaszającego, na którą incydent poważny miał wpływ,
   b) liczbę użytkowników usługi, na których incydent poważny miał wpływ,
   c) zasięg geograficzny obszaru, którego dotyczy incydent poważny,
   d) wpływ incydentu poważnego na świadczenie usługi przez inne podmioty;
2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne lub świadczone usługi;
3) informacje o podjętych działaniach zapobiegawczych;
4) informacje o podjętych działaniach naprawczych;
5) aktualizację informacji, o których mowa w ust. 1, jeżeli nastąpiła ich zmiana.

4. Zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, może zawierać także inne istotne informacje związane z przebiegiem incydentu poważnego lub podjętymi działaniami.

5. Podmiot kluczowy lub podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, które uzupełnia w trakcie obsługi incydentu poważnego.

6. Podmiot kluczowy lub podmiot ważny przekazuje, w niezbędnym zakresie, we wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, informacje stanowiące tajemnice prawnie

chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego.

7. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy może zwrócić się do podmiotu kluczowego lub podmiotu ważnego o uzupełnienie wczesnego ostrzeżenia, o którym mowa w art. 11 ust. 1 pkt 4, lub zgłoszenia, o którym mowa w art. 11 ust. 1 pkt 4a, o informacje, w tym informacje stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

8. We wczesnym ostrzeżeniu, o którym mowa w art. 11 ust. 1 pkt 4, lub w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4a, podmiot kluczowy lub podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 12a. Sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, zawiera:

1) szczegółowy opis incydentu poważnego, w tym spowodowane zakłócenia i szkody;
2) rodzaj zagrożenia lub przyczynę, która prawdopodobnie była źródłem incydentu;
3) zastosowane i wdrażane środki ograniczające ryzyko;
4) transgraniczne skutki incydentu, jeżeli wystąpiły.

Art. 12b. 1. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie z postępu obsługi tego incydentu.

2. W przypadku gdy obsługa incydentu poważnego nie zakończyła się w terminie składania sprawozdania końcowego, o którym mowa w art. 11 ust. 1 pkt 4c, podmiot kluczowy lub podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe niepóźniej niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego.

Art. 12c. Do podmiotu ważnego będącego podmiotem publicznym stosuje się przepisy art. 11 i art. 12, z wyjątkiem przepisów o przekazywaniu wczesnego

ostrzeżenia, sprawozdania okresowego, sprawozdania z postępu obsługi incydentu i sprawozdania końcowego.

Art. 13. 1. Podmiot kluczowy lub podmiot ważny mogą przekazywać do właściwego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego informacje o:

1) innych incydentach;
2) cyberzagrożeniach;
3) wynikach szacowania ryzyka;
4) podatnościach;
5) potencjalnych zdarzeniach dla cyberbezpieczeństwa;
6) wykorzystywanych technologiach.

2. Informacje, o których mowa w ust. 1, są przekazywane w postaci elektronicznej za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, a w przypadku braku możliwości przekazania w postaci elektronicznej przy użyciu innych dostępnych środków komunikacji.

3. Podmiot kluczowy lub podmiot ważny oznacza informacje, o których mowa w ust. 1, stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 14. Podmiot kluczowy lub podmiot ważny w celu realizacji zadań, o których mowa w art. 8 oraz w art. 9–13, powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z dostawcą usług zarządzanych w zakresie cyberbezpieczeństwa.

Art. 15. 1. Podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata, audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zwany dalej „audytem”, licząc od dnia sporządzenia i podpisania przez audytorów przeprowadzających audyt raportu z ostatniego audytu.

1a. Podmiot kluczowy przedstawia w postaci elektronicznej kopię raportu z przeprowadzonego audytu organowi właściwemu do spraw cyberbezpieczeństwa, w terminie 3 dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny.

1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać podmiotowi kluczowemu w każdym czasie lub podmiotowi ważnemu w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, wraz z określeniem terminu przekazania kopii raportu z przeprowadzonego audytu i wskazaniem rodzaju podmiotów uprawnionych do przeprowadzenia audytu. Organ właściwy do spraw cyberbezpieczeństwa może również określić zakres audytu, o którym mowa w zdaniu pierwszym.

1c. Decyzja, o której mowa w ust. 1b, podlega natychmiastowemu wykonaniu.

2. Audyt może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;
2) co najmniej dwóch audytorów posiadających:
   a) certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub
   b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub
   c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;
3) CSIRT sektorowy, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2.

2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 oraz art. 9–13, lub która realizowała te zadania w podmiocie audytowanym w przeciągu roku przed dniem rozpoczęcia audytu.

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

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;
2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;
3) (uchylony)
4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224 oraz z 2025 r. poz. 1158);
5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623).

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

5. Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je podmiotowi kluczowemu lub podmiotowi ważnemu wraz z dokumentacją z przeprowadzonego audytu.

6. (uchylony)

7. Podmiot kluczowy lub podmiot ważny przekazuje kopię raportu z przeprowadzonego audytu na wniosek:

1) (uchylony)
2) dyrektora Rządowego Centrum Bezpieczeństwa – w przypadku gdy podmiot kluczowy lub podmiot ważny jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

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

Art. 16. Podmiot:

1) kluczowy lub ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 12 miesięcy,
2) kluczowy zapewnia przeprowadzenie audytu po raz pierwszy w terminie 24 miesięcy

– od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

Art. 16a. (uchylony)

Rozdział 3a

Obowiązki rejestrów nazw domen najwyższego poziomu oraz zadania i obowiązki podmiotów świadczących usługi rejestracji nazw domen

Art. 16b. 1. Rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen z należytą starannością zbierają i zachowują dokładne i kompletne dane dotyczące rejestracji nazw domen.

2. Podmioty świadczące usługi rejestracji nazw w konkretnej domenie najwyższego poziomu współpracują z rejestrem nazw tej domeny. Baza danych dotycząca rejestracji nazw domen może funkcjonować w szczególności przez umożliwianie podmiotom świadczącym usługi rejestracji nazw domen przez rejestr nazw domen najwyższego poziomu (TLD) na podstawie umów, zautomatyzowanego wprowadzania i aktualizowania danych oraz inicjowanie związanych z tym czynności administracyjnych i technicznych. W takim przypadku przetwarzanie danych przez podmioty świadczące usługi rejestracji nazw domen nie jest uznawane za powielanie zadań rejestru nazw domen najwyższego poziomu (TLD).

3. W odniesieniu do danych będących danymi osobowymi przetwarzanie w zakresie, o którym mowa w ust. 1 i 2, następuje zgodnie z przepisami dotyczącymi ochrony danych osobowych.

4. Baza danych dotyczących rejestracji nazw domen zawiera:

1) nazwę domeny;

2) datę rejestracji;
3) imię i nazwisko lub nazwę abonenta nazwy domeny oraz adres poczty elektronicznej i numer telefonu;
4) adres poczty elektronicznej i numer telefonu, pod którymi można skontaktować się z punktem kontaktowym zarządzającym nazwą domeny, w przypadku gdy różnią się od adresu poczty elektronicznej i numeru telefonu abonenta nazwy domeny, a w przypadku gdy usługi punktu kontaktowego zarządzającego nazwą domeny nie są dopuszczone dla konkretnej domeny najwyższego poziomu (TLD), należy podać co najmniej dane identyfikujące podmiot świadczący usługi rejestracji nazw domen.

5. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen opracowują i wdrażają polityki i procedury, w tym procedury weryfikacji, służące zapewnieniu, aby bazy danych, o których mowa w ust. 1, zawierały dokładne i kompletne dane. Procedury weryfikacji danych:

1) obejmują działania weryfikacyjne na etapie rejestracji nazwy domeny lub po takiej rejestracji;
2) są wyważone i proporcjonalne;
3) prowadzą do zweryfikowania co najmniej jednego ze sposobów kontaktu, o których mowa w ust. 4 pkt 3 lub 4;
4) obejmują uprawnienie rejestru nazw domen najwyższego poziomu (TLD) lub podmiotów świadczących usługi rejestracji nazw domen do żądania, w uzasadnionych przypadkach, udokumentowania danych identyfikacyjnych innych niż wymienione w ust. 3 lub 4, w szczególności numeru lub innego oznaczenia identyfikacyjnego abonenta nazwy domeny zawartego w rejestrach publicznych, o ile obowiązek jego posiadania wynika z przepisów prawa krajowego obowiązującego takiego abonenta.

6. Polityki i procedury, o których mowa w ust. 5, rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen publikują na swoich stronach internetowych. Polityki i procedury podmiotów świadczących usługi rejestracji nazw w konkretnej domenie najwyższego poziomu (TLD) są zgodne z politykami i procedurami opublikowanymi przez rejestr nazw tej domeny najwyższego poziomu (TLD).

7. Po rejestracji nazwy domeny rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen niezwłocznie publikują na stronie internetowej dane dotyczące rejestracji nazwy domeny, z wyłączeniem danych osobowych.

8. Obowiązek, o którym mowa w ust. 7, może zostać zrealizowany w szczególności przez zamieszczenie danych w ogólnodostępnej bazie abonentów upublicznianej przez rejestr nazw domen najwyższego poziomu (TLD).

9. W przypadku gdy podanie danych, w tym adresu poczty elektronicznej abonenta nazwy domeny, wymaga uzyskania zgody, obowiązek jej uzyskania obciąża podmiot przetwarzający te dane jako pierwszy.

Art. 16c. 1. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen na żądanie:

1) sądu – w celu przeprowadzenia dowodu w postępowaniu karnym, postępowaniu w sprawach o wykroczenia lub w postępowaniu cywilnym,
2) prokuratora – w celu przeprowadzenia dowodu w postępowaniu karnym lub postępowaniu w sprawach o wykroczenia,
3) Policji oraz innych upoważnionych organów w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia – w celu przeprowadzenia dowodu w postępowaniu karnym lub czynnościach wyjaśniających w sprawie o wykroczenie i postępowaniu w sprawach o wykroczenia,
4) CSIRT sektorowego – w celu przeprowadzenia obsługi incydentu poważnego przez CSIRT sektorowy związanego z daną domeną,
5) CSIRT GOV, CSIRT MON lub CSIRT NASK – w celu przeprowadzenia obsługi incydentu poważnego lub incydentu krytycznego związanego z daną domeną,
6) podmiotu wykonującego postanowienie sądu w przedmiocie zabezpieczenia środka dowodowego, o którym mowa w art. 479^{100} § 1 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (Dz. U. z 2024 r. poz. 1568, z późn. zm.[11)]),

[11)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1841, z 2025 r. poz. 620, 1172, 1302, 1518 i 1661 oraz z 2026 r. poz. 26.

7) Prezesa Urzędu Komunikacji Elektronicznej – w celu weryfikacji, czy podmiot składający sprzeciw wobec wpisania domeny na listę ostrzeżeń, o którym mowa w art. 21 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803), dysponuje do tej domeny tytułem prawnym

– udzielają dostępu do konkretnych danych dotyczących rejestracji nazw domen, które mają znaczenie dla prowadzonego postępowania lub czynności wyjaśniających w sprawie o wykroczenie, z zachowaniem przepisów dotyczących ochrony danych osobowych.

2. Żądanie udostępnienia danych, o których mowa w ust. 1, składa się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Żądanie zawiera uzasadnienie.

3. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen udzielają odpowiedzi niepóźniej niż w terminie 72 godzin od dnia otrzymania żądania udostępnienia danych, o którym mowa w ust. 1, w sposób określony w opracowanej przez siebie i podanej do publicznej wiadomości polityce i procedurze ujawniania takich danych.

Rozdział 3b

Wspólne wykonywanie obowiązków z zakresu cyberbezpieczeństwa przez podmioty publiczne

Art. 16d. Podmiot publiczny realizuje obowiązki, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b i art. 15, jeżeli wykorzystuje system informacyjny w celu realizacji zadania publicznego.

Art. 16e. 1. Minister kierujący działem administracji rządowej może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych lub organach podległych oraz nadzorowanych przez tego ministra, a także w obsługującym go urzędzie.

2. Centralny organ administracji rządowej, niebędący ministrem, może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego

nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych podległych oraz nadzorowanych przez ten organ, a także w obsługującym go urzędzie.

3. Wojewoda może wyznaczyć obsługujący go urząd, jednostkę jemu podległą albo przez niego nadzorowaną jako jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach organizacyjnych podległych oraz nadzorowanych przez wojewodę, a także w obsługującym go urzędzie.

4. Prokurator Generalny może spośród powszechnych jednostek organizacyjnych prokuratury wyznaczyć jednostkę odpowiedzialną za realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 9–12b lub art. 15, w pozostałych jednostkach prokuratury.

5. Jednostka samorządu terytorialnego może zapewnić wspólną obsługę realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15. Do wyznaczenia jednostki obsługującej i obsługiwanej stosuje się odpowiednio przepisy art. 10a–10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2025 r. poz. 1153 i 1436), art. 6a–6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym (Dz. U. z 2025 r. poz. 1684) oraz art. 8c–8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2025 r. poz. 581 i 1535).

6. Jednostki samorządu terytorialnego mogą zawrzeć porozumienie w sprawie powierzenia jednej z nich realizacji obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15. Porozumienie może przewidywać powierzenie wykonywania obowiązków dowolnej jednostce, spośród jednostek zawierających porozumienie.

7. W porozumieniu, o którym mowa w ust. 6, wskazuje się jednostki organizacyjne, samorządowe osoby prawne lub spółki, o których mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, jednostki samorządu terytorialnego powierzającej realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, objęte porozumieniem.

8. Jednostka samorządu terytorialnego, której powierzono realizację obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8c–8f, art. 8h, art. 9–12b lub art. 15, wyznacza jednostkę organizacyjną, samorządową osobę prawną lub spółkę, o której mowa w art. 9 ust. 1 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej, do realizacji tych obowiązków.

9. Do porozumień, o których mowa w ust. 6, stosuje się odpowiednio przepisy art. 74 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym.

Art. 16f. Podmioty publiczne, dla których jednostka wyznaczona realizuje obowiązki z zakresu cyberbezpieczeństwa, współpracują z tą jednostką w szczególności przez:

1) przekazywanie informacji o incydentach;
2) wykonywanie decyzji kierownika tej jednostki w zakresie systemu zarządzania bezpieczeństwem informacji;
3) publikowanie na swojej stronie internetowej adresu strony internetowej jednostki wyznaczonej zawierającej informacje o cyberbezpieczeństwie, zgodnie z art. 9;
4) uczestnictwo kierownika tej jednostki w szkoleniach z zakresu cyberbezpieczeństwa, jeżeli są prowadzone przez jednostkę wyznaczoną.

Art. 16g. W celu prawidłowego wykonania obowiązków, o których mowa w art. 11 i art. 12, kierownik jednostki wyznaczonej, o której mowa w art. 16e, może wskazać podmiotom publicznym terminy na przekazanie informacji o incydentach.

Art. 16h. Jednostka wyznaczona, o której mowa w art. 16e:

1) zgłasza w imieniu podmiotu publicznego wczesne ostrzeżenie, zgłoszenie incydentu poważnego, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4–4c, do CSIRT sektorowego;
2) wskazuje osobę kontaktową do podmiotów publicznych, dla których realizuje zadania z zakresu cyberbezpieczeństwa;
3) korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w rozdziale 3.

Rozdział 4

(uchylony)

Rozdział 5

(uchylony)

Rozdział 6

Zadania CSIRT MON, CSIRT NASK i CSIRT GOV

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

1a. W czasie stanu wojennego lub w czasie wojny CSIRT MON, w imieniu Ministra Obrony Narodowej, koordynuje działania CSIRT NASK i CSIRT GOV.

2. CSIRT MON, CSIRT NASK i CSIRT GOV na wniosek podmiotów krajowego systemu cyberbezpieczeństwa mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów, w przypadku gdy:

1) incydent może wpłynąć na inne podmioty krajowego systemu cyberbezpieczeństwa;
2) podmiot obsługujący incydent nie dysponuje środkami pozwalającymi mu na jego skuteczną obsługę, a incydent powoduje przerwanie ciągłości świadczenia usługi.

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

1) CSIRT MON, za zgodą Ministra Obrony Narodowej lub
2) CSIRT NASK, lub
3) CSIRT GOV, za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego.

2b. Zgoda może być wyrażona w formie ustnej lub dokumentowej, w szczególności z wykorzystaniem środków komunikacji elektronicznej. Zgoda wyrażona w formie ustnej wymaga udokumentowania w ciągu 14 dni od dnia jej wydania.

2c. O zapewnieniu wsparcia w obsłudze incydentów, o którym mowa w ust. 2 lub 2a, jest informowany właściwy CSIRT sektorowy.

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

1) monitorowanie cyberzagrożeń i incydentów na poziomie krajowym;
2) szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym zapewnianie dynamicznej analizy ryzyka;
3) przekazywanie informacji dotyczących cyberzagrożeń, podatności, incydentów i ryzyk, wczesne ostrzeganie i alarmowanie podmiotów krajowego systemu cyberbezpieczeństwa;
4) wydawanie komunikatów o zidentyfikowanych cyberzagrożeniach;
5) reagowanie na zgłoszone incydenty;
6) klasyfikowanie incydentów, w tym incydentów poważnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
7) zmiana klasyfikacji incydentów;
8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;
9) przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa, zwanych dalej „rekomendacjami dotyczącymi stosowania urządzeń informatycznych lub oprogramowania”;
10) współpraca z CSIRT sektorowymi w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej, i incydentów krytycznych oraz w

zakresie wymiany informacji pozwalających przeciwdziałać cyberzagrożeniom;

11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych dotyczących dwóch lub większej liczby państw, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

12) przekazywanie, w terminie 14 dni od zakończenia danego kwartału, do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednich 3 miesiącach:
   a) poważnych incydentów,
   b) incydentów,
   c) cyberzagrożeń,
   d) potencjalnych zdarzeń dla cyberbezpieczeństwa;

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

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

15) (uchylony)
16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej oraz Komisji Europejskiej;
17) w odpowiednich przypadkach gromadzenie i zabezpieczanie danych na potrzeby postępowań karnych;
18) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych lub podmiotów ważnych oraz wymiana informacji dotyczących cyberbezpieczeństwa, jeżeli wymiana informacji zapewnia zwiększenie poziomu cyberbezpieczeństwa lub służy przeciwdziałaniu incydentom;
19) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich;
20) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji z podmiotami kluczowymi i podmiotami ważnymi oraz innymi podmiotami;
21) prowadzenie działań na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa 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;
22) promowanie, przyjmowanie i stosowanie wspólnych lub znormalizowanych praktyk, systemów klasyfikacji i systematyki związanych z:
    a) procedurami obsługi incydentu,
    b) zarządzaniem kryzysowym w obszarze cyberbezpieczeństwa,
    c) ujawnianiem podatności;
23) przekazywanie Pełnomocnikowi sprawozdania z wykonywania swoich zadań ustawowych zawierającego w szczególności informacje o zgłoszonych do CSIRT incydentach krytycznych, incydentach poważnych, incydentach, cyberzagrożeniach oraz potencjalnych zdarzeniach dla cyberbezpieczeństwa.

3a. Przy realizacji zadania, o którym mowa w ust. 3 pkt 19, CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać informacje, w tym dane osobowe

w celu informowania o potencjalnych cyberzagrożeniach oraz zastosowanych sposobach ich zwalczania, w celu przeciwdziałania cyberzagrożeniom o charakterze transgranicznym. Informacje, w tym dane osobowe, o których mowa w zdaniu pierwszym, przekazuje się w postaci elektronicznej.

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

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

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
2) przedsiębiorcy realizujący zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825, 1014 i 1080);
3) Ministra Obrony Narodowej.

6. Do zadań CSIRT NASK należy:

1) koordynacja obsługi incydentów zgłaszanych przez:
   a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2a–6 i 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem podmiotów, o których mowa w ust. 5,
   aa) urzędy obsługujące jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 2 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
   b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem podmiotów, o których mowa w ust. 5, oraz jednostek, o których mowa w ust. 7 pkt 2,
   c) instytuty badawcze, z wyjątkiem podmiotów, o których mowa w ust. 5,

ca) międzynarodowe instytuty badawcze, z wyjątkiem podmiotów, o których mowa w ust. 5 pkt 2,

cb) Centrum Łukasiewicz,

cc) instytuty działające w ramach Sieci Badawczej Łukasiewicz, z wyjątkiem podmiotów, o których mowa w ust. 5 pkt 2,

d) Urząd Dozoru Technicznego,

e) (uchylony)

f) Polskie Centrum Akredytacji,

g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej,

h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,

i) (uchylony)

j) podmioty kluczowe lub podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7,

k) inne podmioty niż wymienione w lit. a–j oraz ust. 5 i 7,

l) osoby fizyczne;

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

3) zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzących działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. UE L 335 z 17.12.2011, str. 1);

4) monitorowanie występowania smishingu oraz tworzenie wzorca wiadomości wyczerpującej znamiona smishingu, o którym mowa w art. 4 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1803);

5) prowadzenie i udostępnianie na swojej stronie internetowej wykazu nazw oraz ich skrótów zastrzeżonych dla podmiotów publicznych jako nadpis wiadomości pochodzącej od podmiotu publicznego oraz wariantów tych nazw i skrótów, mogących wprowadzać odbiorcę w błąd co do pochodzenia wiadomości od podmiotu publicznego, o którym mowa w art. 10 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

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

1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, i urzędy je obsługujące, z wyjątkiem wymienionych w ust. 5 i 6;
2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;
3) Narodowy Bank Polski;
4) Bank Gospodarstwa Krajowego;
4a) Polską Agencję Żeglugi Powietrznej;
4b) Polską Agencję Prasową;
4c) Państwowe Gospodarstwo Wodne Wody Polskie;
4d) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju (Dz. U. z 2026 r. poz. 9);
4e) Urząd Komisji Nadzoru Finansowego;
5) inne niż wymienione w pkt 1–4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;
6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

8. CSIRT MON, CSIRT NASK lub CSIRT GOV, który otrzymał zgłoszenie incydentu, a nie jest właściwy do koordynacji jego obsługi, przekazuje

niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

8a. Minister właściwy do spraw informatyzacji może udzielić CSIRT NASK dotacji celowej na zakup, utrzymanie i rozbudowę infrastruktury teleinformatycznej niezbędnej do wykonywania zadań CSIRT NASK.

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

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

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

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

12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 40a.

13. Przepisy ust. 2 i 3 stosuje się odpowiednio do zadań realizowanych przez CSIRT NASK lub CSIRT GOV w sektorze bankowości i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne z tego sektora.

14. CSIRT NASK lub CSIRT GOV może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, gdy nie stanowi to dla tego zespołu nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi, oraz z uwzględnieniem

odpowiedniego stosowania przepisów ust. 2 i 3 do realizacji zadań przez CSIRT NASK lub CSIRT GOV.

15. CSIRT NASK lub CSIRT GOV współpracują i wymieniają informacje z właściwym organem w rozumieniu rozporządzenia 2022/2554, gdy jest to niezbędne dla realizacji zadań CSIRT NASK lub CSIRT GOV bądź realizacji zadań tego właściwego organu.

16. CSIRT MON, CSIRT NASK i CSIRT GOV informują organ właściwy do spraw podmiotów krytycznych o poważnych incydentach, cyberzagrożeniach i potencjalnych zdarzeniach dla cyberbezpieczeństwa zgłoszonych przez podmiot krytyczny.

Art. 26a. 1. CSIRT NASK pełni funkcję koordynatora na potrzeby skoordynowanego ujawniania podatności.

2. Osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej może zgłosić wykrytą podatność do CSIRT NASK.

3. Zgłoszenie podatności jest przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania jej w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.

4. CSIRT NASK zapewnia formularz do dokonywania zgłoszeń podatności, zapewniający możliwość zachowania anonimowości przez osobę fizyczną lub osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej zgłaszającą podatność. CSIRT NASK może przetwarzać przekazane dane osobowe w celu realizacji zadań, o których mowa w ust. 5.

5. W ramach zadania, o którym mowa w ust. 1, CSIRT NASK:

1) przyjmuje informacje o wykrytych podatnościach;
2) identyfikuje dostawców produktów ICT lub usług ICT, na które podatność może mieć wpływ i informuje ich o wykrytej podatności;
3) w razie konieczności koordynuje komunikację między osobą fizyczną lub osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT, w zakresie weryfikacji zgłoszenia i terminu ujawniania podatności.

6. CSIRT NASK współpracuje z CSIRT innych państw członkowskich Unii Europejskiej przy podatnościach, które mają wpływ na podmioty, w pozostałych państwach członkowskich Unii Europejskiej.

Art. 26b. Minister Obrony Narodowej udostępnia CSIRT NASK, na jego wniosek, w terminie 14 dni od doręczenia wniosku, listę przedsiębiorców, wobec których wydano decyzję administracyjną, o której mowa w art. 648 ust. 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny (Dz. U. z 2025 r. poz. 825, 1014 i 1080 oraz z 2026 r. poz. 26).

Art. 26c. 1. CSIRT NASK, w celu minimalizacji ryzyka powstania szkód materialnych i niematerialnych związanych z nieuprawnionym upublicznieniem danych osobowych w sieci Internet, tworzy i udostępnia usługę online umożliwiającą sprawdzenie przez osobę fizyczną, czy jej dane osobowe nie zostały ujawnione w sieci Internet w sposób nieuprawniony, na skutek incydentu lub cyberzagrożenia.

2. Dla realizacji usługi online, o której mowa w ust. 1, CSIRT NASK może gromadzić i przetwarzać następujące dane osobowe:

1) imię i nazwisko;
2) datę urodzenia;
3) adres zamieszkania;
4) płeć;
5) imię i nazwisko nadane podczas urodzenia;
6) miejsce urodzenia;
7) identyfikator użytkownika w Węźle Krajowym nadawany tymczasowo podczas uwierzytelniania;
8) login, który uległ nieuprawnionemu upublicznieniu;
9) adres poczty elektronicznej;
10) numer telefonu;
11) numer PESEL.

Art. 26d. 1. Przed rozpoczęciem realizacji zadań CSIRT MON, CSIRT NASK lub CSIRT GOV, osoba, która ma te zadania realizować, przedstawia właściwemu CSIRT informację o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji.

Kierownik właściwego CSIRT dopuszcza osobę do realizacji zadań, o których mowa w art. 26 ust. 3, po otrzymaniu informacji, o której mowa w zdaniu pierwszym.

2. CSIRT MON, CSIRT NASK lub CSIRT GOV wzywa osobę realizującą jego zadania, o których mowa w art. 26 ust. 3, do ponownego przedstawienia informacji o osobie z Krajowego Rejestru Karnego stwierdzającą niekaralność za przestępstwa przeciwko ochronie informacji, jeżeli poważnie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji.

3. Wymagania, o których mowa w ust. 1 i 2, uznaje się za spełnione, jeśli osoba realizująca zadania CSIRT MON, CSIRT NASK lub CSIRT GOV posiada ważne poświadczenie bezpieczeństwa upoważniające do dostępu do informacji niejawnych o klauzuli „poufne” lub wyższej.

4. Osoba skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji nie może realizować zadań CSIRT MON, CSIRT NASK lub CSIRT GOV, o których mowa w art. 26 ust. 3.

Art. 27. 1. CSIRT GOV jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2025 r. poz. 194).

2. CSIRT MON jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 5 ust. 1 pkt 2a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2024 r. poz. 1405 oraz z 2025 r. poz. 179 i 1366).

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

Art. 28. 1. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV informuje na podstawie zgłoszenia incydentu poważnego dokonanego przez podmiot kluczowy lub podmiot ważny inne państwa członkowskie Unii

Europejskiej, których dotyczy ten incydent, za pośrednictwem Pojedynczego Punktu Kontaktowego.

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

3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić z wnioskiem do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego, o którym mowa w ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich Unii Europejskiej, których dotyczy ten incydent.

Art. 29. (uchylony)

Art. 30. 1. Podmioty inne niż podmioty kluczowe lub podmioty ważne, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK. W zgłoszeniu należy podać:

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

2. Zgłoszenia incydentów od podmiotów kluczowych lub podmiotów ważnych są traktowane priorytetowo względem zgłoszeń, o których mowa w ust. 1.

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

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

Art. 31. 1. CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe określą sposób przekazywania informacji i zgłoszeń, o których mowa w art. 11 i art. 13, w przypadku braku możliwości przekazania ich za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.

2. CSIRT NASK określi sposób dokonywania zgłoszeń, o których mowa w art. 30 ust. 1.

3. Komunikat zawierający informacje o sposobie dokonywania zgłoszeń, o których mowa odpowiednio w art. 11, art. 13 i art. 30 ust. 1, CSIRT MON, CSIRT NASK, CSIRT GOV oraz CSIRT sektorowe publikują odpowiednio na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa.

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

2. CSIRT MON, CSIRT NASK lub CSIRT GOV mogą wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego lub krytycznego.

3. Podmiot kluczowy lub podmiot ważny na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV udostępnia informacje techniczne związane z incydentem, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi incydentu.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowe na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od podmiotu kluczowego lub podmiotu ważnego, mogą przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.

Art. 33. 1. CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie produktu ICT lub usługi ICT w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa.

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 CSIRT.

1b. Badanie, o którym mowa w ust. 1, przeprowadza się w środowisku testowym i nie może ono wpłynąć na ciągłość świadczenia usług przez podmioty kluczowe lub podmioty ważne.

1c. CSIRT MON, CSIRT NASK i CSIRT GOV, prowadząc badanie, o którym mowa w ust. 1, są uprawnieni do stosowania technik mających na celu:

1) obserwację i analizę pracy produktu ICT lub usługi ICT;
2) uzyskanie dostępu do przetwarzanych danych;
3) odtworzenie postaci źródłowej produktu ICT lub usługi ICT;
4) zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy;
5) odtworzenie algorytmu przetwarzania danych;
6) identyfikację realizowanych funkcji;
7) usunięcie lub przełamanie zabezpieczeń przed badaniem;
8) identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT lub usługę ICT.

1d. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, o którym mowa w ust. 1, nie są związane postanowieniami umów, w szczególności umów licencyjnych, badanych produktów ICT lub usług ICT, które ograniczyłyby możliwość przeprowadzenia tego badania.

1e. Badanie, o którym mowa w ust. 1:

1) nie narusza autorskich praw osobistych oraz majątkowych, oraz
2) nie wymaga zgody licencjodawcy lub dysponenta produktu ICT lub usługi ICT.

1f. Postanowienia umów sprzeczne z ust. 1–1e są nieważne.

2. CSIRT MON, CSIRT NASK albo CSIRT GOV, podejmując badanie produktu ICT, usługi ICT lub procesu ICT, informuje pozostałe CSIRT poziomu krajowego o fakcie podjęcia badań oraz o produkcie ICT lub usłudze ICT, których badanie dotyczy.

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

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

4a. W przypadku uzyskania przez Pełnomocnika informacji o cyberzagrożeniu, która uprawdopodobni możliwość wystąpienia incydentu krytycznego, Pełnomocnik może wydać rekomendacje, o których mowa w ust. 4, z urzędu.

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

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

5. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do rekomendacji dotyczących stosowania produktów ICT lub usług ICT, z uwagi na ich negatywny wpływ na świadczoną usługę lub realizowane zadanie publiczne, niepóźniej niż w terminie 14 dni od dnia publikacji rekomendacji na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

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

7. Podmiot krajowego systemu cyberbezpieczeństwa informuje Pełnomocnika, na jego wniosek, o sposobie i zakresie uwzględnienia rekomendacji dotyczących stosowania produktów ICT lub usług ICT.

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

9. CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzający badanie mogą zwrócić się do producenta badanego produktu ICT lub dostawcy badanej usługi ICT o przekazanie dokumentacji. Przepisy art. 53c stosuje się odpowiednio. O zwróceniu się do producenta, jak również o nieprzekazaniu przez producenta dokumentacji w terminie, CSIRT przeprowadzający badanie informuje ministra właściwego do spraw informatyzacji.

Art. 34. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań.

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

3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe oraz dostawcy usług zarządzanych z zakresu cyberbezpieczeństwa współpracują z Prezesem Urzędu Lotnictwa Cywilnego, Prezesem Urzędu Komunikacji Elektronicznej oraz Komisją Nadzoru Finansowego.

4. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe współpracują z Narodowym Bankiem Polskim w zakresie wymiany informacji o incydentach, podatnościach i cyberzagrożeniach, które mają wpływ na systemy płatności.

Art. 35. 1. CSIRT MON, CSIRT NASK i CSIRT GOV przekazują sobie wzajemnie informacje o incydencie krytycznym lub incydencie w cyberbezpieczeństwie na dużą skalę oraz informują o nim Rządowe Centrum Bezpieczeństwa, właściwy CSIRT sektorowy oraz ministra właściwego do spraw zagranicznych.

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

1) wstępną analizę potencjalnych skutków incydentu, z uwzględnieniem w szczególności:
   a) liczby użytkowników, których dotyczy incydent,
   b) momentu wystąpienia i wykrycia incydentu oraz czasu jego trwania,

c) zasięgu geograficznego obszaru, którego dotyczy incydent;

2) rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

2a. Informacja, o której mowa w ust. 1, może zawierać dane osobowe tylko wtedy, gdy jest to niezbędne dla ochrony podmiotów krajowego systemu cyberbezpieczeństwa przed incydentami.

3. Informacja, o której mowa w ust. 1, może zawierać wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych, zwanego dalej „Zespołem”.

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

5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą publikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje, w niezbędnym zakresie, o podatnościach, incydentach krytycznych oraz o cyberzagrożeniach, o ile przekazywanie informacji przyczyni się do zwiększenia bezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów. Publikowane informacje nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.

Art. 35a. W przypadku wystąpienia incydentu krytycznego Prezes Rady Ministrów może, na podstawie propozycji Rządowego Zespołu Zarządzania Kryzysowego, o której mowa w art. 9 ust. 1 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2023 r. poz. 122, z późn. zm.[12)]), zobowiązać Ministra Obrony Narodowej do udzielenia wsparcia CSIRT

[12)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 834, 1222, 1473, 1572 i 1907 oraz z 2025 r. poz. 1795.

koordynującemu obsługę tego incydentu przez właściwe jednostki organizacyjne podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.

Art. 36. 1. Zespół jest organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa.

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

3. Pełnomocnik przewodniczy pracom Zespołu.

4. Obsługę prac Zespołu zapewnia urząd obsługujący Pełnomocnika.

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

6. W przypadku, o którym mowa w art. 35 ust. 3, albo na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 1, Pełnomocnik zawiadamia niezwłocznie członków Zespołu o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej.

7. Zespół na posiedzeniu:

1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 1;
2) określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 1;
3) określa sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV;

4) podejmuje decyzję o wystąpieniu przez dyrektora Rządowego Centrum Bezpieczeństwa z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego;
5) w przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego.

Rozdział 6a

Ocena bezpieczeństwa

Art. 36a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy 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. Wyboru rodzaju testów bezpieczeństwa dokonuje się adekwatnie do systemu informacyjnego i świadczonej usługi z uwzględnieniem specyfiki sektora lub podsektora.

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, o których mowa w art. 32a ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;
2) akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2025 r. poz. 1209).

4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest:

1) w przypadku podmiotów, o których mowa w art. 26 ust. 5 – CSIRT MON;

2) w przypadku podmiotów, o których mowa w art. 26 ust. 6 pkt 1 lit. a–k – CSIRT NASK;
3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4d – CSIRT GOV.

5. CSIRT MON, CSIRT NASK albo CSIRT GOV przeprowadza ocenę bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa, po poinformowaniu organu właściwego do spraw cyberbezpieczeństwa o zamiarze przeprowadzenia oceny bezpieczeństwa.

6. CSIRT sektorowy może przeprowadzić ocenę bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego po uzyskaniu zgody CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla danego podmiotu kluczowego lub podmiotu ważnego. O zamiarze przeprowadzenia oceny bezpieczeństwa systemu informacyjnego podmiotu krajowego systemu cyberbezpieczeństwa CSIRT sektorowy informuje organ właściwy do spraw cyberbezpieczeństwa dla danego sektora.

7. Przepisów ust. 5 i 6 nie stosuje się, gdy ocena bezpieczeństwa systemu informacyjnego jest przeprowadzana na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

Art. 36b. 1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona:

1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo
2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

2. Ocenę bezpieczeństwa systemów informacyjnych Kancelarii Sejmu, Kancelarii Senatu, Kancelarii Prezydenta Rzeczypospolitej Polskiej, Narodowego Banku Polskiego, Biura Rzecznika Praw Obywatelskich, Biura Rzecznika Praw Dziecka, Instytutu Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu, Państwowej Inspekcji Pracy, Trybunału Konstytucyjnego, Sądu Najwyższego, sądów administracyjnych, Najwyższej Izby Kontroli, Krajowej Rady Radiofonii i Telewizji, Krajowego Biura Wyborczego, Urzędu Ochrony Danych Osobowych przeprowadza się wyłącznie po uzyskaniu zgody tych podmiotów.

3. Organ właściwy do spraw cyberbezpieczeństwa przed zleceniem przeprowadzenia oceny bezpieczeństwa przeprowadza analizę ryzyka, o której mowa w art. 53b ust. 2, i na jej podstawie dokonuje wyboru podmiotu kluczowego lub podmiotu ważnego, którego system informacyjny będzie podlegał ocenie bezpieczeństwa.

4. Ocenę bezpieczeństwa systemu informacyjnego przeprowadza się z uwzględnieniem zasady minimalizacji zakłócenia pracy systemu informacyjnego lub ograniczenia jego dostępności i nie może prowadzić ona do nieodwracalnego zniszczenia danych przetwarzanych w systemie informacyjnym podlegającym tej ocenie.

5. Ocena bezpieczeństwa nie może być przeprowadzona, a rozpoczętą przerywa się, jeżeli:

1) podmiot krajowego systemu cyberbezpieczeństwa nie posiada kopii bezpieczeństwa badanego systemu;
2) istnieje zagrożenie nieodwracalnego zniszczenia danych przetwarzanych w systemie;
3) czas potrzebny na przywrócenie systemu z kopii bezpieczeństwa może w istotny sposób zakłócić pracę systemu lub ograniczyć jego dostępność;
4) czynności podejmowane podczas oceny bezpieczeństwa mogą doprowadzić do uszkodzenia produktów ICT wchodzących w skład tego systemu oraz innych systemów informacyjnych podmiotu kluczowego;
5) istnieje zagrożenie ograniczenia dostępności usług świadczonych przez podmiot krajowego systemu cyberbezpieczeństwa.

6. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy uzgadnia z podmiotem krajowego systemu cyberbezpieczeństwa, w drodze porozumienia, tryb i ramowe warunki przeprowadzania tej oceny, w szczególności datę rozpoczęcia, harmonogram oraz zakres i rodzaj przeprowadzanych w ramach oceny bezpieczeństwa testów bezpieczeństwa.

7. Podmiot krajowego systemu cyberbezpieczeństwa, którego system informacyjny podlega ocenie bezpieczeństwa, przekazuje CSIRT przeprowadzającemu ocenę niezbędne informacje techniczne i organizacyjne niezbędne do przeprowadzenia oceny bezpieczeństwa oraz wskazuje imię i

nazwisko, adres służbowej poczty elektronicznej oraz numer telefonu służbowego osoby upoważnionej do reprezentacji podmiotu, a także osoby upoważnionej do udzielania wyjaśnień CSIRT w trakcie przeprowadzania oceny bezpieczeństwa.

8. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą wytwarzać lub pozyskiwać urządzenia lub programy komputerowe, o których mowa w art. 269b ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, 1818 i 1872), oraz ich używać w celu określenia podatności ocenianego systemu informacyjnego 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 § 1 i 2 albo art. 269a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny.

9. Używając urządzeń lub programów komputerowych, o których mowa w ust. 8, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy mogą uzyskać dostęp do informacji dla nich nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenie, lub mogą uzyskać dostęp do całości lub części tego systemu informacyjnego.

10. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy w wyniku przeprowadzania oceny bezpieczeństwa systemu informacyjnego stanowią tajemnicę prawnie chronioną i nie mogą być wykorzystane do realizacji innych zadań ustawowych CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego.

11. Materiały zawierające informacje, o których mowa w ust. 10, podlegają niezwłocznemu, trwałemu i nieodwracalnemu, protokolarnemu zniszczeniu, którego dokonuje komisja. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego.

12. Komisja, o której mowa w ust. 11 zdanie pierwsze, składa się z trzech osób powołanych przez osobę kierującą zespołem CSIRT spośród pracowników, funkcjonariuszy lub żołnierzy realizujących zadania odpowiednio w CSIRT MON, CSIRT NASK, CSIRT GOV albo CSIRT sektorowym.

13. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy sporządzają i przekazują podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport zawierający podsumowanie przeprowadzonych w ramach oceny bezpieczeństwa

czynności oraz wskazanie wykrytych podatności systemu informacyjnego. Jeżeli ocenę bezpieczeństwa przeprowadza CSIRT sektorowy, to raport przekazywany jest do właściwego CSIRT MON, CSIRT NASK albo CSIRT GOV.

Art. 36c. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy informują niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych.

Art. 36d. Rada Ministrów określi, w drodze rozporządzenia:

1) tryb przeprowadzania oceny bezpieczeństwa, o której mowa w art. 36a,
2) szczegółowe informacje przekazywane do CSIRT niezbędne do przeprowadzenia oceny bezpieczeństwa,
3) rodzaje przeprowadzanych testów bezpieczeństwa w ramach oceny bezpieczeństwa, o których mowa w art. 36a ust. 2,
4) sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10,
5) tryb działania komisji, o której mowa w art. 36b ust. 11 zdanie pierwsze,
6) wzór protokołu zniszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 10

– mając na uwadze konieczność zapewnienia sprawnego przeprowadzenia oceny bezpieczeństwa, bezpieczeństwo systemów informacyjnych podlegających ocenie, rodzaj materiałów podlegających zniszczeniu i konieczność zapewnienia efektywności i przejrzystości prowadzonych działań komisji.

Rozdział 7

Zasady udostępniania informacji i przetwarzania danych osobowych

Art. 37. 1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się przepisów:

1) ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej;
2) ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, z wyjątkiem informacji,

których udostępnienie nie zagrażałoby bezpieczeństwu państwa lub bezpieczeństwu publicznemu.

2. Właściwy CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowy mogą, po konsultacji ze zgłaszającym podmiotem kluczowym lub podmiotem ważnym, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego, Agencji Bezpieczeństwa Wewnętrznego lub organu właściwego do spraw cyberbezpieczeństwa informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu.

3. (uchylony)

4. Opublikowanie informacji, o których mowa w ust. 2, nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych ani przepisów o ochronie danych osobowych.

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

Art. 39. 1. W celu realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane pozyskane w związku z incydentami i cyberzagrożeniami, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.[13)]), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i w celu niezbędnym do realizacji tych zadań.

[13)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 127 z 23.05.2018, str. 1 oraz Dz. Urz. UE L 74 z 04.03.2021, str. 35.

2. CSIRT MON, CSIRT NASK i CSIRT sektorowe, przetwarzając dane osobowe określone w art. 9 ust. 1 art. 10 rozporządzenia 2016/679, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem oraz mechanizmy kontroli dostępu, a także opracowują procedury bezpiecznej wymiany informacji.

3. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowe przetwarzają dane osobowe pozyskane w związku z incydentami i cyberzagrożeniami:

1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych;
2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu art. 2 pkt 71 ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej;
3) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług;
4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

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

1) gromadzone przez podmioty kluczowe lub podmioty ważne w związku ze świadczeniem usług;
2) (uchylony)
3) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.

4a. Minister właściwy do spraw informatyzacji przetwarza dane osobowe zawierające imię i nazwisko oraz numer PESEL osób fizycznych lub niepowtarzalny identyfikator środka identyfikacji elektronicznej, o którym mowa w aktach wykonawczych Komisji Europejskiej, wydanych na podstawie art. 12 ust. 8 rozporządzenia 910/2014, które w imieniu podmiotu kluczowego lub podmiotu ważnego korzystają z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu ich uwierzytelnienia w tym systemie.

5. Dane, o których mowa w ust. 3 i 4, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy niezwłocznie po stwierdzeniu, że nie są

niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3.

6. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadań, o których mowa w art. 26 ust. 3 pkt 1–11, 14 i 16–21 i ust. 5–8, art. 26a–26c oraz art. 44 ust. 1–1c i 3, są anonimizowane przez CSIRT MON, CSIRT NASK i CSIRT sektorowy po upływie 5 lat od zakończenia obsługi incydentu, którego dotyczą, z uwzględnieniem ust. 6a.

6a. Dane, o których mowa w ust. 3 i 4, niezbędne do realizacji zadania, o którym mowa w art. 26a, są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania.

6b. Dane, o których mowa w art. 26c ust. 2, są anonimizowane przez CSIRT NASK po upływie 5 lat od dnia ich pozyskania.

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

8. Realizacja obowiązków wynikających z art. 15, art. 16, art. 18 ust. 1 lit. a i d oraz art. 19 zdanie drugie rozporządzenia 2016/679 przez CSIRT MON, CSIRT NASK i CSIRT sektorowe, w zakresie danych, o których mowa w ust. 3, jest możliwa dopiero po zakończeniu obsługi incydentu, w związku z którym dane zostały pozyskane, lub po zakończeniu obsługi incydentu, do którego obsługi te dane są niezbędne.

9. CSIRT MON, CSIRT NASK i CSIRT sektorowe publikują na swoich stronach internetowych:

1) dane kontaktowe administratora danych osobowych oraz, gdy ma to zastosowanie, dane kontaktowe inspektora ochrony danych osobowych;
2) cele przetwarzania i podstawę prawną przetwarzania;
3) kategorie przetwarzanych danych osobowych;
4) informacje o odbiorcach danych osobowych;
5) informacje o tym, przez jaki okres dane osobowe będą przechowywane;
6) informacje o ograniczeniach obowiązków i praw osób, których dane dotyczą;
7) informacje o prawie wniesienia skargi do organu właściwego do spraw ochrony danych osobowych;

8) źródło pochodzenia danych osobowych.

10. Dane, o których mowa w ust. 4, są anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika, ministra właściwego do spraw zagranicznych oraz organy właściwe do spraw cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z ustawy, niepóźniej niż po 5 latach po ich uzyskaniu.

11. Minister właściwy do spraw informatyzacji przetwarza dane osobowe, w tym dane, o których mowa w art. 9 ust. 1 rozporządzenia 2016/679, które zostały zawarte w stanowiskach zgłoszonych w ramach konsultacji publicznych projektu dokumentu, o którym mowa w art. 45 ust. 3.

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

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

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

Art. 40a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i organy właściwe do spraw cyberbezpieczeństwa mogą, w porozumieniu z Pełnomocnikiem, uczestniczyć w procesie oceny wzajemnej, w celu wymiany doświadczeń, zwiększania wzajemnego zaufania pomiędzy organami z różnych państw, osiągnięcia wysokiego, wspólnego poziomu cyberbezpieczeństwa, a także zwiększenia kluczowych zdolności państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa i doskonalenia ich polityki w tej dziedzinie.

2. Ocena wzajemna jest przeprowadzana przez ekspertów do spraw cyberbezpieczeństwa wyznaczonych na podstawie metodyki obejmującej

obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria jako uprawnionych do prowadzenia ocen wzajemnych.

3. Ocena wzajemna może obejmować:

1) stopień wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz obowiązków dotyczących zgłaszania incydentów;
2) poziom zdolności, w tym dostępne zasoby finansowe, techniczne i ludzkie, oraz skuteczność wykonywania zadań przez właściwe organy;
3) zdolność operacyjną CSIRT;
4) poziom wdrożenia wzajemnej pomocy;
5) poziom wdrożenia ustaleń dotyczących mechanizmów wymiany informacji na temat cyberbezpieczeństwa;
6) szczególne zagadnienia transgraniczne lub międzysektorowe.

4. W ramach procesu oceny wzajemnej podmioty, o których mowa w ust. 1, mogą przekazywać wyznaczonym przez inne państwa członkowskie Unii Europejskiej ekspertom do spraw cyberbezpieczeństwa informacje dotyczące funkcjonowania tych podmiotów, z uwzględnieniem przepisów o tajemnicach prawnie chronionych.

5. Pełnomocnik może wskazać innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej szczególne zagadnienia transgraniczne lub międzysektorowe, które należy uwzględnić w ocenie wzajemnej.

6. Pełnomocnik informuje inne państwa członkowskie Unii Europejskiej uczestniczące w ocenie wzajemnej o zakresie oceny wzajemnej przeprowadzanej w Rzeczypospolitej Polskiej.

7. W porozumieniu z Pełnomocnikiem podmioty, o których mowa w ust. 1, mogą przeprowadzić ocenę, o której mowa w ust. 3, dotyczącą krajowego systemu cyberbezpieczeństwa i przedstawić jej wyniki ekspertom z innych państw uczestniczących w ocenie wzajemnej. Ocenę tę przeprowadza się zgodnie z metodyką przyjętą przez Grupę Współpracy.

8. Oceny wzajemnej nie przeprowadza się w terminie 2 lat od sporządzenia sprawozdania z poprzedniej oceny wzajemnej, jeżeli dotyczy tego samego zakresu. Ocena wzajemna dotycząca tego samego zakresu może być przeprowadzona, jeżeli Pełnomocnik zwróci się o to do innego państwa członkowskiego Unii Europejskiej

lub państwa członkowskie Unii Europejskiej uzgodnią to w ramach Grupy Współpracy.

9. Pełnomocnik może sprzeciwić się przeprowadzeniu oceny wzajemnej przez konkretnych ekspertów z innego państwa członkowskiego Unii Europejskiej, jeżeli występuje konflikt interesów.

10. Eksperci do spraw cyberbezpieczeństwa, wyznaczeni przez podmioty, o których mowa w ust. 1, uczestniczący w ocenie wzajemnej sporządzają sprawozdanie z oceny wzajemnej, które zatwierdza Pełnomocnik. Sprawozdanie zawiera podsumowanie czynności podjętych w ramach oceny wzajemnej oraz zalecenia. Sprawozdanie udostępnia się innym państwom członkowskim Unii Europejskiej uczestniczącym w ocenie wzajemnej oraz organom właściwym do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV.

11. Pełnomocnik może udostępnić sprawozdanie Grupie Współpracy lub Sieci CSIRT. Sprawozdanie to może zostać opublikowane w Biuletynie Informacji Publicznej Pełnomocnika w zakresie, w jakim nie zawiera informacji stanowiących tajemnice prawnie chronione.

Rozdział 8

Organy właściwe do spraw cyberbezpieczeństwa

Art. 41. Organami właściwymi do spraw cyberbezpieczeństwa są:

1) dla sektora energii – minister właściwy do spraw energii;
1a) dla sektora inwestycji energii jądrowej – minister właściwy do spraw energii;
2) dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu;
3) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej;
4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego;
5) dla sektora ochrony zdrowia z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1 – minister właściwy do spraw zdrowia;
6) dla sektora ochrony zdrowia obejmującego podmioty, o których mowa w art. 26 ust. 5 pkt 1 – Minister Obrony Narodowej;

7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej;
8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1, oraz z wyłączeniem podsektora komunikacji elektronicznej – minister właściwy do spraw informatyzacji;
8a) dla podsektora komunikacji elektronicznej, z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1 – Prezes Urzędu Komunikacji Elektronicznej;
9) dla sektora infrastruktury cyfrowej obejmującego podmioty, o których mowa w art. 26 ust. 5 pkt 1 – Minister Obrony Narodowej;
9a) dla sektora zbiorowego odprowadzania ścieków – minister właściwy do spraw gospodarki wodnej;
9b) dla sektora zarządzania usług ICT – minister właściwy do spraw informatyzacji;
9c) dla sektora przestrzeni kosmicznej – minister właściwy do spraw gospodarki;
9d) dla sektora produkcji, wytwarzania i dystrybucji chemikaliów – minister właściwy do spraw gospodarki;
9e) dla sektora produkcji, przetwarzania i dystrybucji żywności – minister właściwy do spraw rolnictwa;
9f) dla sektora produkcji, z wyłączeniem podsektora produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw gospodarki;
9g) dla podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro – minister właściwy do spraw zdrowia;
9h) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;
9i) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu;
9j) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyzacji;
9k) dla sektora badań naukowych, z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 pkt 1 – minister właściwy do spraw szkolnictwa wyższego i nauki;
9l) dla sektora badań naukowych obejmującego podmioty, o których mowa w art. 26 ust. 5 pkt 1 – Minister Obrony Narodowej.

10) (uchylony)

11) (uchylony)

Art. 41a. 1. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych, z wyłączeniem podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz urzędu obsługującego tego ministra, jest minister właściwy do spraw informatyzacji.

2. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych oraz dla urzędu obsługującego tego ministra jest Minister Obrony Narodowej.

3. Organem właściwym do spraw cyberbezpieczeństwa w sektorze podmiotów publicznych dla jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych lub przez niego nadzorowanych, urzędu obsługującego tego ministra oraz spółki, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji rządowej budżet i finanse publiczne (Dz. U. z 2025 r. poz. 1642), jest minister właściwy do spraw finansów publicznych.

4. Dla podmiotu publicznego, który jest wymieniony w innym sektorze niż sektor podmiotów publicznych, organem właściwym do spraw cyberbezpieczeństwa jest organ właściwy dla danego sektora. Przepis nie dotyczy samorządowych podmiotów publicznych.

5. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze podmiotów publicznych CSIRT NASK, z wyjątkiem wydawania decyzji administracyjnych. Zadania te są finansowane w ramach dotacji, o której mowa w art. 26 ust. 9. Przepisów art. 42 ust. 3–6 nie stosuje się w tym zakresie.

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

1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za podmiot kluczowy lub podmiot ważny;

2) wpisuje z urzędu podmiot kluczowy lub podmiot ważny do wykazu, jeżeli podmiot ten nie zarejestrował się w tym wykazie;

3) wydaje decyzję o uznaniu podmiotu za podmiot kluczowy lub podmiot ważny, o której mowa w art. 7l ust. 1;
4) (uchylony)
5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i CSIRT sektorowymi rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
6) monitoruje stosowanie przepisów ustawy przez podmioty kluczowe lub podmioty ważne;
7) wzywa na wniosek CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego podmioty kluczowe lub podmioty ważne do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego lub krytycznego;
8) prowadzi kontrole podmiotów kluczowych lub podmiotów ważnych;
9) może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;
10) przetwarza informacje, w tym dane osobowe, dotyczące podmiotów kluczowych lub podmiotów ważnych oraz świadczonych przez nich usług, w zakresie niezbędnym do:
    a) identyfikacji podmiotów kluczowych lub podmiotów ważnych,
    b) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi lub podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa,
    c) prowadzenia czynności nadzorczych nad podmiotami kluczowymi lub podmiotami ważnymi;
11) uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej;
12) współpracuje oraz wymienia informacje i dokumenty z właściwym organem w rozumieniu rozporządzenia 2022/2554, w zakresie niezbędnym do wykonywania przez ten organ obowiązków wynikających z rozporządzenia 2022/2554;

13) współpracuje oraz wymienia informacje i dokumenty z organem właściwym do spraw podmiotów krytycznych w zakresie nadzoru nad podmiotem kluczowym będącym podmiotem krytycznym.

2. (uchylony)

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

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

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

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

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

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

8. Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów, o których mowa w ust. 1 pkt 5, przygotowuje się z uwzględnieniem w szczególności Polskich Norm przenoszących normy europejskie, wspólnych specyfikacji technicznych, rozumianych jako specyfikacje techniczne w dziedzinie produktów teleinformatycznych określone zgodnie z art. 13 i art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającego dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz.

Urz. UE L 316 z 14.11.2012, str. 12) oraz wytycznych Komisji Europejskiej oraz ENISA w tym zakresie.

9. Organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych realizuje swoje zadania, z uwzględnieniem zakresu zastosowania ustawy do podmiotów finansowych.

10. W ramach współpracy, o której mowa w ust. 1 pkt 12, mającej związek z podmiotem kluczowym lub podmiotem ważnym, który zgodnie z rozporządzeniem 2022/2554 został wyznaczony jako kluczowy zewnętrzny dostawca usług ICT, organ właściwy do spraw cyberbezpieczeństwa w szczególności udziela informacji oraz istotnych zaleceń technicznych i pomocy technicznej, a także umożliwia skuteczną i szybką koordynację działań nadzorczych, w tym na potrzeby prowadzenia kontroli.

11. Organ właściwy do spraw cyberbezpieczeństwa prowadzi i regularnie aktualizuje wykaz osób, wobec których wydana została decyzja o zastosowaniu środka nadzorczego, o którym mowa w art. 53 ust. 9 pkt 6, obejmujący:

1) imię (imiona);
2) nazwisko;
3) numer PESEL, a w przypadku jego nieposiadania – datę urodzenia;
4) nazwę podmiotu kluczowego;
5) datę wydania decyzji;
6) znak sprawy;
7) okres obowiązywania zakazu;
8) podstawę prawną wydania decyzji.

Art. 43. 1. Organ właściwy do spraw cyberbezpieczeństwa może, bez wszczynania postępowania, o którym mowa w art. 7j lub art. 7l, wystąpić do podmiotu, o którym mowa w załączniku nr 1 lub 2 do ustawy, o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot kluczowy lub podmiot ważny. Przepisy art. 53c ust. 2 i 3 stosuje się odpowiednio.

2. (uchylony)

3. (uchylony)

4. (uchylony)

5. (uchylony)

6. Informacje udzielone przez podmiot, o którym mowa w ust. 1, mogą stanowić podstawę do wpisania podmiotu do wykazu na podstawie art. 7j albo wydania decyzji, o której mowa w art. 7l.

Art. 44. 1. Organ właściwy do spraw cyberbezpieczeństwa zapewnia funkcjonowanie CSIRT sektorowego dla podmiotów kluczowych lub podmiotów ważnych w danym sektorze lub podsektorze wymienionych w załączniku nr 1 i 2 do ustawy, do którego zadań należy:

1) przyjmowanie wczesnych ostrzeżeń, zgłoszeń o incydentach, sprawozdań okresowych i sprawozdań końcowych, o których mowa w art. 11 ust. 1 pkt 4–4c;
2) przyjmowanie zgłoszeń o potencjalnych zdarzeniach dla cyberbezpieczeństwa;
3) reagowanie na incydenty;
4) gromadzenie informacji o podatnościach i cyberzagrożeniach;
5) współpraca z podmiotem kluczowym lub podmiotem ważnym w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
6) 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;
7) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.

1a. CSIRT sektorowy przekazuje, za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, wczesne ostrzeżenie, zgłoszenie incydentu, sprawozdanie okresowe i sprawozdanie końcowe, o których mowa w art. 11 ust. 1 pkt 4–4c, niezwłocznie, niepóźniej niż 8 godzin od jego otrzymania, do właściwego CSIRT MON, 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 podmiotów kluczowych lub podmiotów ważnych danego sektora lub podsektora;

2) wykonywać niezbędne działania techniczne związane z analizą cyberzagrożeń oraz reagowaniem na incydent poważny;

3) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z podmiotami kluczowymi lub podmiotami ważnymi obsługę incydentów, które ich dotyczą;

4) wspierać, w uzgodnieniu z podmiotem kluczowym lub podmiotem ważnym, wykonywanie przez niego obowiązków określonych w art. 11, art. 12–12b i art. 13;

5) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego lub podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego;

6) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów kluczowych lub podmiotów ważnych 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;

7) na wniosek podmiotu kluczowego lub podmiotu ważnego wspierać dany podmiot w zakresie monitorowania ich sieci i systemów informatycznych w czasie rzeczywistym lub zbliżonym do rzeczywistego.

1c. CSIRT sektorowy, który otrzymał zgłoszenie incydentu, a nie jest właściwy do jego przyjęcia, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami.

1d. CSIRT sektorowy informuje o złożeniu wniosku, o którym mowa w ust. 1b pkt 5, właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV.

2. (uchylony)

3. CSIRT sektorowy może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego Unii Europejskiej dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. CSIRT sektorowy

przekazuje te zgłoszenia do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz Pojedynczego Punktu Kontaktowego.

4. Organ właściwy do spraw cyberbezpieczeństwa informuje podmioty kluczowe lub podmioty ważne w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu CSIRT sektorowego i zakresie realizowanych zadań.

5. Przepisy ust. 1–1d, 3 i 4 stosuje się odpowiednio do CSIRT sektorowego ustanowionego w sektorze bankowości i infrastruktury rynków finansowych, w szczególności w zakresie poważnych incydentów związanych z ICT zgłaszanych przez podmioty kluczowe lub podmioty ważne.

6. CSIRT sektorowy ustanowiony w sektorze bankowości i infrastruktury rynków finansowych może również realizować swoje zadania w odniesieniu do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, w szczególności w zakresie wsparcia w obsłudze poważnych incydentów związanych z ICT, gdy nie stanowi to dla niego nieproporcjonalnego czy nadmiernego obciążenia, z uwzględnieniem priorytetowego traktowania poważnych incydentów związanych z ICT zgłaszanych przez podmioty finansowe będące podmiotami kluczowymi lub podmiotami ważnymi oraz odpowiedniego stosowania przepisów ust. 1–1d, 3 i 4 do realizacji zadań.

Art. 44a. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego:

1) jednostce jemu podległej lub przez niego nadzorowanej;
2) organowi przez niego nadzorowanemu;
3) urzędowi, który go obsługuje.

2. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania albo zadań CSIRT sektorowego państwowej osobie prawnej, o której mowa w art. 3 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym, jeżeli dysponuje ona zdolnościami technicznymi i organizacyjnymi niezbędnymi do wypełniania zadań CSIRT sektorowego w danym sektorze lub podsektorze.

3. Organy właściwe do spraw cyberbezpieczeństwa mogą, w drodze porozumienia, powierzyć realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, dla których są właściwe, jednostce podległej

jednemu z tych organów albo nadzorowanej przez jeden z tych organów. Stroną tego porozumienia jest również jednostka, której powierzono zadania.

4. Organy właściwe do spraw cyberbezpieczeństwa określają w porozumieniu, o którym mowa w ust. 3, w szczególności zakres powierzonych zadań, weryfikację prawidłowości ich wykonania oraz sposób finansowania powierzonych zadań.

Art. 44b. 1. Minister będący organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów może powierzyć jednostce jemu podległej albo nadzorowanej przez niego zadanie lub zadania CSIRT sektorowego.

2. Powierzenie odbywa się w drodze decyzji, do której nie stosuje się przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Komunikat o powierzeniu przez ministra będącego organem właściwym do spraw cyberbezpieczeństwa dla kilku sektorów lub podsektorów zadania lub zadań CSIRT sektorowego jednostce podległej albo nadzorowanej przez tego ministra ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa.

4. Ministrowie, którzy przejęli właściwość nadzorczą nad sektorami, dla których dotychczasowy minister wyznaczył wspólny CSIRT sektorowy, zawierają porozumienie, w którym wyznaczą jednostkę, która przejmie zadania CSIRT sektorowego dla poszczególnych sektorów lub podsektorów. Do czasu zawarcia porozumienia decyzja, o której mowa w ust. 2, zachowuje moc.

Art. 44c. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć CSIRT MON, CSIRT NASK albo CSIRT GOV realizację zadania albo zadań CSIRT sektorowego.

2. Powierzenie, o którym mowa w ust. 1, 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 – Państwowego Instytutu Badawczego;

2) w przypadku powierzenia zadań CSIRT GOV – z Szefem Agencji Bezpieczeństwa Wewnętrznego;
3) w przypadku powierzenia zadań CSIRT MON – z Ministrem Obrony Narodowej.

3. Do porozumienia, o którym mowa w ust. 2, stosuje się przepis art. 44a ust. 4.

4. Minister Obrony Narodowej, jako organ właściwy do spraw cyberbezpieczeństwa, może powierzyć CSIRT MON realizację zadań CSIRT sektorowego w drodze decyzji niepodlegającej ogłoszeniu.

Art. 44d. 1. Zadania CSIRT sektorowego:
1) są finansowane z części budżetu państwa, której dysponentem jest minister albo centralny organ administracji rządowej, będący organem właściwym do spraw cyberbezpieczeństwa;
2) mogą być dofinansowywane:
   a) ze środków pochodzących z budżetu Unii Europejskiej,
   b) ze środków przeznaczonych na realizację programów finansowanych z udziałem środków pochodzących z budżetu Unii Europejskiej.

2. Jednostka, której powierzono zadania CSIRT sektorowego dla danego sektora lub podsektora, może otrzymać na realizację tych zadań dotację celową, z części budżetowej, której dysponentem jest minister będący organem właściwym do spraw cyberbezpieczeństwa dla danego sektora lub podsektora.

3. W przypadku gdy jednostce budżetowej powierzono realizację zadania lub zadań CSIRT sektorowego dla kilku sektorów lub podsektorów, otrzymuje ona środki z części budżetowych, których dysponentami są organy właściwe do spraw cyberbezpieczeństwa dla danego sektora lub podsektora, które zawarły porozumienie, o którym mowa w art. 44a ust. 3.

Art. 44e. 1. Komunikat o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2, ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa i 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.

2. Organ właściwy do spraw cyberbezpieczeństwa informuje Pełnomocnika o zawarciu porozumienia, o którym mowa w art. 44a ust. 3, art. 44b ust. 3 lub art. 44c ust. 2. Pełnomocnik publikuje komunikat o zawarciu porozumienia na swojej stronie podmiotowej Biuletynu Informacji Publicznej.

Art. 44f. Organ właściwy do spraw cyberbezpieczeństwa raz w roku, w terminie do dnia 31 stycznia, przedkłada Pełnomocnikowi sprawozdanie z funkcjonowania CSIRT sektorowego za rok poprzedni.

Rozdział 9

Zadania ministra właściwego do spraw informatyzacji

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

1) monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zwanej dalej „Strategią”, oraz realizację planów działań na rzecz jej wdrożenia;
1a) monitorowanie wdrażania Krajowego planu oraz realizację działań na rzecz jego wdrożenia;
1b) prowadzenie wykazu;
2) rekomendowanie obszarów współpracy z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa Rzeczypospolitej Polskiej;
3) opracowywanie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez podmioty kluczowe lub podmioty ważne mających wpływ na ciągłość świadczenia usług przez te podmioty w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług w państwach członkowskich Unii Europejskiej;
4) prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników;
5) gromadzenie informacji o incydentach poważnych, które dotyczą lub zostały przekazane przez inne państwo członkowskie Unii Europejskiej;

6) udostępnianie informacji i dobrych praktyk uzyskanych z Grupy Współpracy podmiotom krajowego systemu cyberbezpieczeństwa w celu usprawnienia działań krajowego systemu cyberbezpieczeństwa;
7) rekomendowanie i wspieranie przy wykorzystywaniu europejskich lub międzynarodowych standardów, a także specyfikacji technicznych mających znaczenie dla bezpieczeństwa systemów informacyjnych;
8) zachęcanie do korzystania z produktów ICT, usług ICT i procesów ICT certyfikowanych w ramach europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa;
9) ustanowienie odpowiednich struktur komunikacyjnych na potrzeby wczesnego wykrywania kryzysów w cyberbezpieczeństwie, reagowania kryzysowego w cyberbezpieczeństwie i zarządzania kryzysowego w cyberbezpieczeństwie, a także koordynacji współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu we współpracy z sektorem prywatnym;
10) współpracę w obszarze cyberbezpieczeństwa z państwami trzecimi;
11) koordynację działań organów państwa w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie niedotyczącej wymiaru militarnego;
12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa;
13) przekazywanie Komisji Europejskiej aktualnych informacji o organach właściwych do spraw cyberbezpieczeństwa oraz Pojedynczym Punkcie Kontaktowym, ich danych identyfikacyjnych oraz zadaniach;
14) przekazywanie Komisji Europejskiej aktualnych informacji o CSIRT MON, CSIRT NASK i CSIRT GOV oraz CSIRT sektorowych, wraz z ich danymi kontaktowymi oraz zadaniami;
15) udzielanie wsparcia finansowego na działania służące rozwojowi cyberbezpieczeństwa.

2. Przez Grupę Współpracy rozumie się grupę, o której mowa w art. 14 dyrektywy 2022/2555.

3. Minister właściwy do spraw informatyzacji może opublikować na swojej stronie podmiotowej Biuletynu Informacji Publicznej zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12

września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), których wykonywanie realizuje obowiązki wynikające z przepisów ustawy oraz z przepisów wydanych na podstawie art. 8a.

4. Projekt zestawienia, o którym mowa w ust. 3, minister właściwy do spraw informatyzacji kieruje do 30-dniowych konsultacji publicznych, z których sporządza raport, w którym wskazuje główne tezy zawarte w stanowiskach zgłoszonych do projektu zestawienia oraz odniesienie się do nich.

5. Projekt zestawienia, o którym mowa w ust. 3, uwagi zgłoszone w ramach konsultacji publicznych oraz raport ministra właściwego do spraw informatyzacji publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, z wyłączeniem danych osobowych osób fizycznych biorących udział w konsultacjach publicznych.

Art. 45a. 1. Minister właściwy do spraw informatyzacji może udzielić wsparcia finansowego w ramach programów rządowych lub innych programów finansowanych w całości albo w części z udziałem środków, o których mowa w art. 5 ust. 3 pkt 6 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, na realizację projektów, których celem jest:

1) tworzenie i rozwój produktów ICT, usług ICT oraz procesów ICT z zakresu cyberbezpieczeństwa;
2) rozwój kompetencji w obszarze cyberbezpieczeństwa;
3) zapewnianie cyberbezpieczeństwa w danej jednostce organizacyjnej;
4) promocja dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa;
5) wsparcie w obszarze standaryzacji i certyfikacji cyberbezpieczeństwa;
6) rozwój infrastruktury służącej zapewnianiu cyberbezpieczeństwa;
7) wsparcie badań naukowych, rozwoju technologicznego i projektów pilotażowych związanych z cyberbezpieczeństwem;
8) wsparcie w obsłudze incydentów;
9) identyfikacja i mitygacja podatności produktów ICT, usług ICT i procesów ICT;
10) zwiększenie rozpoznawalności produktów lub usług z zakresu cyberbezpieczeństwa;

11) inne działanie służące rozwojowi cyberbezpieczeństwa.

2. Wsparcie finansowe, o którym mowa w ust. 1, może być udzielane podmiotom publicznym, jak i prywatnym, i może stanowić:

1) pomoc publiczną dla podmiotów prywatnych;

2) pomoc *de minimis* dla podmiotów prywatnych;

3) dofinansowanie dla podmiotów publicznych.

3. Wsparcie finansowe, o którym mowa w ust. 1, jest udzielane podmiotom, które mają zdolność do realizacji projektu, o którym mowa w ust. 1.

4. Wsparcie finansowe, o którym mowa w ust. 1, może mieć charakter zwrotny albo bezzwrotny.

5. Wybór projektów, na które jest udzielane wsparcie finansowe, o którym mowa w ust. 1, następuje w trybie konkursowym albo pozakonkursowym.

6. Minister właściwy do spraw informatyzacji określi, odrębnie dla danego programu, o którym mowa w ust. 1, w drodze rozporządzenia, szczegółowe warunki, formę oraz tryb udzielania wsparcia finansowego, o którym mowa w ust. 1, a także podmioty go udzielające, uwzględniając konieczność realizacji celów określonych w tych programach, efektywność i skuteczność wykorzystania tego wsparcia oraz przejrzystość jego udzielania, a także zapewnienie jego zgodności z rynkiem wewnętrznym.

Art. 45b. Wsparcie finansowe, o którym mowa w art. 45a ust. 1, może być udzielane w imieniu ministra właściwego do spraw informatyzacji przez podmiot mu podległy albo przez niego nadzorowany.

Art. 45c. 1. Wyboru projektów dokonuje się w sposób przejrzysty, rzetelny i bezstronny na podstawie obiektywnych kryteriów oceny, biorąc pod uwagę w szczególności wpływ projektu na realizację celów określonych w art. 45a ust. 1 oraz na krajowy system cyberbezpieczeństwa.

2. Podstawę dofinansowania projektu stanowi umowa o dofinansowanie projektu zawarta z beneficjentem przez podmiot udzielający wsparcia finansowego, o którym mowa w art. 45a ust. 1.

3. Beneficjent może wykorzystywać otrzymane wsparcie tylko na wydatki służące realizacji celów wskazanych w art. 45a ust. 1.

4. Beneficjent jest obowiązany zwrócić wsparcie wykorzystane niezgodnie z ust. 3, w terminie niedłuższym niż 15 dni od określonego w umowie dnia wykonania zadania.

5. Beneficjent informuje podmiot udzielający wsparcia o postępach w realizacji projektu w terminach wskazanych w umowie, o której mowa w ust. 2.

6. Do umowy, o której mowa w ust. 2, stosuje się odpowiednio przepis art. 150 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.

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

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) zgłaszanie i obsługę incydentów;
4) szacowanie ryzyka na poziomie krajowym;
5) ostrzeganie o cyberzagrożeniach;
6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;
7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206), przez podmioty kluczowe lub podmioty ważne;
8) wymianę informacji o aktach ministra właściwego do spraw informatyzacji, Pełnomocnika, organów właściwych do spraw cyberbezpieczeństwa oraz Prezesa Rady Ministrów, o których mowa w art. 33 ust. 4, art. 42 ust. 1 pkt 5, art. 45 ust. 3, art. 67, art. 67a, art. 67b ust. 15, art. 67g ust. 1 i art. 67l ust. 1.

1a. W systemie teleinformatycznym prowadzi się wykaz.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezes Urzędu Ochrony Danych Osobowych korzystają z systemu teleinformatycznego w celu realizacji swoich zadań ustawowych.

3. (uchylony)

4. Podmioty kluczowe lub podmioty ważne, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, w terminie 12 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

5. Uwierzytelnienie w systemie teleinformatycznym następuje za pomocą środków określonych w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

6. W celu zapewnienia bezpiecznego korzystania z systemu teleinformatycznego podmioty kluczowe lub podmioty ważne są obowiązane zapewnić bezpieczeństwo, ciągłość działania, aktualność i skuteczność zabezpieczeń oraz rozliczalność stosowanych systemów teleinformatycznych.

7. W celu wykonania obowiązku, o którym mowa w ust. 6, podmioty kluczowe lub podmioty ważne dostosowują swoje systemy informacyjne do minimalnych wymagań technicznych i funkcjonalnych korzystania z systemu teleinformatycznego, opublikowanych przez ministra właściwego do spraw informatyzacji na jego stronie podmiotowej Biuletynu Informacji Publicznej w terminie 6 miesięcy od dnia opublikowania tych wymagań.

8. Minister właściwy do spraw informatyzacji publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej wykaz usług stosowany w systemie teleinformatycznym, w szczególności świadczonych przez podmioty kluczowe lub podmioty ważne.

9. CSIRT MON, CSIRT NASK, CSIRT GOV, po uzyskaniu zgody właściwego CSIRT poziomu krajowego, mogą uzyskać dostęp do wszelkich informacji przetwarzanych w systemie teleinformatycznym, w zakresie dotyczącym podmiotu będącego we właściwości innego CSIRT, w szczególności w celu szacowania ryzyka bezpieczeństwa łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi przez podmiot pozostający we właściwości danego CSIRT.

Art. 46a. W celu realizacji zadań, o których mowa w art. 11 ust. 2 oraz w art. 46 ust. 1 pkt 3, 4 i 6, Minister Obrony Narodowej, urząd go obsługujący oraz podmioty podległe Ministrowi Obrony Narodowej i przez niego nadzorowane mogą korzystać ze środków komunikacji elektronicznej, innych niż system, o którym mowa w art. 46 ust. 1, zapewniających poufność, integralność, dostępność i autentyczność przetwarzanych danych.

Art. 46b. 1. W przypadku doręczenia pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, przez organ administracji publicznej doręczenie jest skuteczne, jeżeli adresat potwierdzi odbiór pisma w systemie.

2. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, organ administracji publicznej po upływie 7 dni, licząc od dnia jego wysłania, przesyła zawiadomienie o możliwości odebrania tego pisma.

3. Zawiadomienie o możliwości odebrania pisma może być automatycznie tworzone i przesyłane za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, a odbioru tego zawiadomienia nie potwierdza się.

4. W przypadku nieodebrania pisma w postaci elektronicznej za pośrednictwem systemu, o którym mowa w art. 46 ust. 1, doręczenie uważa się za dokonane po upływie 14 dni, licząc od dnia wysłania pisma.

Art. 47. 1. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań, o których mowa w art. 45 ust. 1, art. 45a ust. 1 i art. 46 ust. 1 i 1a, jednostkom jemu podległym lub przez niego nadzorowanym.

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

3. Minister właściwy do spraw informatyzacji może udostępniać jednostkom, o których mowa w ust. 1, dane z wykazu w zakresie i w celu realizacji zadań im powierzonych, z uwzględnieniem poufności, integralności, dostępności i autentyczności tych danych.

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

1) odbieranie zgłoszeń incydentu dotyczącego więcej niż jednego sektora lub dotyczącego innych państw członkowskich Unii Europejskiej z Pojedynczych Punktów Kontaktowych w innych państwach członkowskich Unii Europejskiej, także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego;

2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu dotyczącego więcej niż jednego sektora lub innych państw członkowskich Unii Europejskiej do Pojedynczych Punktów Kontaktowych w innych państwach członkowskich Unii Europejskiej;
3) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy;
4) zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa;
5) koordynacja współpracy między organami właściwymi do spraw cyberbezpieczeństwa i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej;
6) zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT.

Art. 49. 1. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy:
1) informacje, o których mowa w art. 45 ust. 1 pkt 3;
2) dobre praktyki, o których mowa w art. 45 ust. 1 pkt 4, związane ze zgłaszaniem incydentów;
3) propozycje do programu prac Grupy Współpracy;
4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju z zakresu cyberbezpieczeństwa;
5) dobre praktyki w odniesieniu do identyfikowania podmiotów kluczowych lub podmiotów ważnych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów.

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

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

1) ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa oraz skuteczności CSIRT, a także dobrych praktyk w zakresie cyberbezpieczeństwa;
2) działań podjętych w odniesieniu do ćwiczeń dotyczących cyberbezpieczeństwa, europejskich programów edukacyjnych i szkoleń, w tym działań ENISA;
3) wytycznych o charakterze strategicznym dotyczących działalności Sieci CSIRT;
4) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów poważnych przez podmioty kluczowe lub podmioty ważne;
5) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących podnoszenia świadomości, szkolenia, zakresu badań i rozwoju w zakresie cyberbezpieczeństwa;
6) dobrych praktyk w zakresie identyfikowania podmiotów kluczowych lub podmiotów ważnych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.

4. Pojedynczy Punkt Kontaktowy przekazuje ENISA aktualne dane z wykazu dotyczące dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usługi centrum przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych.

5. Dane, o których mowa w ust. 4, obejmują:

1) nazwę (firmę) podmiotu;
2) sektor, podsektor i rodzaj podmiotu;
3) siedzibę i adres;
4) adres poczty elektronicznej;
5) numer telefonu przyporządkowany do wykonywanej działalności;
6) informację o wyznaczeniu przedstawiciela wraz z danymi kontaktowymi, o których mowa w art. 7 ust. 2 pkt 17 lit. a lub b;

7) adresy innych miejsc prowadzenia działalności na terenie Unii Europejskiej;
8) adres wyznaczonego przedstawiciela, jeśli został wyznaczony;
9) wskazanie państw członkowskich Unii Europejskiej, w których podmiot świadczy usługi;
10) główne miejsce prowadzenia działalności ustalone zgodnie z art. 5a ust. 3–6.

6. Pojedynczy Punkt Kontaktowy, co trzy miesiące, przedkłada ENISA sprawozdanie podsumowujące, zawierające dane o:
1) incydentach poważnych;
2) incydentach;
3) cyberzagrożeniach;
4) potencjalnych zdarzeniach dla cyberbezpieczeństwa.

7. Organ właściwy do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej, CSIRT sektorowy dla tego sektora oraz CSIRT MON, CSIRT NASK, CSIRT GOV może, za pośrednictwem Pojedynczego Punktu Kontaktowego, złożyć wniosek do ENISA o udostępnienie danych z rejestru dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców chmury obliczeniowej, dostawców usług ośrodka przetwarzania danych, dostawców sieci dostarczania treści, dostawców usług zarządzanych, dostawców usług zarządzanych w zakresie cyberbezpieczeństwa, jak również dostawców internetowych platform handlowych, wyszukiwarek internetowych i platform usług sieci społecznościowych. We wniosku wskazuje się zakres żądanych danych.

8. Organy właściwe do spraw cyberbezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego, Minister Obrony Narodowej, minister właściwy do spraw informatyzacji mogą, za pomocą Pojedynczego Punktu Kontaktowego, zwrócić się do ENISA o udzielenie wsparcia przy rozwijaniu CSIRT sektorowych oraz CSIRT MON, CSIRT NASK lub CSIRT GOV.

Art. 50. 1. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:
1) niezwłocznie informacje o:
   a) wyznaczonych organach właściwych do spraw cyberbezpieczeństwa, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa;

2) co 2 lata informacje dotyczące krajowego systemu cyberbezpieczeństwa, w szczególności:
   a) liczbę podmiotów kluczowych w podziale na poszczególne sektory,
   b) liczbę podmiotów ważnych w podziale na poszczególne sektory,
   c) rodzaje usług świadczonych przez podmioty kluczowe lub podmioty ważne,
   d) przepisy, na podstawie których podmioty kluczowe lub podmioty ważne zostały wskazane.
3) informacje o zadaniach CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu.

2. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy:
1) liczbę podmiotów kluczowych w podziale na poszczególne sektory;
2) liczbę podmiotów ważnych w podziale na poszczególne sektory.

Rozdział 10

Zadania Ministra Obrony Narodowej

Art. 51. Minister Obrony Narodowej jest odpowiedzialny za:
1) współpracę Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa;
2) zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku cyberzagrożenia powodującego konieczność działań obronnych;
3) rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;
4) pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej;
5) koordynację działań związanych z obsługą incydentów w czasie stanu wojennego lub w czasie wojny, z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych;

6) ocenę wpływu incydentów poważnych i krytycznych na system obronny państwa;
7) ocenę cyberzagrożeń, w zakresie ich wpływu na system obronny państwa oraz przedstawianie właściwym organom, w przypadku wprowadzenia stanu wojennego lub stanu wojny, propozycji dotyczących działań obronnych z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych;
8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego lub w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia z zastrzeżeniem kompetencji Naczelnego Dowódcy Sił Zbrojnych.

Art. 52. Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego, do którego zadań należy:

1) zapewnienie współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa;
2) koordynacja działań w zakresie wzmacniania zdolności obronnych w przypadku cyberzagrożenia;
3) zapewnienie współpracy między narodowymi i sojuszniczymi siłami zbrojnymi w zakresie zapewnienia cyberbezpieczeństwa;
4) rozwijanie systemów wymiany informacji o cyberzagrożeniach w obszarze obrony narodowej;
5) udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.

Rozdział 10a

Zadania ministra właściwego do spraw energii

Art. 52a. 1. Organem właściwym, o którym mowa w art. 4 ust. 1 rozporządzenia 2024/1366, jest minister właściwy do spraw energii.

2. Właściwy organ, określony w ust. 1, identyfikuje podmioty o dużym wpływie i podmioty o krytycznym wpływie zgodnie z art. 24 rozporządzenia

2024/1366. Identyfikacja podmiotu o dużym wpływie lub podmiotu o krytycznym wpływie jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego, i wymaga uzasadnienia.

3. Minister właściwy do spraw energii może wystąpić do podmiotu kluczowego lub podmiotu ważnego z podsektora energii elektrycznej o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot o dużym wpływie lub podmiot o krytycznym wpływie zgodnie z art. 24 rozporządzenia 2024/1366. Przepisy art. 53c ust. 1–3 stosuje się odpowiednio.

Art. 52b. 1. Minister właściwy do spraw energii prowadzi kontrole podmiotów zidentyfikowanych jako podmioty o krytycznym wpływie, o których mowa w rozporządzeniu 2024/1366.

2. W przypadku kontroli, o której mowa w ust. 1, przepisy art. 54 stosuje się.

Rozdział 10b

Zadania ministra właściwego do spraw zagranicznych

Art. 52c. Minister właściwy do spraw zagranicznych prowadzi i koordynuje działalność dyplomatyczną w zakresie cyberbezpieczeństwa w stosunkach z państwami trzecimi i organizacjami międzynarodowymi.

Art. 52d. Minister właściwy do spraw informatyzacji przekazuje ministrowi właściwemu do spraw zagranicznych, z wyłączeniem danych osobowych:

1) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, o wystąpieniu incydentu dotyczącego innych państw wraz z krótkim opisem i wskazaniem wszystkich państw, których dotyczył incydent;
2) sprawozdanie, o którym mowa w art. 49 ust. 6;
3) informacje pochodzące z Grupy Współpracy, o których mowa w art. 49 ust. 3 pkt 4–6;
4) informacje, o których mowa w art. 49 ust. 1;
5) informacje, odebrane i wysyłane przez Pojedynczy Punkt Kontaktowy, dotyczące sytuacji kryzysowych w cyberprzestrzeni.

Rozdział 10c

Organy odpowiedzialne za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę

Art. 52e. Minister właściwy do spraw informatyzacji pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym, z wyłączeniem spraw dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem.

Art. 52f. Minister Obrony Narodowej pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze militarnym.

Art. 52g. Szef Agencji Bezpieczeństwa Wewnętrznego pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym w sprawach dotyczących zagrożeń terrorystycznych oraz zagrożeń związanych ze szpiegostwem.

Art. 52h. Organ odpowiedzialny za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę koordynuje działania organów państwa zgodnie z Krajowym planem.

Rozdział 11

Nadzór i kontrola podmiotów kluczowych lub podmiotów ważnych

Art. 53. 1. Nadzór dotyczący stosowania przepisów ustawy sprawują organy właściwe do spraw cyberbezpieczeństwa w zakresie wykonywania przez podmioty kluczowe i podmioty ważne wynikających z ustawy obowiązków.

2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych może:

1) prowadzić kontrole, w tym doraźne, w siedzibie podmiotu, miejscu wykonywania działalności gospodarczej lub zdalnie;
2) w drodze decyzji nałożyć na podmiot obowiązek przeprowadzania audytu, o którym mowa w art. 15 ust. 1b, w szczególności w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów ustawy;

3) zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego;
4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny środków, o których mowa w art. 8 ust. 1 pkt 2 i 5, a także zgodności danych i informacji przekazanych przez podmiot do wykazu;
5) wystąpić z wnioskiem o udzielenie dostępu do danych, dokumentów i informacji koniecznych do wykonywania nadzoru;
6) wystąpić z wnioskiem o przedstawienie dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.

3. Organy właściwe do spraw cyberbezpieczeństwa za pomocą działań nadzorczych sprawują nadzór o charakterze:
1) prewencyjnym i następczym nad podmiotami kluczowymi;
2) następczym nad podmiotami ważnymi, w szczególności w przypadku uzasadnionego podejrzenia, że zachodzi możliwość naruszenia przepisów ustawy.

4. W przypadku uzasadnionego podejrzenia, że działania lub zaniechania podmiotu kluczowego mogą naruszać przepisy ustawy, organ właściwy do spraw cyberbezpieczeństwa kieruje do tego podmiotu pismo w formie elektronicznej z ostrzeżeniem, w którym wskazuje czynności, jakie należy podjąć w celu zapobieżenia lub zaprzestania naruszania przepisów ustawy oraz termin na ich wykonanie.

5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, także wtedy gdy podmiot kluczowy nie zastosował się do pisma z ostrzeżeniem, o którym mowa w ust. 4, może:
1) nakazać podjęcie określonych czynności dotyczących obsługi incydentu;
2) nakazać, w drodze decyzji, zaniechanie naruszania przepisów ustawy;
3) nakazać, w drodze decyzji, zapewnienie zgodności systemu zarządzania bezpieczeństwem informacji zgodnie z art. 8 ust. 1 pkt 2 lub zgodnie z art. 8 ust. 3 lub realizacji obowiązku zgłaszania incydentu poważnego;
4) nakazać, w drodze decyzji, poinformowanie, w określony przez niego sposób, odbiorców usług tego podmiotu, których dotyczy poważne cyberzagrożenie,

o charakterze tego zagrożenia oraz o możliwych środkach ochronnych lub naprawczych, jakie należy podjąć w reakcji na to zagrożenie;

5) nakazać, w drodze decyzji, wdrożenie, w określonym terminie, zaleceń wydanych w wyniku audytu lub audytu, o którym mowa w art. 15 ust. 1b;

6) wyznaczyć, w drodze decyzji, na określony czas, niedłuższy niż miesiąc, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3, wskazując ściśle określone zadania, które urzędnik monitorujący realizuje w tym czasie;

7) nakazać, w drodze decyzji, podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy;

8) nakazać, w drodze decyzji wydanej w postępowaniu uproszczonym, o którym mowa w rozdziale 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, podanie do publicznej wiadomości informacji o incydencie poważnym.

6. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5, wyznacza podmiotowi kluczowemu termin, w którym zobowiązuje ten podmiot do podjęcia określonych czynności, usunięcia uchybień lub zapewnienia zgodności z wymogami określonymi przez organ.

7. Nakaz, o którym mowa w ust. 5 pkt 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego i wymaga uzasadnienia.

8. Postępowanie w sprawach, o którym mowa w ust. 5 pkt 2–8, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.

9. Organ właściwy do spraw cyberbezpieczeństwa, w przypadku gdy podmiot kluczowy nie zastosował się do nakazu, o którym mowa w ust. 5 pkt 1, lub postanowień decyzji, o której mowa w ust. 5 pkt 2–8, może:

1) wstrzymać udzieloną temu podmiotowi koncesję albo ograniczyć jej zakres do czasu usunięcia uchybień lub zaprzestania naruszeń lub

2) wstrzymać w całości albo w części działalność podmiotu kluczowego wpisanego do rejestru działalności regulowanej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub

3) wstrzymać zezwolenie na prowadzenie działalności gospodarczej wydane podmiotowi kluczowemu albo ograniczyć zakres tego zezwolenia do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
4) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do Centralnej Ewidencji i Informacji o Działalności Gospodarczej, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
5) wstrzymać w całości albo w części działalność podmiotu kluczowego, wpisanego do rejestru przedsiębiorców Krajowego Rejestru Sądowego, do czasu usunięcia uchybień lub zaprzestania naruszeń, lub
6) zakazać pełnienia w podmiocie kluczowym funkcji zarządczych przez kierownika podmiotu do czasu usunięcia uchybień lub zaprzestania naruszeń, o ile nie doprowadzi to do uniemożliwienia funkcjonowania podmiotu kluczowego w zakresie, jaki jest niezbędny do usunięcia uchybień lub zaprzestania naruszeń.

10. Środków, o których mowa w ust. 9, nie stosuje się do podmiotów publicznych.

11. W przypadku wniesienia przez podmiot kluczowy skargi do sądu administracyjnego, o której mowa w ust. 7 lub 8, środków, o których mowa w ust. 9, nie stosuje się do czasu rozstrzygnięcia sprawy przez ten sąd. Sąd rozstrzyga sprawę w terminie miesiąca od dnia wniesienia skargi.

12. Organ właściwy do spraw cyberbezpieczeństwa, podejmując działania, o których mowa w ust. 5 i 9, uwzględnia:

1) wagę naruszenia i znaczenie naruszonych przepisów ustawy, przy czym za poważne naruszenie należy uznać:
   a) powtarzające się naruszenie,
   b) niezgłoszenie lub nieobsłużenie incydentów poważnych,
   c) nieusunięcie uchybień zgodnie z wiążącymi nakazami organów właściwych do spraw cyberbezpieczeństwa,
   d) utrudnianie prowadzenia audytów lub działań monitorujących nakazanych przez organ właściwy do spraw cyberbezpieczeństwa po stwierdzeniu naruszenia,

e) dostarczanie nieprawdziwych lub rażąco niedokładnych informacji w odniesieniu do środków zarządzania ryzykiem w cyberbezpieczeństwie lub obowiązków zgłaszania incydentów poważnych;

2) czas trwania naruszenia;

3) wcześniejsze poważne naruszenia ze strony danego podmiotu;

4) spowodowane szkody majątkowe i niemajątkowe, w tym straty finansowe lub gospodarcze, wpływ na inne usługi i liczbę użytkowników, których dotyka incydent;

5) umyślny lub nieumyślny charakter czynu ze strony sprawcy naruszenia;

6) środki zastosowane przez podmiot, aby zapobiec szkodom majątkowym i niemajątkowym lub je ograniczyć;

7) stopień współpracy podmiotu z organem właściwym do spraw cyberbezpieczeństwa.

13. Organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków, o których mowa w ust. 4, 5 i 9, oraz przed nałożeniem kary pieniężnej, informuje podmiot kluczowy o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji lub podjęcia działań, o których mowa w ust. 4, 5 i 9, lub do nałożenia kary pieniężnej. Informacja o wstępnych ustaleniach zawiera szczegółowe uzasadnienie, potwierdzające zasadność zamiaru zastosowania środków lub nałożenia kary pieniężnej.

14. Podmiot kluczowy może przedstawić swoje stanowisko niezwłocznie, niepóźniej niż w terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, o których mowa w ust. 13.

15. Organ właściwy do spraw cyberbezpieczeństwa po przedstawieniu przez podmiot kluczowy swojego stanowiska:

1) uwzględnia stanowisko tego podmiotu i odstępuje od zastosowania środków, o których mowa w ust. 4, 5 lub 9, lub od nałożenia kary pieniężnej, oraz informuje podmiot o tym fakcie;

2) odrzuca stanowisko tego podmiotu i stosuje środki, o których mowa w ust. 4, 5 lub 9, lub nakłada karę pieniężną, oraz informuje podmiot o tym fakcie wraz ze szczegółowym uzasadnieniem przyczyn odrzucenia stanowiska podmiotu.

16. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od poinformowania o wstępnych ustaleniach w przypadku, gdy utrudniłoby to

natychmiastowe działanie w celu zapobieżenia incydentom, reakcji na nie lub mogłoby mieć niekorzystny wpływ na bezpieczeństwo państwa lub porządek publiczny.

17. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje przepisy ust. 2, 4, 5 pkt 1–5 i 7–8 oraz ust. 6–8 i 12–16.

Art. 53a. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą tworzyć, samodzielnie lub wspólnie, metodyki nadzoru dotyczące prowadzenia nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi w zakresie stosowania przepisów ustawy.

2. Metodyki nadzoru określają w szczególności:

1) zakres nadzoru;
2) sposób przeprowadzania nadzoru;
3) kryteria oceny.

3. W przypadku stworzenia metodyki nadzoru organy właściwe do spraw cyberbezpieczeństwa co dwa lata oceniają skuteczność stosowania tej metodyki nadzoru, w szczególności oceniając efektywność sprawowanego nadzoru.

4. Na podstawie oceny skuteczności organy właściwe do spraw cyberbezpieczeństwa dokonują zmian w metodykach nadzoru.

Art. 53b. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą ustalać hierarchię priorytetów w sprawowaniu nadzoru w oparciu o metodykę nadzoru, o której mowa w art. 53a ust. 1, uwzględniając w szczególności wyniki analizy ryzyka dla konkretnego podmiotu kluczowego lub podmiotu ważnego.

2. Analiza ryzyka przeprowadzana jest przez organ właściwy do spraw cyberbezpieczeństwa i uwzględnia w szczególności:

1) znaczenie usługi dla bezpieczeństwa narodowego i porządku publicznego;
2) wpływ usługi na gospodarkę i społeczeństwo;
3) prawdopodobieństwo wystąpienia incydentu w podmiocie nadzorowanym oraz rodzaj tego incydentu;
4) potencjalne skutki incydentu takie jak straty finansowe, szkody wizerunkowe, utrata danych osobowych lub zakłócenia w funkcjonowaniu systemów i infrastruktury.

Art. 53c. 1. Podmiot kluczowy lub podmiot ważny przekazuje na żądanie organu właściwego do spraw cyberbezpieczeństwa dane, informacje i dokumenty niezbędne do wykonywania przez ten organ jego uprawnień i obowiązków z zakresu sprawowania nadzoru i kontroli określonych w ustawie.

2. Żądanie, o którym mowa w ust. 1, ma być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać:

1) wskazanie podmiotu kluczowego lub podmiotu ważnego, do którego jest skierowane;
2) datę żądania;
3) wskazanie żądanych danych, informacji lub dokumentów oraz okresu, których dotyczą;
4) wskazanie celu, jakiemu dane, informacje lub dokumenty mają służyć;
5) wskazanie terminu przekazania danych, informacji lub dokumentów adekwatnego do zakresu tego żądania, niekrótszego niż 7 dni;
6) uzasadnienie żądania;
7) pouczenie o zagrożeniu karą za niespełnienie żądania, o którym mowa w ust. 1.

3. Żądanie, o którym mowa w ust. 1, sporządza się w postaci elektronicznej i doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego albo przez system teleinformatyczny, o którym mowa w art. 46 ust. 1 pkt 6.

4. Przepisy ust. 1–3 stosuje się odpowiednio do żądania udzielenia dostępu do danych, dokumentów i informacji koniecznych do wykonania nadzoru oraz dowodów realizacji wymogów, o których mowa w art. 8 ust. 1.

Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego po uzyskaniu przepustki, wydanej bezzwłocznie, której wydania nie można odmówić;
2) wglądu do dokumentów dotyczących działalności podmiotu kluczowego;
3) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu nadzoru;

4) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu nadzoru;
5) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych, po wcześniejszym zawiadomieniu podmiotu kluczowego.

2. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 6, realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej.

3. Do nadzorowania przez urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, stosuje się przepis art. 58.

4. Zawiadomienie, o którym mowa w ust. 1 pkt 5, przekazuje się na adres do doręczeń elektronicznych albo za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w terminie 1 dnia przed przeprowadzeniem oględzin.

Art. 53e. 1. Realizując uprawnienie, o którym mowa w art. 53 ust. 9, organ właściwy do spraw cyberbezpieczeństwa wydaje decyzję, która zawiera:
1) dane podmiotu kluczowego lub kierownika podmiotu kluczowego;
2) rodzaj stwierdzonych uchybień lub naruszeń dokonanych przez podmiot kluczowy lub kierownika podmiotu kluczowego;
3) podjęte dotychczas środki nadzorcze nad podmiotem kluczowym;
4) podstawę prawną i rodzaj środka określonego w art. 53 ust. 9;
5) termin stosowania tego środka;
6) uzasadnienie.

2. Termin stosowania środków, o których mowa w art. 53 ust. 9, określa się przy uwzględnieniu kryteriów, o których mowa w art. 53 ust. 12. Środek nie może być stosowany dłużej niż 14 dni od daty doręczenia decyzji o jego zastosowaniu.

3. W zależności od zastosowanego środka, jeżeli podmiot kluczowy usunął uchybienia lub zaprzestał naruszania przepisów ustawy przed terminem określonym w decyzji, uchyla się decyzję o zastosowaniu tego środka.

4. W przypadku powzięcia informacji, w szczególności na skutek stosowania innych środków nadzorczych, określonych w art. 53 ust. 1, 4 i 5, że podmiot kluczowy nie usunął wcześniej stwierdzonych uchybień lub w dalszym ciągu narusza przepisy ustawy lub w przypadku, gdy podmiot kluczowy nie wykazał w terminie, na jaki został zastosowany środek, że usunął uchybienia lub zaprzestał naruszania przepisów ustawy, organ właściwy do spraw cyberbezpieczeństwa

ponownie wydaje decyzję o zastosowaniu środka określonego w art. 53 ust. 9 na kolejny okres, niedłuższy niż 14 dni. Przepis ten stosuje się do czasu usunięcia uchybień lub zaprzestania naruszeń przez podmiot kluczowy. W stosunku do ponownej decyzji nie stosuje się przepisów art. 53 ust. 13–16.

5. Organ właściwy do spraw cyberbezpieczeństwa z urzędu lub na wniosek podmiotu kluczowego uchyla decyzję, o której mowa w ust. 1, po usunięciu uchybień lub zaprzestaniu naruszeń przez podmiot kluczowy.

6. Podmiot kluczowy może złożyć wniosek, o którym mowa w ust. 5, po usunięciu uchybień lub zaprzestaniu naruszeń, przedstawiając dowody potwierdzające zastosowanie się odpowiednio do nakazu, o którym mowa w art. 53 ust. 5 pkt 1, lub postanowień decyzji, o której mowa w art. 53 ust. 5 pkt 2–8.

7. Wniosek, o którym mowa w ust. 5, organ właściwy do spraw cyberbezpieczeństwa rozpatruje niezwłocznie, niepóźniej niż w terminie 7 dni od dnia jego otrzymania.

8. Czynności, o których mowa w ust. 3 i 5, organ dokonuje w formie decyzji.

9. Decyzja, o której mowa w ust. 1, jest wykonalna z dniem jej doręczenia podmiotowi kluczowemu. Decyzje, o których mowa w ust. 3, 4 i 5, są natychmiast wykonalne.

10. Postępowanie w sprawie stosowania i uchylania środków, o których mowa w art. 53 ust. 9, jest jednoinstancyjne. Na decyzje, o których mowa w ust. 1 i 3–5, podmiot kluczowy może wnieść skargę do sądu administracyjnego.

11. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o zastosowaniu wobec podmiotu kluczowego lub kierownika podmiotu kluczowego środków, o których mowa w art. 53 ust. 9. Informacja zawiera:

1) dane podmiotu kluczowego lub imię i nazwisko kierownika tego podmiotu kluczowego;
2) podstawę prawną i rodzaj zastosowanego środka, o którym mowa w art. 53 ust. 9;
3) wskazanie daty początkowej i końcowej okresu na jaki zastosowano środek;
4) wskazanie, czy wobec podmiotu kluczowego lub kierownika podmiotu kluczowego ponownie zastosowano środek, a jeśli tak, to wskazanie nowej daty końcowej stosowania tego środka.

12. Publikacja, o której mowa w ust. 11, nie obejmuje tajemnicy przedsiębiorstwa.

13. Organ właściwy do spraw cyberbezpieczeństwa publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej informację o uchyleniu decyzji, o której mowa w ust. 1.

14. Podmiot kluczowy, w okresie stosowania wobec niego środka, o którym mowa w art. 53 ust. 9, nie może wykonywać działalności, której dotyczy ten środek.

15. W okresie stosowania środka, o którym mowa w art. 53 ust. 9, podmiot kluczowy ma obowiązek niezwłocznie podjąć działania zmierzające jedynie do usunięcia uchybień bądź zaprzestania naruszeń. W tym celu w szczególności może składać oświadczenia woli i wiedzy, podejmować czynności procesowe w postępowaniach, przedsiębrać czynności faktyczne, jeżeli nie stoją one w sprzeczności z celem stosowanego środka lub nie zmierzają do jego obejścia.

16. W zakresie nieuregulowanym, a dotyczącym zawieszania, ograniczania i wznawiania koncesji, zezwolenia na prowadzenie działalności gospodarczej lub wstrzymania prowadzenia działalności gospodarczej zastosowanie mają przepisy odrębne.

Art. 53f. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą wspólnie sprawować nadzór, w tym wspólnie prowadzić kontrolę, nad podmiotami kluczowymi lub podmiotami ważnymi.

2. Organy właściwe do spraw cyberbezpieczeństwa, sprawując wspólnie nadzór, w tym prowadząc kontrolę, mogą wyznaczyć wiodący organ właściwy do spraw cyberbezpieczeństwa.

3. Organy właściwe do spraw cyberbezpieczeństwa informują się wzajemnie o zamiarze wszczęcia kontroli w podmiocie, nad którym wspólnie sprawują nadzór.

4. Przepisy ust. 1–3 stosuje się odpowiednio do współpracy organów właściwych do spraw cyberbezpieczeństwa i organów właściwych do spraw podmiotów krytycznych w przypadku, gdy nadzór jest sprawowany nad podmiotem kluczowym będącym podmiotem krytycznym.

Art. 54. Do kontroli realizowanej wobec podmiotów kluczowych lub podmiotów ważnych:

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;
3) będących jednostkami samorządu terytorialnego stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.

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

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

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

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

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. Zlecenie tłumaczenia dokumentacji podmiotom trzecim odbywa się z poszanowaniem tajemnicy prawnie chronionej na podstawie odrębnych przepisów.

4. Organ przeprowadzający kontrolę, występując do podmiotu kontrolowanego z żądaniem, o którym mowa w ust. 3, wskazuje zakres dokumentów, które mają zostać przetłumaczone, ich związek z przeprowadzaną kontrolą oraz określa termin na przedstawienie tłumaczenia dokumentacji, uwzględniający zakres koniecznego tłumaczenia.

Art. 57. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

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

2. Protokół kontroli zawiera:

1) wskazanie nazwy albo imienia i nazwiska oraz adresu podmiotu kontrolowanego;
2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot;
3) imię i nazwisko, stanowisko oraz numer upoważnienia osoby prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;

6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7) wyszczególnienie załączników.

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

4. W przypadku zastrzeżeń dotyczących ustaleń zawartych w protokole kontroli, podmiot kontrolowany ma prawo odmówić podpisania protokołu kontroli oraz złożyć umotywowane pisemne zastrzeżenia do tego protokołu w terminie 7 dni od dnia przedstawienia mu go do podpisu.

5. Odmowę podpisania protokołu kontroli osoba prowadząca czynności kontrolne odnotowuje w protokole wraz ze wskazaniem daty tej odmowy.

6. W razie złożenia zastrzeżeń do protokołu kontroli kierownik komórki organizacyjnej do spraw kontroli dokonuje ich analizy.

7. Kierownik komórki organizacyjnej do spraw kontroli:
1) odrzuca zastrzeżenia do protokołu kontroli wniesione przez osobę nieuprawnioną lub wniesione po upływie terminu i informuje o tym na piśmie zgłaszającego zastrzeżenia, podając przyczyny, albo
2) uwzględnia zastrzeżenia do protokołu kontroli w całości albo w części albo je oddala.

8. W razie potrzeby, w związku ze zgłoszeniem zastrzeżeń do protokołu, osoba prowadząca czynności kontrolne podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia przez kierownika komórki organizacyjnej do spraw kontroli zasadności zastrzeżeń do protokołu kontroli zmienia lub uzupełnia odpowiednią część protokołu kontroli w formie aneksu do protokołu.

9. Kierownik komórki organizacyjnej do spraw kontroli, po rozpatrzeniu zastrzeżeń do protokołu kontroli, sporządza stanowisko wobec tych zastrzeżeń.

10. O nieuwzględnieniu zastrzeżeń do protokołu kontroli w całości albo w części kierownik komórki organizacyjnej do spraw kontroli informuje podmiot kontrolowany na piśmie.

11. Protokół kontroli:
1) w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu;

2) w postaci elektronicznej doręcza się podmiotowi kontrolowanemu na adres do doręczeń elektronicznych.

Art. 59. 1. Jeżeli na podstawie informacji zgromadzonych w toku kontroli organ właściwy do spraw cyberbezpieczeństwa uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne wzywające do usunięcia nieprawidłowości. Organ właściwy do spraw cyberbezpieczeństwa wskazuje termin usunięcia tych nieprawidłowości, uwzględniając zakres i rodzaj naruszeń.

2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze.

3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy do spraw cyberbezpieczeństwa o sposobie wykonania zaleceń.

Art. 59a. 1. W przypadku stwierdzenia podczas sprawowania nadzoru podejrzenia naruszenia ochrony danych osobowych organ właściwy do spraw cyberbezpieczeństwa informuje o tym Prezesa Urzędu Ochrony Danych Osobowych w terminie 7 dni od dnia stwierdzenia podejrzenia tego naruszenia.

2. W przypadku stwierdzenia podejrzenia naruszenia ochrony danych osobowych podczas sprawowania nadzoru nad jednostką organizacyjną prokuratury organ właściwy do spraw cyberbezpieczeństwa informuje właściwy organ prokuratury, o którym mowa w art. 191a § 1 ustawy z dnia 28 stycznia 2016 r. – Prawo o prokuraturze (Dz. U. z 2024 r. poz. 390, z 2025 r. poz. 304 i 1178 oraz z 2026 r. poz. 26).

3. W przypadku stwierdzenia podejrzenia naruszenia ochrony danych osobowych podczas sprawowania nadzoru nad sądem organ właściwy do spraw cyberbezpieczeństwa informuje właściwego prezesa sądu albo Krajową Radę Sądownictwa, o których mowa w art. 175dd § 1 ustawy z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych (Dz. U. z 2024 r. poz. 334, z późn. zm.[14)]).

Art. 59b. 1. Organ właściwy do spraw cyberbezpieczeństwa udziela pomocy organom innych państw członkowskich Unii Europejskiej w sprawowaniu nadzoru nad podmiotami kluczowymi lub podmiotami ważnymi, których systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej.

14) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1907, z 2025 r. poz. 526, 820, 1172, 1178 i 1609 oraz z 2026 r. poz. 26.

2. Organ właściwy do spraw cyberbezpieczeństwa może, za pośrednictwem Pojedynczego Punktu Kontaktowego, zwracać się do organów innych państw członkowskich Unii Europejskiej o przeprowadzenie czynności nadzorczych nad podmiotami kluczowymi lub podmiotami ważnymi, świadczącymi usługi na terytorium Rzeczypospolitej Polskiej, których siedziba, zarząd lub systemy informacyjne znajdują się na terytorium innego państwa członkowskiego Unii Europejskiej.

3. Organ właściwy do spraw cyberbezpieczeństwa odmawia udzielenia pomocy, o której mowa w ust. 1, jeżeli:

1) nie jest właściwy w sprawie;
2) żądana pomoc jest nieproporcjonalna do realizowanych przez organ zadań z zakresu nadzoru;
3) organ innego państwa członkowskiego Unii Europejskiej żąda udostępnienia informacji lub dokumentów, których udostępnienie narusza podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności.

4. Przed odmową udzielenia pomocy organ właściwy do spraw cyberbezpieczeństwa konsultuje się z wnioskującym o udzielenie pomocy organem innego państwa, a także z Komisją Europejską i ENISA, jeśli żąda tego państwo członkowskie Unii Europejskiej.

5. Organ właściwy do spraw cyberbezpieczeństwa może prowadzić wspólne czynności nadzorcze z organem innego państwa członkowskiego Unii Europejskiej.

6. Organy właściwe do spraw cyberbezpieczeństwa współpracują za pośrednictwem Pojedynczego Punktu Kontaktowego z organami innych państw członkowskich Unii Europejskiej właściwych do stosowania rozporządzenia 2022/2554.

7. Organy właściwe do spraw cyberbezpieczeństwa informują forum nadzoru, o którym mowa w art. 32 ust. 1 rozporządzenia 2022/2554, jeżeli podejmują czynności nadzorcze wobec podmiotu kluczowego, który został wyznaczony jako kluczowy dostawca usług ICT zgodnie z art. 31 rozporządzenia 2022/2554.

Art. 59c. 1. W przypadkach uzasadnionych charakterem sprawy lub pilnością przeprowadzenia czynności kontrolnych wynikających z ochrony bezpieczeństwa

państwa lub bezpieczeństwa i porządku publicznego lub w przypadku potrzeby realizacji wzajemnej pomocy, o której mowa w art. 59b ust. 1, lub potrzeby sprawdzenia, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń, można zarządzić przeprowadzenie kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1.

2. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być zarządzona w szczególności w razie potrzeby:

1) sprawdzenia informacji uzyskanej od urzędnika monitorującego, o którym mowa w art. 53 ust. 5 pkt 6, że podmiot kluczowy może naruszać przepisy ustawy;
2) sprawdzenia, w celu podjęcia działań na podstawie art. 53e ust. 4 i 5, czy podmiot kluczowy usunął uchybienia lub zaprzestał dokonywania naruszeń;
3) sprawdzenia wykonania zaleceń pokontrolnych, wykonania decyzji albo postanowień nakazujących usunięcie naruszeń prawa w związku z przeprowadzoną kontrolą.

3. Kontrolę doraźną, o której mowa w art. 53 ust. 2 pkt 1, prowadzi się zgodnie z przepisami dotyczącymi kontroli na zasadach ogólnych. Do podmiotów kontrolowanych niebędących przedsiębiorcami nie stosuje się przepisów dotyczących programu kontroli i sporządzania wystąpienia pokontrolnego.

4. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, może być prowadzona także wtedy, gdy nie było możliwości wcześniejszego powiadomienia podmiotu kontrolowanego o terminie przeprowadzenia kontroli. Uzasadnienie przyczyny braku powiadomienia o zamiarze wszczęcia kontroli umieszcza się w sprawozdaniu z kontroli albo protokole kontroli.

5. Kontrola doraźna, o której mowa w art. 53 ust. 2 pkt 1, kończy się sporządzeniem:

1) sprawozdania z kontroli – w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami,
2) protokołu kontroli – w przypadku podmiotów będących przedsiębiorcami

– zawierającymi opis ustalonego stanu faktycznego oraz jego ocenę, a także, w razie potrzeby, zalecenia lub wnioski wzywające do usunięcia nieprawidłowości lub usprawnienia funkcjonowania podmiotu kontrolowanego. Sprawozdanie z

kontroli albo protokół kontroli podpisuje kierownik komórki do spraw kontroli w organie właściwym do spraw cyberbezpieczeństwa.

6. Kierownik podmiotu kontrolowanego w terminie 3 dni roboczych od dnia otrzymania sprawozdania z kontroli albo protokołu kontroli, o których mowa w ust. 5, ma prawo przedstawić do niego stanowisko. Nie wstrzymuje to realizacji ustaleń kontroli doraźnej.

7. Jeżeli w toku kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, zostaną ujawnione okoliczności wskazujące na naruszenia przepisów ustawy, które wykraczają poza zakres tej kontroli, kontrolę w dalszej części przeprowadza się na zasadach ogólnych z zastosowaniem przepisów art. 54–59b.

8. Do kontroli doraźnej, o której mowa w art. 53 ust. 2 pkt 1, w zakresie nieuregulowanym niniejszą ustawą w stosunku do podmiotów będących przedsiębiorcami stosuje się odpowiednio przepisy ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, a w przypadku jednostek samorządu terytorialnego oraz podmiotów niebędących przedsiębiorcami – przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej. Przepisów art. 47 ust. 1 i 2 oraz art. 54 ust. 1 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców nie stosuje się.

Rozdział 12

Pełnomocnik i Kolegium

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

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

2. Pełnomocnik podlega Radzie Ministrów.

3. Pełnomocnikiem jest minister właściwy do spraw informatyzacji, sekretarz stanu albo podsekretarz stanu w urzędzie obsługującym ministra właściwego do spraw informatyzacji.

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

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

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

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

1) współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;
2) podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa;
3) podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie cyberzagrożeń i bezpiecznego korzystania z Internetu.

3. Pełnomocnik może dokonywać zakupów produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa na rzecz podmiotów, o których mowa w art. 62a ust. 2 pkt 3, na podstawie umowy, przekazując prawa do zakupionych produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa.

4. Pełnomocnik może, w zakresie realizacji jego zadań, zlecać przeprowadzanie badań lub ekspertyz.

5. Pełnomocnik może, w drodze zarządzenia, powoływać zespoły doradcze.

6. Pełnomocnik może upoważnić do realizacji swoich zadań pracownika ministerstwa lub urzędu administracji rządowej go obsługującego, który:

1) pełni funkcję dyrektora departamentu, zastępcy dyrektora departamentu lub naczelnika wydziału;
2) spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”.

7. Organy administracji rządowej oraz jednostki organizacyjne podległe tym organom lub przez nie nadzorowane są obowiązane do udzielania pomocy Pełnomocnikowi przy realizacji jego zadań, w szczególności przez udostępnianie mu informacji i dokumentów.

8. Zadania Pełnomocnika są finansowane z części budżetowej, której dysponentem jest minister właściwy do spraw informatyzacji.

Art. 62a 1. Przy Pełnomocniku działa PCOC, jako organ pomocniczy w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej.

2. W skład PCOC wchodzą:

1) Pełnomocnik;
2) sekretarz PCOC;
3) przedstawiciele:
   a) ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, jeżeli został powołany,
   b) ministra właściwego do spraw informatyzacji,
   c) ministra właściwego do spraw wewnętrznych,
   d) ministra właściwego do spraw zagranicznych,
   e) Ministra Obrony Narodowej,
   f) Ministra Sprawiedliwości,
   g) Szefa Kancelarii Prezesa Rady Ministrów,
   h) organów właściwych do spraw cyberbezpieczeństwa,
   i) CSIRT GOV,
   j) CSIRT MON,
   k) CSIRT NASK,
   l) CSIRT sektorowych,
   m) Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni,

n) dyrektora Rządowego Centrum Bezpieczeństwa,

o) Komendanta Centralnego Biura Zwalczania Cyberprzestępczości,

p) Komendanta Głównego Policji,

q) Komendanta Służby Ochrony Państwa,

r) Komendanta Głównego Straży Granicznej,

s) Prokuratora Krajowego,

t) Szefa Agencji Bezpieczeństwa Wewnętrznego,

u) Szefa Agencji Wywiadu,

v) Szefa Służby Kontrwywiadu Wojskowego,

w) Szefa Służby Wywiadu Wojskowego.

3. Prezydent Rzeczypospolitej Polskiej może skierować do udziału w pracach PCOC swojego przedstawiciela.

4. Na posiedzenia PCOC mogą być zapraszani przedstawiciele podmiotów kluczowych, podmiotów ważnych lub innych podmiotów, jeżeli wymaga tego temat spotkania.

5. Posiedzeniu PCOC przewodniczy Pełnomocnik.

6. Do zadań PCOC należy:

1) wymiana informacji na temat cyberzagrożeń, incydentów i podatności na poziomie krajowym;
2) wymiana informacji o wynikach szacowania ryzyka związanego z ujawnionymi cyberzagrożeniami oraz zaistniałymi incydentami;
3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1;
4) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;
5) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika;
6) wymiana informacji dotycząca procesów i współpracy międzynarodowej w zakresie bezpieczeństwa w cyberprzestrzeni.

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

8. Sekretarza PCOC powołuje Pełnomocnik spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne”. Sekretarza PCOC odwołuje Pełnomocnik.

9. Sekretarz PCOC może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 8. Zastępcę sekretarza PCOC odwołuje sekretarz PCOC.

10. W przypadku nieobecności sekretarza PCOC jego obowiązki wykonuje zastępca sekretarza PCOC.

11. Obsługę PCOC zapewnia ministerstwo lub inny urząd administracji rządowej obsługujący Pełnomocnika.

12. Pełnomocnik określi, w drodze zarządzenia, tryb pracy PCOC, mając na uwadze charakter zadań PCOC oraz konieczność zapewnienia jego sprawnej pracy.

13. Zarządzenie jest publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

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

2. Pełnomocnik może przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie.

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

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

1) kierunków i planów na rzecz przeciwdziałania cyberzagrożeniom;

1a) planowanych do ustalenia przez Prezesa Urzędu Komunikacji Elektronicznej w projekcie rozstrzygnięcia decyzji w sprawie rezerwacji częstotliwości, o którym mowa w art. 110 ust. 2 ustawy z dnia 12 lipca 2024 r. – Prawo

komunikacji elektronicznej, jeżeli rezerwacja będzie obejmować co najmniej 30 % obszaru kraju i jest dokonywana bez przeprowadzenia postępowania selekcyjnego, o którym mowa w art. 104 ust. 3 tej ustawy, lub po przeprowadzeniu przetargu lub aukcji, o których mowa w art. 104 ust. 3 pkt 2 tej ustawy;

2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, CSIRT sektorowe i organy właściwe do spraw cyberbezpieczeństwa powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania cyberzagrożeniom;
3) współdziałania organów prowadzących lub nadzorujących CSIRT MON, CSIRT GOV, CSIRT NASK i CSIRT sektorowych;
4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego oraz ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, CSIRT sektorowych i organów właściwych do spraw cyberbezpieczeństwa;
5) organizacji wymiany informacji istotnych dla cyberbezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej między organami administracji rządowej;
6) wniosków CSIRT MON, CSIRT NASK lub CSIRT GOV w sprawie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania;
7) wniosków o przyznanie świadczenia teleinformatycznego, o którym mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662 oraz z 2025 r. poz. 1017) w zakresie maksymalnej kwoty prognozowanych kosztów, związanych z przyznaniem świadczenia teleinformatycznego;
8) współdziałania zespołów CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowego w sektorze bankowości i infrastruktury rynków finansowych oraz właściwego organu w rozumieniu rozporządzenia 2022/2554, w zakresie działalności podmiotów finansowych będących podmiotami kluczowymi lub podmiotami ważnymi;

9) decyzji w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka.

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

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

Art. 65a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług świadczonych przez podmioty określone w art. 67b ust. 1, uwzględniającej informacje przekazane przez państwa członkowskie Unii Europejskiej lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium, działając z urzędu lub na wniosek członka Kolegium, może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania, o którym mowa w art. 67b ust. 1, 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 lub CSIRT GOV.

Art. 66. 1. W skład Kolegium wchodzą:

1) przewodniczący Kolegium – Prezes Rady Ministrów;
2) Pełnomocnik;
3) sekretarz Kolegium;
4) członkowie Kolegium:
   a) minister właściwy do spraw wewnętrznych,
   b) minister właściwy do spraw informatyzacji,
   c) Minister Obrony Narodowej,

d) minister właściwy do spraw zagranicznych,

e) Szef Kancelarii Prezesa Rady Ministrów,

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

g) minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego,

h) organy właściwe do spraw cyberbezpieczeństwa.

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

3. Członkowie Kolegium, o których mowa w ust. 1 pkt 4 lit. a–e oraz lit. h, mogą być zastępowani przez upoważnionych przedstawicieli w randze sekretarza stanu, podsekretarza stanu, wiceprezesa urzędu lub zastępcy przewodniczącego.

4. W posiedzeniach Kolegium uczestniczą również:

1) dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;
2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;
3) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;
4) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
5) Przewodniczący Komisji Nadzoru Finansowego;
6) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;
7) Prokurator Generalny albo jego zastępca;
8) Szef Agencji Wywiadu albo jego zastępca;
9) Szef Służby Wywiadu Wojskowego albo jego zastępca.

5. Przewodniczący Kolegium:

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

3) może pisemnie wnioskować o przeprowadzenie badania, o którym mowa w art. 33 ust. 1;
4) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, przeprowadzenie analizy dotyczącej wpływu konkretnych produktów ICT, usług ICT lub procesów ICT na bezpieczeństwo usług, o której mowa w art. 65a ust. 1;
5) może zlecić CSIRT MON, CSIRT NASK lub CSIRT GOV, 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. 65a ust. 2;
6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 67b ust. 1;
7) powołuje zespół opiniujący, o którym mowa w art. 67b ust. 13 pkt 1, oraz wskazuje przedstawicieli członków Kolegium wchodzących w jego skład;
8) rozstrzyga spór, o którym mowa w art. 67b ust. 13 pkt 3, wskazując właściwego członka zespołu opiniującego.

5a. Kolegium przyjmuje i rozpatruje sprawy na posiedzeniu albo w drodze korespondencyjnego uzgodnienia stanowisk (tryb obiegowy).

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

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

7a. Sekretarz Kolegium może powołać swojego zastępcę spośród osób spełniających wymagania określone w ust. 6. Zastępcę sekretarza Kolegium odwołuje sekretarz Kolegium.

7b. W przypadku nieobecności sekretarza Kolegium jego obowiązki wykonuje zastępca sekretarza Kolegium, w tym zastępuje go na posiedzeniu Kolegium.

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

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

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

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

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

Rozdział 12a

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

Art. 67a. 1. Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa.

2. Rekomendacje Pełnomocnika są publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

5. Stosowanie rekomendacji jest dobrowolne.

Art. 67b. 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 dostawcy sprzętu lub oprogramowania, które są wykorzystywane przez:

1) podmioty kluczowe lub podmioty ważne, z wyłączeniem podsektora komunikacji elektronicznej,
2) przedsiębiorców komunikacji elektronicznej, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych,
3) podmioty finansowe, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554

– za dostawcę wysokiego ryzyka.

2. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka, jeżeli ustawa nie stanowi inaczej, stosuje się 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.

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

4. Do postępowania w sprawie uznania za dostawcę wysokiego ryzyka może przystąpić, na wniosek, na prawach strony, przedsiębiorca telekomunikacyjny mający siedzibę na terytorium Rzeczypospolitej Polskiej wpisany do rejestru przedsiębiorców telekomunikacyjnych, 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 2025 r. poz. 1749 oraz z 2026 r. poz. 26). Przepisy art. 31 § 2 i 3 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego stosuje się odpowiednio.

5. 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 ogłoszony przed wszczęciem postępowania.

6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie publikuje się także na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji, niezwłocznie po doręczeniu tego zawiadomienia.

7. Minister właściwy do spraw informatyzacji zawiadamia Prokuratora Generalnego o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka.

8. 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) – strony umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, publikuje się na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia zawiadomienia stronie po upływie 14 dni od dnia jego dokonania.

9. W terminie 14 dni od dnia opublikowania na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji zawiadomienia, o którym mowa w ust. 6 i 8, organizacja społeczna może przedstawić ministrowi właściwemu do spraw informatyzacji stanowisko co do dostawcy sprzętu lub oprogramowania, wobec którego wszczęto postępowanie, oraz dostarczanych przez niego produktów ICT, usług ICT oraz procesów ICT. Minister właściwy do spraw informatyzacji, przed wydaniem decyzji, publikuje na swojej stronie podmiotowej Biuletynu Informacji Publicznej raport ze złożonych w

terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach.

10. Przed wydaniem decyzji minister właściwy do spraw informatyzacji zasięga opinii Kolegium. Kolegium przekazuje opinię w terminie 3 miesięcy od dnia wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do Kolegium do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

11. Opinia, o której mowa w ust. 10 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 lub oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich Unii Europejskiej lub organów Unii Europejskiej lub 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 w przypadku, gdy 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) 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 17.05.2019, str. 1, z późn. zm.[15)]);

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) trybu i zakresu, w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla podmiotów, o których mowa w ust. 1, oraz ryzyka dla procesu wytwarzania i dostarczania sprzętu lub oprogramowania;
6) treści wydanych rekomendacji, o których mowa w art. 33 ust. 4, dotyczących sprzętu lub oprogramowania danego dostawcy.

12. Sporządzając opinię, o której mowa w ust. 10 zdanie pierwsze, 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, w szczególności certyfikaty wydane w ramach europejskich programów certyfikacji cyberbezpieczeństwa;
2) analizy, o których mowa w art. 65a ust. 1 i 2.

13. Procedura sporządzenia opinii, o której mowa w ust. 10 zdanie pierwsze, 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, które następnie przekazuje zespołowi opiniującemu;

15) Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 230 z 17.07.2020, str. 37, Dz. Urz. UE L 246 z 30.07.2020, str. 4, Dz. Urz. UE L 351I z 22.10.2020, str. 1, Dz. Urz. UE L 393 z 23.11.2020, str. 1, Dz. Urz. UE L 114 z 12.04.2022, str. 60, Dz. Urz. UE L 2023/2694 z 28.11.2023, Dz. Urz. UE L 2024/1390 z 17.05.2024, Dz. Urz. UE L 2024/1778 z 24.06.2024, Dz. Urz. UE L 2024/90397 z 09.07.2024, Dz. Urz. UE L 2024/2465 z 12.09.2024, Dz. Urz. UE L 2025/173 z 27.01.2025 oraz Dz. Urz. UE L 2025/886 z 13.05.2025.

3) w przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium, wskazując właściwego członka zespołu opiniującego;
4) jeżeli nie zostały wykonane analizy, o których mowa w art. 65a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie;
5) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
6) ustalenie opinii następuje na posiedzeniu Kolegium;
7) ustaloną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

14. W zespole opiniującym może wziąć udział również przedstawiciel Prezesa Urzędu Ochrony Konkurencji i Konsumentów. W posiedzeniu Kolegium, na którym następuje ustalenie opinii, może wziąć udział Prezes lub Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów.

15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania oraz podmioty wchodzące w skład grupy kapitałowej, w rozumieniu art. 3 ust. 1 pkt 44 ustawy z dnia 29 września 1994 r. o rachunkowości, w ramach której funkcjonuje dostawca, za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi zagrożenie dla podstawowego interesu bezpieczeństwa państwa.

16. Decyzja, o której mowa w ust. 15, zawiera w szczególności wskazanie typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawcy sprzętu lub oprogramowania uwzględnionych w postępowaniu w sprawie uznania za dostawcę wysokiego ryzyka.

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

18. Decyzja, o której mowa w ust. 15, podlega natychmiastowemu wykonaniu.

19. Od decyzji, o której mowa w ust. 15, nie przysługuje wniosek o ponowne rozpatrzenie sprawy.

Art. 67c. 1. W przypadku wydania decyzji, o której mowa w art. 67b ust. 15, podmioty, o których mowa w art. 67b 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 niepóźniej niż w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, 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 pkt 2 oraz w ust. 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, jeżeli 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. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320, z późn. zm.[16)]), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15.

5. W przypadku gdy podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia decyzji, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej

16) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2025 r. poz. 620, 769, 794, 1165, 1173 i 1235.

decyzji, mogą korzystać z tych produktów, usług lub procesów niedłużej niż 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski", a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, niedłużej niż 4 lata od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15.

Art. 67d. 1. Podmioty kluczowe lub podmioty ważne 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. 67b ust. 15.

2. Uprawnionymi organami do uzyskania informacji, o których mowa w ust. 1, są organy właściwe do spraw cyberbezpieczeństwa.

3. Wniosek, o którym mowa w ust. 1, zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;
2) datę wydania decyzji, o której mowa w art. 67b ust. 15;
3) wskazanie zakresu żądanych informacji;
4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, niekrótszego niż 7 dni;
5) uzasadnienie;
6) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 1 pkt 18 i 19.

4. Minister właściwy do spraw informatyzacji może zwrócić się do organów właściwych do spraw cyberbezpieczeństwa, aby uzyskały informacje, o których mowa w ust. 1.

5. Na wniosek ministra właściwego do spraw informatyzacji organ właściwy do spraw cyberbezpieczeństwa przekazuje uzyskane informacje, o których mowa w ust. 1, temu ministrowi.

Art. 67e. 1. Sąd administracyjny rozpatruje skargę na decyzję, o której mowa w art. 67b ust. 15, 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. 67f. Minister właściwy do spraw informatyzacji publikuje na stronie podmiotowej Biuletynu Informacji Publicznej urzędu go obsługującego listę produktów ICT, usług ICT i konkretnych procesów ICT objętych decyzjami, o których mowa w art. 67b ust. 15.

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

2. Polecenie zabezpieczające dotyczy nieokreślonej liczby podmiotów kluczowych lub podmiotów ważnych oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554.

3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się przepisów 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 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, a pozostałe przepisy tej ustawy stosuje się odpowiednio.

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

5. Przed wydaniem polecenia zabezpieczającego minister właściwy do spraw informatyzacji przeprowadza we współpracy z Zespołem analizę obejmującą:

1) istotność cyberzagrożenia związanego z incydentem krytycznym;
2) szacowanie ryzyka związanego z zaistniałym incydentem krytycznym;
3) przewidywane lub zaistniałe skutki incydentu krytycznego;
4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;
5) ocenę stopnia dotkliwości wprowadzanych obowiązków dla podmiotów objętych poleceniem zabezpieczającym oraz proporcjonalności tych obowiązków do celu ich wprowadzania.

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

7. Pełnomocnik, 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. Organy administracji publicznej udzielają informacji, o których mowa w zdaniu pierwszym, niezwłocznie, niepóźniej niż w ciągu 72 godzin od otrzymania wezwania.

8. Przedstawiciele podmiotów, o których mowa w ust. 2, organizacji społecznych zrzeszających podmioty, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Pełnomocnika do udziału w pracach Zespołu lub w jego posiedzeniach 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;
3) termin jego wdrożenia.

10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:

1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;
2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT posiadającym daną podatność;
4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności;
5) nakaz wzmożonego monitorowania zachowania systemu informacyjnego;
6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;
7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany

przez CSIRT MON, 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, niedłużej 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 komunikat o wydaniu polecenia zabezpieczającego, w swoim dzienniku urzędowym oraz na stronie internetowej urzędu obsługującego ministra. Załącznikiem do komunikatu jest wydane polecenie zabezpieczające.

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

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

Art. 67h. Podmioty, których dotyczy polecenie zabezpieczające, są obowiązane przekazać informacje na wniosek organów właściwych do spraw cyberbezpieczeństwa, o wykonywaniu polecenia zabezpieczającego. Przepisy art. 67c ust. 2–5 stosuje się.

Art. 67i. 1. Skargę na polecenie zabezpieczające wnosi się w terminie 2 miesięcy od dnia, w którym komunikat o wydaniu polecenia zabezpieczającego został ogłoszony 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. 67j. 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 67b, art. 67f oraz art. 67g.

2. Minister właściwy do spraw informatyzacji przekazuje niezwłocznie Prezesowi Narodowego Banku Polskiego informacje o decyzjach wydanych na podstawie art. 67b ust. 15 oraz art. 67f ust. 1.

Art. 67k. 1. Do podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi stosuje się przepisy art. 67c, art. 67d, art. 67g oraz art. 67h.

2. Obowiązków, o których mowa w art. 67c, art. 67d, art. 67g oraz art. 67h, nie stosuje się wobec podmiotów finansowych niebędących podmiotami kluczowymi lub podmiotami ważnymi, do których stosuje się przepis art. 16 ust. 1 rozporządzenia 2022/2554.

3. Nadzór nad wykonywaniem obowiązków, o których mowa w art. 67c, art. 67d, art. 67g oraz art. 67h, sprawuje organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowości i infrastruktury rynków finansowych.

4. Do nadzoru i kontroli wykonywania obowiązków, o których mowa w art. 67c, art. 67d, art. 67g oraz art. 67h, oraz do kar pieniężnych nakładanych za naruszenia tych obowiązków, stosuje się odpowiednio przepisy rozdziałów 11 i 14.

Art. 67l. 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.

2. Powierzając realizację wybranych zadań, o których mowa w art. 26, określa się w szczególności:

1) zakres powierzonych zadań;

2) czas realizacji powierzonych zadań, niedłuższy niż 1 rok, 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 wybranych zadań, o których mowa w art. 26, jest dokonywana przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych, z uwzględnieniem art. 12a ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2025 r. poz. 504 oraz z 2026 r. poz. 20).

4. Prezes Rady Ministrów wydaje komunikat o powierzeniu realizacji wybranych zadań, o których mowa w art. 26, i niezwłocznie ogłasza go w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski". Informacja o komunikacie jest publikowana również na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

Rozdział 13

Strategia

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

Art. 69. 1. Strategia określa:
1) cele strategiczne i cele szczegółowe oraz środki organizacyjne i regulacyjne, służące ich realizacji;
2) mechanizm służący określeniu istotnych zasobów i szacowania ryzyka związanego z cyberbezpieczeństwem;
3) zasady współpracy między sektorem publicznym i prywatnym;
4) podmioty zaangażowane we wdrażanie i realizację Strategii;
5) środki służące koordynacji i wymianie informacji pomiędzy organami właściwymi w sprawach cyberbezpieczeństwa a właściwymi organami na podstawie dyrektywy 2022/2557 na temat ryzyka, cyberzagrożeń i incydentów, a także ryzyka, zagrożeń i incydentów poza cyberprzestrzenią oraz wykonywania zadań nadzorczych;

6) działania w zakresie zwiększenia ogólnego poziomu wiedzy obywateli o cyberbezpieczeństwie;
7) cele i sposób realizacji interesów cyberbezpieczeństwa krajowego w wymiarze międzynarodowym.

2. Przy opracowaniu strategii uwzględnia się:

1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT, usług ICT i procesów ICT wykorzystywanych przez podmioty do świadczenia usług;
2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT, usług ICT i procesów ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień, w tym w odniesieniu do certyfikacji cyberbezpieczeństwa, szyfrowania oraz wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu;
3) rozwiązania dotyczące zarządzania podatnościami, obejmujące promowanie i ułatwianie skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy 2022/2555;
4) utrzymanie ogólnej dostępności, integralności i poufności publicznego rdzenia otwartego Internetu, w tym, w stosownych przypadkach, cyberbezpieczeństwa podmorskich kabli komunikacyjnych;
5) promowanie rozwoju i integracji odpowiednich zaawansowanych technologii służących wdrożeniu najnowocześniejszych środków zarządzania ryzykiem w cyberbezpieczeństwie;
6) kształcenie i szkolenia w dziedzinie cyberbezpieczeństwa, umiejętności z zakresu cyberbezpieczeństwa, rozwój i promocję kwalifikacji rynkowych w zakresie cyberbezpieczeństwa w przemyśle, podnoszenie świadomości oraz inicjatywy badawczo-rozwojowe, a także wytyczne dotyczące dobrych praktyk i kontroli w zakresie higieny cyfrowej;
7) wspieranie instytucji akademickich i naukowych, w opracowywaniu, usprawnianiu i propagowaniu wprowadzania narzędzi z zakresu cyberbezpieczeństwa oraz bezpiecznej infrastruktury sieciowej;
8) zapewnienie odpowiednich procedur oraz narzędzi służących wymianie informacji;

9) rozwiązania wzmacniające podstawowy poziom cyberodporności i higieny cyfrowej małych i średnich przedsiębiorstw;
10) rozwiązania wspierające aktywne działania w cyberprzestrzeni.

3. Strategia obejmuje sektory, o których mowa w załącznikach nr 1 i 2 do ustawy.

4. Strategia jest realizowana w oparciu o plan działań uwzględniający w szczególności koszty realizacji i źródła finansowania działań określonych w Strategii, a także podmioty odpowiedzialne i planowany termin realizacji poszczególnych działań. Plan działań stanowi załącznik do Strategii.

5. Strategia jest przyjmowana na okres pięcioletni z możliwością wprowadzania w niej zmian na podstawie wyników przeglądu i oceny, o których mowa w art. 71.

Art. 70. 1. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami, właściwymi kierownikami urzędów centralnych, a także właściwym organem w rozumieniu rozporządzenia 2022/2554.

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

3. Strategia jest ogłaszana w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 70a. 1. Podmioty, o których mowa w art. 69 ust. 1 pkt 4, przekazują na żądanie ministra właściwego do spraw informatyzacji informację o bieżącym stanie realizacji celów szczegółowych Strategii i działań określonych w planie działań.

2. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy i organ właściwy do spraw cyberbezpieczeństwa przekazują ministrowi właściwemu do spraw informatyzacji, w terminie do dnia 30 marca, informacje o realizacji celów Strategii w poprzednim roku i działań określonych w planie działań.

Art. 71. Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii i oceny jej skuteczności, nierzadziej niż co 2,5 roku.

Art. 72. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej Strategię w terminie 3 miesięcy od dnia jej przyjęcia przez Radę Ministrów.

Rozdział 13a

Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Art. 72a. Rada Ministrów przyjmuje, w drodze uchwały, Krajowy plan.

Art. 72b. 1. Krajowy plan określa cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę.

2. Krajowy plan zawiera w szczególności:

1) cele działań w zakresie zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę;
2) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie;
3) procedury zarządzania kryzysowego w cyberprzestrzeni oraz kanały wymiany informacji;
4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów w cyberbezpieczeństwie na dużą skalę, w tym ćwiczenia i szkolenia;
5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
6) kryteria oceny infrastruktury informatycznej pod kątem jej znaczenia dla zarządzania kryzysowego;
7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego Unii Europejskiej w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii Europejskiej oraz efektywnego wsparcia ze strony danego państwa członkowskiego Unii Europejskiej dla tego rodzaju skoordynowanego zarządzania;

8) postanowienia dotyczące zarządzania kryzysami i reagowania na nie w odniesieniu do transgranicznych przepływów energii elektrycznej, w rozumieniu art. 41 ust. 2 i 3 rozporządzenia 2024/1366;
9) uporządkowaną listę działań na rzecz ograniczenia ryzyka wystąpienia incydentu krytycznego w zakresie organizacyjnym i technicznym, z uwzględnieniem:
   a) hierarchii działań,
   b) ram czasowych ich realizacji,
   c) podmiotów wiodących oraz współpracujących przy ich wykonywaniu,
   d) sposobów finansowania oraz wysokości nakładów finansowych,
   e) oceny osiągniętych efektów oraz wniosków z wdrożonych działań.

Art. 72c. Podmioty realizujące zadania z zakresu zarządzania kryzysowego na żądanie ministra właściwego do spraw informatyzacji przekazują informację o bieżącym stanie realizacji zadań wynikających z Krajowego planu.

Art. 72d. 1. Projekt Krajowego planu opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, Rządowym Centrum Bezpieczeństwa, oraz z innymi ministrami, właściwymi kierownikami urzędów centralnych oraz z właściwym organem określonym w art. 52a ust. 1.

2. W pracach nad projektem uczestniczy przedstawiciel Prezydenta Rzeczypospolitej Polskiej.

3. Krajowy plan jest ogłaszany w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”.

Art. 72e. Krajowy plan podlega aktualizacji nierzadziej niż raz na dwa lata.

Art. 72f. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa ważne informacje związane z Krajowym planem, w szczególności procedury, o których mowa w art. 72b ust. 2 pkt 3, w terminie 3 miesięcy od dnia jego przyjęcia przez Radę Ministrów.

Rozdział 14

Przepisy o karach pieniężnych

Art. 73. 1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który:

1) nie uzupełnił w terminie brakujących danych w wykazie albo nie dokonał korekty danych pomimo wezwania, o którym mowa w art. 7b ust. 2 albo art. 7j ust. 3, albo art. 7k ust. 2, art. 7l ust. 3 pkt 2 albo art. 7m ust. 3;
2) nie przeprowadza systematycznego szacowania ryzyka wystąpienia incydentu lub nie zarządza tym ryzykiem, o którym mowa w art. 8 ust. 1 pkt 1;
3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi albo system ten nie zapewnia funkcjonalności lub nie spełnia wymogów, o których mowa w art. 8 ust. 1 albo 3;
4) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1;
5) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1;
6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4;
7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4a;
8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b;
9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4c;
10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5;
11) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 pkt 2;
12) nie usuwa podatności, o których mowa w art. 32 ust. 2;
13) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11, gdy korzystanie z tego systemu przy realizacji tych obowiązków jest wymagane;
14) uniemożliwia lub utrudnia wykonywanie kontroli, o których mowa w art. 53 ust. 2 pkt 1;
15) nie realizuje obowiązku, o którym mowa w art. 53c;
16) uniemożliwia lub utrudnia urzędnikowi monitorującemu, o którym mowa w art. 53 ust. 5 pkt 6, wykonywanie powierzonych mu zadań lub realizację uprawnień, o których mowa w art. 53d ust. 1;

17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1;
18) nie wykonuje obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5;
19) nie przekazuje informacji, o których mowa w art. 67d ust. 1;
20) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10;
21) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego;
22) nie przekazuje informacji, o których mowa w art. 67h.

1a. Organ właściwy do spraw cyberbezpieczeństwa, jeżeli przemawia za tym waga i znaczenie naruszonych przepisów, może nałożyć karę pieniężną na podmiot, który:

1) w terminie, o którym mowa w art. 7c ust. 1, nie złożył wniosku o wpis do wykazu;
2) nie wykonuje obowiązków, o których mowa w art. 9.

1b. Karze pieniężnej podlega także podmiot kluczowy lub podmiot ważny, którego działanie lub zaniechanie, o którym mowa w ust. 1 pkt 2, 4–12, 14–16, 18, 19 i 22 oraz ust. 1a pkt 2, miało charakter jednorazowy.

1c. Podmiot ważny będący podmiotem publicznym podlega karze pieniężnej, jeżeli nie wykonuje obowiązku, o którym mowa w art. 8 ust. 3.

1d. Przepisu ust. 1 pkt 13 nie stosuje się do Ministra Obrony Narodowej, urzędu go obsługującego oraz podmiotów podległych Ministrowi Obrony Narodowej i przez niego nadzorowanych.

2. (uchylony)

3. Wysokość kary pieniężnej nie może przekroczyć 10 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 2 % przychodów osiągniętych przez podmiot kluczowy z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary, przy czym zastosowanie ma kwota wyższa. Kara ta nie może być jednak niższa niż 20 000 zł.

3a. W przypadku gdy okres wykonywania działalności gospodarczej jest krótszy niż 12 miesięcy albo podmiot nie osiągnął przychodu za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 500 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary.

4. Wysokość kary pieniężnej nie może przekroczyć 7 000 000 euro, wyrażonej w złotych i ustalanej przy zastosowaniu kursu średniego ogłaszanego przez Narodowy Bank Polski obowiązującego w dniu 31 grudnia w roku poprzedzającym rok wydania decyzji o wymierzeniu kary lub 1,4 % przychodów osiągniętych przez podmiot ważny z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary. Kara ta nie może być jednak niższa niż 15 000 zł. Przepis ust. 3a stosuje się odpowiednio z zastrzeżeniem, że za podstawę wymiaru kary pieniężnej przyjmuje się równowartość kwoty 250 000 euro.

5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:

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

– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł.

Art. 73a. 1. Karze pieniężnej może podlegać kierownik podmiotu kluczowego lub podmiotu ważnego, który:

1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 7b ust. 4, art. 7c ust. 1, 3 lub art. 7f ust. 3,
2) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8,
3) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8d,
4) nie wykonuje obowiązku, o którym mowa w art. 8e,
5) nie wykonał obowiązku, o którym mowa w art. 8f ust. 1 lub 2,
6) nie wyznaczył co najmniej dwóch osób do kontaktu z podmiotami kluczowymi lub podmiotami ważnymi, albo w przypadku kierowania mikro- lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I

do rozporządzenia 651/2014/UE, co najmniej jednej osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa,

7) nie zapewnił użytkownikowi możliwości zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą,
8) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 10 ust. 1 i 6–8,
9) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 11,
10) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 12 ust. 5–8,
11) przekazał sprawozdanie końcowe, o którym mowa w art. 11 ust. 1 pkt 4c, niezawierające elementów określonych w art. 12a,
12) nie wykonuje obowiązku, o którym mowa w art. 12b,
13) nie wykonuje obowiązku, o którym mowa w art. 14,
14) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 15

– jeżeli przemawia za tym czas, zakres lub charakter naruszenia.

2. Karze pieniężnej może podlegać także kierownik podmiotu kluczowego lub podmiotu ważnego, którego zaniechanie w realizacji obowiązków, o których mowa w ust. 1, miało charakter jednorazowy.

3. Niezależnie od kary pieniężnej, o której mowa w art. 73 ust. 1, karę pieniężną można nałożyć również na kierownika podmiotu kluczowego lub podmiotu ważnego za niewykonanie obowiązków wskazanych w tym przepisie.

4. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 300 % otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.

5. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona kierownikowi podmiotu kluczowego lub podmiotu ważnego będącym podmiotem publicznym w kwocie nie większej niż 100 % otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop. W przypadku gdy podmiot kluczowy lub podmiot ważny będące podmiotem publicznym są zobowiązane do stosowania ustawy również na podstawie innego sektora wskazanego w załączniku nr 1 lub 2

do ustawy, do kar pieniężnych wymierzanych kierownikom tych podmiotów stosuje się przepis ust. 4.

Art. 73b. 1. Karze pieniężnej podlega:

1) podmiot świadczący usługi rejestracji nazw domen, który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
2) rejestr nazw domen najwyższego poziomu (TLD), który nie wykonuje obowiązków, o których mowa w art. 16b i art. 16c;
3) producent lub dostawca, który nie przekazał dokumentacji badanego produktu ICT lub usługi ICT na wezwanie CSIRT MON, CSIRT NASK lub CSIRT GOV;
4) podmiot, który nie przekazał informacji, o których mowa w art. 43 ust. 1;
5) dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej, który nie wyznaczył przedstawiciela zgodnie z art. 5a ust. 7.

2. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 1 i 5, jeżeli dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca chmury obliczeniowej, dostawca usług centrum przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowej platformy handlowej, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych jest:

1) podmiotem kluczowym – stosuje się przepis art. 73 ust. 3;
2) podmiotem ważnym – stosuje się przepis art. 73 ust. 4.

3. Do wysokości kary pieniężnej, o której mowa w ust. 1 pkt 2, stosuje się przepis art. 73 ust. 3.

4. Kara pieniężna, o której mowa w ust. 1 pkt 3 i 4, wynosi 50 000 zł.

Art. 73c. 1. Podmiot finansowy, który nie jest podmiotem kluczowym lub podmiotem ważnym oraz nie jest podmiotem określonym w art. 16 ust. 1 rozporządzenia 2022/2554, podlega karze pieniężnej, jeżeli:

1) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 67c ust. 1, 2, 4 i 5;
2) nie wdrożył w terminie określonym w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9 pkt 3, określonego zachowania, o którym mowa w art. 67g ust. 10;
3) odstąpił od wykonywania zawartego w poleceniu zabezpieczającym, o którym mowa w art. 67g ust. 9, określonego zachowania, o którym mowa w art. 67g ust. 10, przed wygaśnięciem polecenia zabezpieczającego.

2. Do wysokości kary pieniężnej, o której mowa w ust. 1, stosuje się przepis art. 73 ust. 3.

Art. 74. 1. Karę pieniężną, o której mowa w art. 73, art. 73a i art. 73b ust. 1 pkt 4 i 5, nakłada, w drodze decyzji, organ właściwy do spraw cyberbezpieczeństwa.

2. Karę pieniężną, o której mowa w art. 73b ust. 1 pkt 1–3, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

3. Karę pieniężną, o której mowa w art. 73c ust. 1, nakłada, w drodze decyzji, właściwy organ w rozumieniu rozporządzenia 2022/2554.

4. Organ właściwy do spraw cyberbezpieczeństwa lub właściwy organ w rozumieniu rozporządzenia 2022/2554 może decyzji, o której mowa w ust. 1 lub 3, nadać rygor natychmiastowej wykonalności w całości albo w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego.

5. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73–73c, 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.

6. Minister właściwy do spraw informatyzacji przekazuje Komisji Wspólnej Rządu i Samorządu Terytorialnego, do końca pierwszego kwartału danego roku, informację za rok poprzedni o wysokości wpływów z tytułu kar pieniężnych, nałożonych na samorządowe podmioty publiczne, stanowiących 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.

Art. 75. (uchylony)

Art. 76. (uchylony)

Art. 76a. 1. Organ właściwy do spraw cyberbezpieczeństwa, podejmując decyzję o nałożeniu kary pieniężnej i ustalając jej wysokość, uwzględnia odpowiednio kryteria określone w art. 53 ust. 12 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej, możliwości finansowe podmiotu kluczowego lub podmiotu ważnego będącego podmiotem publicznym albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego. Przepisu art. 189a § 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

2. W przypadku gdy podmiot kluczowy lub podmiot ważny powstał w wyniku połączenia lub przekształcenia innych podmiotów, obliczając wysokość jego przychodu organ właściwy do spraw cyberbezpieczeństwa uwzględnia przychód osiągnięty przez te podmioty w roku obrotowym poprzedzającym rok nałożenia kary pieniężnej. Przepisy art. 73 ust. 3–4 stosuje się odpowiednio.

3. W związku z toczącym się postępowaniem w sprawie nałożenia kary pieniężnej, podmiot, wobec którego wszczęto to postępowanie lub podmiot zatrudniający kierownika podmiotu kluczowego lub podmiotu ważnego jest obowiązany do dostarczenia organowi uprawnionemu do nałożenia kary pieniężnej na każde jego żądanie, w terminie wskazanym w wezwaniu, nie dłuższym niż 1 miesiąc od dnia otrzymania żądania, danych niezbędnych do określenia podstawy wymiaru kary pieniężnej.

4. W przypadku niedostarczenia danych lub dostarczenia danych uniemożliwiających ustalenie podstawy wymiaru kary pieniężnej, organ właściwy do spraw cyberbezpieczeństwa ustala podstawę wymiaru kary pieniężnej w sposób szacunkowy, uwzględniając w szczególności wielkość danego podmiotu kluczowego lub podmiotu ważnego, specyfikę działalności tego podmiotu lub ogólnodostępne dane finansowe.

5. Karę pieniężną uiszcza się w terminie 14 dni od dnia, w którym decyzja o jej wymierzeniu stała się ostateczna, lub od dnia doręczenia decyzji z rygorem natychmiastowej wykonalności, na rachunek bankowy organu właściwego do spraw cyberbezpieczeństwa, wskazany w decyzji o wymierzeniu kary pieniężnej.

6. Kary pieniężne nieuiszczone w terminie wraz z odsetkami podlegają ściągnięciu przez organ właściwy do spraw cyberbezpieczeństwa, który wymierzył karę pieniężną, w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

7. Organ właściwy do spraw cyberbezpieczeństwa przekazuje na rachunek Funduszu Cyberbezpieczeństwa środki pochodzące z kar pieniężnych w terminie 14 dni od dnia ich uiszczenia albo pobrania. W tym samym terminie przekazuje ministrowi właściwemu do spraw informatyzacji kopię decyzji o wymierzeniu kary pieniężnej lub innego dokumentu stanowiącego podstawę naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa kary pieniężnej lub odsetek od nieterminowej wpłaty.

8. Organ właściwy do spraw cyberbezpieczeństwa w terminie 14 dni od dnia wystąpienia zdarzenia mogącego skutkować zmianą lub uchyleniem decyzji lub innego dokumentu stanowiącego podstawę do naliczenia, pobrania i przekazania na rachunek Funduszu Cyberbezpieczeństwa środków pochodzących z kar pieniężnych, informuje ministra właściwego do spraw informatyzacji o tym zdarzeniu, a w szczególności o wniesieniu skargi do sądu administracyjnego, skargi kasacyjnej, wydaniu prawomocnego wyroku, wszczęciu lub zakończeniu postępowania administracyjnego w zakresie wznowienia postępowania, uchylenia, zmiany lub stwierdzenia nieważności decyzji.

9. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, jeżeli waga naruszenia i znaczenie naruszonych przepisów są znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

10. Do postępowania w sprawie nałożenia kar pieniężnych, o których mowa w art. 73b ust. 1 i art. 73c ust. 1, stosuje się odpowiednio przepisy ust. 1–9.

Art. 76b. 1. Niezależnie od kary pieniężnej nałożonej na podstawie art. 73 ust. 1, organ właściwy do spraw cyberbezpieczeństwa, w celu przymuszenia podmiotu kluczowego albo podmiotu ważnego do wykonania nałożonych na niego

obowiązków, może nałożyć na ten podmiot, w drodze decyzji, okresową karę pieniężną w wysokości od 500 zł do 100 000 złotych za każdy dzień opóźnienia, w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–8.

2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary.

3. Do okresowej kary pieniężnej stosuje się przepisy art. 74 ust. 4 i 5.

Art. 76c. 1. Jeżeli za czyn zagrożony karą określoną w art. 73 lub art. 73a została nałożona prawomocnie kara pieniężna przez Prezesa Urzędu Ochrony Danych Osobowych w związku z naruszeniem ochrony danych osobowych, organ właściwy do spraw cyberbezpieczeństwa nie wszczyna postępowania w sprawie nałożenia kary i poprzestaje na pouczeniu. Jeżeli zostało wszczęte postępowanie w sprawie nałożenia kary pieniężnej, stosuje się odpowiednio przepis art. 189f ust. 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

2. W przypadku, o którym mowa w ust. 1, organ właściwy do spraw cyberbezpieczeństwa może stosować środki nadzoru określone w art. 53 ust. 4, 5 i 9.

Art. 76d. 1. W przypadku, o którym mowa w art. 73 ust. 1 pkt 3, kara pieniężna może być nakładana w sposób określony w art. 14 § 1b ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

2. Do postępowania w sprawie nałożenia kary pieniężnej stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, z wyjątkiem przepisów o milczącym załatwieniu sprawy.

Art. 76e. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Rozdział 15

Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe

Art. 77–82. (pominięte)

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

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

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

1) wyznaczonych organach właściwych do spraw cyberbezpieczeństwa, Pojedynczym Punkcie Kontaktowym oraz o ich zadaniach;
2) zakresie zadań CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku incydentu.

Art. 86. Organy właściwe do spraw cyberbezpieczeństwa w terminie do dnia 9 listopada 2018 r. wydadzą decyzje o uznaniu za operatora usługi kluczowej oraz przekażą ministrowi właściwemu do spraw informatyzacji wnioski o wpisanie operatorów usług kluczowych do wykazu, o którym mowa w art. 7.

Art. 87. Minister właściwy do spraw informatyzacji w terminie do dnia 9 sierpnia 2018 r. przekaże Grupie Współpracy sprawozdanie podsumowujące o:

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

Art. 88. Minister właściwy do spraw informatyzacji w terminie do dnia 9 listopada 2018 r. przekaże Komisji Europejskiej informacje o:

1) krajowych środkach umożliwiających identyfikację operatorów usług kluczowych;
2) wykazie usług kluczowych;
3) liczbie zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o którym mowa w załączniku nr 1 do ustawy, ze wskazaniem ich znaczenia w odniesieniu do tego sektora;

4) progach istotności skutku zakłócającego dla świadczonej usługi kluczowej branych pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych.

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

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

Art. 91. 1. Roczny plan wdrożenia, o którym mowa w art. 32aa ust. 2 ustawy zmienianej w art. 79[17)], Szef Agencji Bezpieczeństwa Wewnętrznego opracuje po raz pierwszy na rok 2019.

2. Podmiot, który do dnia wejścia w życie ustawy przystąpił do realizowanego przez Agencję Bezpieczeństwa Wewnętrznego programu ARAKIS-GOV, uznaje się za podmiot, który przystąpił do systemu ostrzegania, w rozumieniu art. 32aa ust. 4 ustawy zmienianej w art. 79[17)].

3. Podmiot, o którym mowa w ust. 2, który do dnia wejścia w życie ustawy nie dokonał pełnego wdrożenia elementów systemu ostrzegania, w rozumieniu art. 32aa ust. 4 ustawy zmienianej w art. 79[17)] obowiązany jest do ich uzupełnienia w terminie roku od dnia wejścia w życie ustawy.

4. Zawarte przed dniem wejścia w życie ustawy porozumienia w sprawie udziału w programie ARAKIS-GOV uznaje się za porozumienia, o których mowa w art. 32aa ust. 7 ustawy zmienianej w art. 79[17)].

Art. 92. 1. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 77[18)] dotyczące realizacji danego programu rządowego przyjętego na podstawie art. 90u ust. 1 pkt 6 ustawy zmienianej w art. 77[18)], zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 77[18)] w brzmieniu nadanym niniejszą ustawą, dotyczących realizacji tego programu rządowego, nie dłużej jednak niż do dnia 31 marca 2021 r., i mogą być zmieniane.

---

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

18) Artykuł 77 zawiera zmiany do ustawy z dnia 7 września 1991 r. o systemie oświaty.

2. Dotychczasowe przepisy wykonawcze, wydane na podstawie art. 176a ust. 5 ustawy zmienianej w art. 81[19)], zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 176a ust. 5 ustawy zmienianej w art. 81[19)], jednak nie dłużej niż przez 24 miesiące od dnia wejścia w życie niniejszej ustawy.

3. Dotychczasowe przepisy wykonawcze, wydane na podstawie art. 5a ust. 6 ustawy zmienianej w art. 82[20)], zachowują moc do dnia wejścia w życie nowych przepisów wykonawczych wydanych na podstawie art. 5a ust. 6 ustawy zmienianej w art. 82[20)], jednak nie dłużej niż przez 12 miesięcy od dnia wejścia w życie niniejszej ustawy.

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

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

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – Gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 388 tys. zł;
3) w 2020 r. – 404 tys. zł;
4) w 2021 r. – 404 tys. zł;

19) Artykuł 81 zawiera zmiany do ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.
20) Artykuł 82 zawiera zmiany do ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

5) w 2022 r. – 404 tys. zł;
6) w 2023 r. – 404 tys. zł;
7) w 2024 r. – 404 tys. zł;
8) w 2025 r. – 404 tys. zł;
9) w 2026 r. – 404 tys. zł;
10) w 2027 r. – 404 tys. zł.

3. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – Informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 6450 tys. zł;
2) w 2019 r. – 13 349 tys. zł;
3) w 2020 r. – 17 334 tys. zł;
4) w 2021 r. – 17 314 tys. zł;
5) w 2022 r. – 27 404 tys. zł;
6) w 2023 r. – 50 335 tys. zł;
7) w 2024 r. – 50 335 tys. zł;
8) w 2025 r. – 80 300 tys. zł;
9) w 2026 r. – 91 400 tys. zł;
10) w 2027 r. – 50 335 tys. zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – Transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

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

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – Zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

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

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – Energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 758 tys. zł;
3) w 2020 r. – 789 tys. zł;
4) w 2021 r. – 789 tys. zł;
5) w 2022 r. – 789 tys. zł;
6) w 2023 r. – 789 tys. zł;
7) w 2024 r. – 789 tys. zł;
8) w 2025 r. – 789 tys. zł;
9) w 2026 r. – 789 tys. zł;
10) w 2027 r. – 789 tys. zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2018 r. – 0 zł;
2) w 2019 r. – 255 tys. zł;
3) w 2020 r. – 3605 tys. zł;
4) w 2021 r. – 5605 tys. zł;

5) w 2022 r. – 5605 tys. zł;
6) w 2023 r. – 9705 tys. zł;
7) w 2024 r. – 705 tys. zł;
8) w 2025 r. – 705 tys. zł;
9) w 2026 r. – 705 tys. zł;
10) w 2027 r. – 8705 tys. zł.

8. (uchylony)

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

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

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

1) w 2018 r. – 242 tys. zł;
2) w 2019 r. – 360 tys. zł;
3) w 2020 r. – 0 zł;
4) w 2021 r. – 0 zł;
5) w 2022 r. – 0 zł;
6) w 2023 r. – 0 zł;
7) w 2024 r. – 0 zł;
8) w 2025 r. – 0 zł;
9) w 2026 r. – 0 zł;
10) w 2027 r. – 0 zł.

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

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

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

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

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

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

16. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw gospodarki morskiej.

17. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw gospodarki wodnej.

18. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw informatyzacji.

19. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw transportu.

20. Minister właściwy do spraw ochrony zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw ochrony zdrowia.

21. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 11, dokonuje minister właściwy do spraw energii.

22. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i przynajmniej cztery razy do roku dokonuje, według stanu na koniec każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmu korygującego, o którym mowa w ust. 12, dokonuje Szef Agencji Bezpieczeństwa Wewnętrznego.

23. (uchylony)

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

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

Art. 94. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia[21)].

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

Załączniki do ustawy z
dnia 23 stycznia 2026 r.
(Dz. U. poz. 252)

Załącznik nr 1

SEKTORY KLUCZOWE

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Energia	Wydobywanie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną
		Podmioty, o których mowa w art. 3 pkt 28b ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 6e ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 59 i 59a ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Przedsiębiorcy odpowiedzialni za zarządzanie punktem ładowania i jego obsługę, świadczący usługę ładowania na rzecz użytkowników końcowych, w tym w imieniu i na rzecz dostawcy usług w zakresie mobilności
	Ciepło	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła
	Ropa i paliwa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o której mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych
		Agencja wykonawcza utworzona na podstawie ustawy z dnia 17 grudnia 2020 r. o rezerwach strategicznych (Dz. U. z 2024 r. poz. 1598 i 1907 oraz z 2026 r. poz. 203)
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw gazowych
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu magazynowania paliw gazowych
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego
		Przedsiębiorstwa energetyczne prowadzące działalność gospodarczą w zakresie rafinacji i przetwarzania gazu ziemnego
	Energetyka jądrowa	Podmiot będący operatorem obiektu energetyki jądrowej, określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących
	Wodór	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie przesyłania wodoru
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie magazynowania wodoru

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania wodoru
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie dystrybucji wodoru
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylającego rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE L 97 z 09.04.2008, str. 72)
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2025 r. poz. 1431 i 1668 oraz z 2026 r. poz. 176)
		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący zadania związane z kontrolą bezpieczeństwa
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2025 r. poz. 1234 oraz z 2026 r. poz. 41), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6, z późn. zm.[1)]), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2025 r. poz. 18)
		Podmiot zarządzający portem morskim, o którym mowa w art. 3 ust. 1 pkt 2 ustawy z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich (Dz. U. z 2024 r. poz. 597)

[1)] Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 161 z 20.06.2008 r., zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 29 z 31.01.2009, str. 53 oraz Dz. Urz. UE L 87 z 31.03.2009, str. 109.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski ujęte w klasie 52.22 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.[2)])
		VTS (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2025 r. poz. 883 i 1535)
	Transport drogowy	Zarządca drogi, o którym mowa w art. 19 ust. 2 pkt 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych
		Podmioty świadczące usługę ITS, o której mowa w art. 4 pkt 36 ustawy z dnia 21 marca 1985 r. o drogach publicznych
Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2026 r. poz. 38 i 176)
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2024 r. poz. 722, z późn. zm.[3)])
		Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Podmiot prowadzący ASO w rozumieniu art. 3 pkt 2 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Podmiot prowadzący OTF w rozumieniu art. 3 pkt 10b ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi
		Administratorzy kluczowych wskaźników referencyjnych
		Podmiot utworzony na podstawie art. 67 ustawy z dnia 29 sierpnia

[2)] Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 90785 z 06.12.2024, str. 1, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 97 z 09.04.2008, str. 13, Dz. Urz. UE L 198 z 25.07.2019, str. 241 oraz Dz. Urz. UE L 19 z 20.01.2023, str. 5.

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1863, z 2025 r. poz. 146, 820, 923, 1014, 1069, 1216 i 1556 oraz z 2026 r. poz. 176.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		1997 r. – Prawo bankowe
		Podmiot, o którym mowa w art. 3 pkt 21a ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi mający siedzibę na terytorium Rzeczypospolitej Polskiej
Ochrona zdrowia	Udzielanie świadczeń zdrowotnych i zdrowie publiczne	Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2026 r. poz. 156)
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz. Urz. UE L 314 z 06.12.2022, str. 1)
		Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia
		Urzędy obsługujące organy Państwowej Inspekcji Sanitarnej
		Krajowe Centrum Monitorowania Ratownictwa Medycznego, o którym mowa w art. 27a ustawy z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2026 r. poz. 141)
		Jednostki organizacyjne publicznej służby krwi, o których mowa w art. 4 ust. 3 pkt 2 ustawy z dnia 22 sierpnia 1997 r. o publicznej służbie krwi (Dz. U. z 2024 r. poz. 1782)
		Podmioty udzielające świadczeń opieki zdrowotnej będące podwykonawcą dla podmiotów kluczowych lub podmiotów ważnych w sektorze ochrona zdrowia, w rozumieniu art. 133 ustawy z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz. U. z 2025 r. poz. 1461, 1537 i 1739 oraz z 2026 r. poz. 26 i 203)
		Świadczeniodawcy posiadający w swojej strukturze organizacyjnej Szpitalny Oddział Ratunkowy, Centrum Urazowe lub Centrum Urazowe dla Dzieci
	Produkcja i dystrybucja substancji czynnych, produktów leczniczych i wyrobów medycznych	Urząd Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych
		Urzędy obsługujące organy Inspekcji Farmaceutycznej
		Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy 2001/83/WE Parlamentu Europejskiego i Rady z dnia 6 listopada 2001 r. w sprawie wspólnotowego kodeksu odnoszącego się do produktów leczniczych stosowanych u ludzi (Dz. Urz. UE L 311 z 28.11.2001, str. 67, z późn. zm.[4)])
		Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2

[4)] Sprostowanie wymienionej dyrektywy zostało ogłoszone w Dz. Urz. UE L 230 z 24.08.2006, str. 12, Dz. Urz. UE L 87 z 31.03.2009, str. 174, Dz. Urz. UE L 276 z 21.10.2011, str. 63 oraz Dz. Urz. UE L 131 z 22.05.2012, str. 11, zmiany wymienionej dyrektywy zostały ogłoszone w Dz. Urz. UE L 33 z 08.02.2003, str. 30, Dz. Urz. UE L 159 z 27.06.2003, str. 46, Dz. Urz. UE L 136 z 30.04.2004, str. 34 i 85, Dz. Urz. UE L 378 z 27.12.2006, str. 1, Dz. Urz. UE L 324 z 10.12.2007, str. 121, Dz. Urz. UE L 81 z 20.03.2008, str. 51, Dz. Urz. UE L 168 z 30.06.2009, str. 33, Dz. Urz. UE L 242 z 15.09.2009, str. 3, Dz. Urz. UE L 348 z 31.12.2010, str. 74, Dz. Urz. UE L 174 z 01.07.2011, str. 74, Dz. Urz. UE L 299 z 27.10.2012, str. 1, Dz. Urz. UE L 117 z 05.05.2017, str. 1, Dz. Urz. UE L 4 z 07.01.2019, str. 24, Dz. Urz. UE L 198 z 25.07.2019, str. 241, Dz. Urz. UE L 118 z 20.04.2022, str. 4 oraz Dz. Urz. UE L 157 z 20.06.2023, str. 1.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Podmioty produkujące wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego („wykaz wyrobów medycznych o krytycznym znaczeniu w przypadku stanu zagrożenia zdrowia publicznego") w rozumieniu art. 22 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/123 z dnia 25 stycznia 2022 r. w sprawie wzmocnienia roli Europejskiej Agencji Leków w zakresie gotowości na wypadek sytuacji kryzysowej i zarządzania kryzysowego w odniesieniu do produktów leczniczych i wyrobów medycznych (Dz. Urz. UE L 20 z 31.01.2022, str. 1, z późn. zm.[5)])
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2025 r. poz. 750, 905, 924, 1416, 1537 i 1795)
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego
		Importer produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Wytwórca produktu leczniczego lub substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne
Zaopatrzenie w wodę pitną i jej dystrybucja		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2024 r. poz. 757), z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności
Zbiorowe odprowadzanie ścieków		Podmiot odprowadzający lub oczyszczający ścieki, w tym przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków, z wyłączeniem podmiotów, dla których odprowadzanie lub oczyszczanie ścieków jest inną niż istotna częścią ich ogólnej działalności
Infrastruktura cyfrowa	Infrastruktura cyfrowa z wyłączeniem komunikacji elektronicznej	Dostawca punktu wymiany ruchu internetowego
		Dostawca usług DNS, z wyłączeniem operatorów głównych serwerów nazw
		Rejestr nazw domen najwyższego poziomu (TLD)
		Dostawca chmury obliczeniowej

[5)] Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 71 z 09.03.2023, str. 37, zmiana wymienionego rozporządzenia została ogłoszona w Dz. Urz. UE L 2024/568 z 14.02.2024.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		Dostawca usług centrum przetwarzania danych
		Dostawca sieci dostarczania treści
		Dostawca usług zaufania
		Podmiot świadczący usługę rejestracji nazw domen
	Komunikacja elektroniczna	Przedsiębiorca komunikacji elektronicznej
Zarządzanie usługami ICT		Dostawca usług zarządzanych
		Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem operatora, o którym mowa w art. 2 pkt 40 lit. b ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej
		Polska Agencja Kosmiczna
Podmioty publiczne		1) Podmioty z uwzględnieniem pkt 2–4: a) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, oraz urzędy je obsługujące, b) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 3, 5–6, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, c) państwowe instytucje kultury, d) instytuty badawcze, e) Narodowy Bank Polski, f) Bank Gospodarstwa Krajowego, g) Urząd Dozoru Technicznego, h) Polska Agencja Żeglugi Powietrznej, i) Polskie Centrum Akredytacji, j) Urząd Komisji Nadzoru Finansowego, k) Polska Agencja Prasowa, l) Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. z 2025 r. poz. 960 i 1535), m) Polski Fundusz Rozwoju i inne instytucje rozwoju, o których mowa w art. 2 ust. 1 pkt 1 i 3–6 ustawy z dnia 4 lipca 2019 r. o systemie instytucji rozwoju, n) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej, o) wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, p) Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych, q) Zakład Unieszkodliwiania Odpadów Promieniotwórczych z siedzibą w Otwocku-Świerku, r) państwowa osoba prawna, wobec której wydano decyzję, o której mowa w art. 7m, s) spółka, o której mowa w art. 2 ust. 1 ustawy z dnia 29 kwietnia 2016 r. o szczególnych zasadach wykonywania niektórych zadań dotyczących informatyzacji w zakresie działów administracji

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
		rządowej budżet i finanse publiczne
		2) w odniesieniu do samorządu województwa: jednostki budżetowe oraz zakłady budżetowe z wyłączeniem: a) jednostek organizacyjnych, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe (Dz. U. z 2025 r. poz. 1043, 1160 i 1837 oraz z 2026 r. poz. 187 i 203), oraz ich zespołów, b) jednostek organizacyjnych wspierania rodziny i systemu pieczy zastępczej, o których mowa w art. 2 ust. 3 ustawy z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej (Dz. U. z 2025 r. poz. 49 i 1301 oraz z 2026 r. poz. 187 i 203), c) jednostek organizacyjnych, o których mowa w art. 6 pkt 5 ustawy z dnia 12 marca 2004 r. o pomocy społecznej, oprócz regionalnych ośrodków polityki społecznej, d) wojewódzkich urzędów pracy, e) parków krajobrazowych i ich zespołów, f) jednostek obsługujących, o których mowa w art. 8d ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, w zakresie, w jakim prowadzą wspólną obsługę jednostek, o których mowa w lit. a–e
		3) w odniesieniu do samorządu powiatu: starostwo powiatowe
		4) w odniesieniu do samorządu gminy: urząd gminy, jeżeli zatrudnia na dzień 1 stycznia danego roku w przeliczeniu na pełny wymiar czasu pracy na podstawie umowy o pracę co najmniej 50 osób

Załącznik nr 2

SEKTORY WAŻNE

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Usługi pocztowe		Operator pocztowy, o którym mowa w art. 3 pkt 12 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2025 r. poz. 366, 820 i 1456)
Inwestycje energetyki jądrowej		Podmiot będący inwestorem obiektu energetyki jądrowej określonego w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących, który uzyskał decyzję zasadniczą, o której mowa w art. 3a ust. 1 tej ustawy
Gospodarowanie odpadami	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach (Dz. U. z 2023 r. poz. 1587, z późn. zm.[6)]), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. z 2024 r. poz. 1799 oraz z 2025 r. poz. 1792)
	Transport odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na transporcie odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
	Przetwarzanie odpadów, w tym sortowanie, wraz z nadzorem nad wymienionymi działaniami, a także późniejsze postępowanie z miejscami unieszkodliwiania odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na przetwarzaniu odpadów, w tym sortowaniu, wraz z nadzorem nad wymienionymi działaniami, a także podmioty świadczące usługi z późniejszym postępowaniem z miejscami unieszkodliwiania odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
	Działania wykonywane w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, polegające na działaniach wykonywanych w charakterze sprzedawcy odpadów lub pośrednika w obrocie odpadami, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy z dnia 14 grudnia 2012 r. o odpadach, z wyłączeniem przedsiębiorstw, dla których usługi te nie stanowią podstawowej działalności gospodarczej określonej zgodnie z przepisami wydanymi na podstawie art. 40 ust. 2 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej
Produkcja,		Przedsiębiorstwa zajmujące się produkcją substancji oraz

[6)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1597, 1688, 1852 i 2029, z 2024 r. poz. 1834, 1911 i 1914, z 2025 r. poz. 1812 oraz z 2026 r. poz. 174.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
wytwarzanie i dystrybucja chemikaliów		dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniającego dyrektywę 1999/45/WE oraz uchylającego rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE (Dz. Urz. UE L 396 z 30.12.2006, str. 1, z późn. zm.[7)])
		Przedsiębiorstwa zajmujące się wytwarzaniem z substancji lub mieszanin wyrobów, o których mowa w art. 3 pkt 3 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2006 r. w sprawie rejestracji, oceny, udzielania zezwoleń i stosowanych ograniczeń w zakresie chemikaliów (REACH) i utworzenia Europejskiej Agencji Chemikaliów, zmieniającego dyrektywę 1999/45/WE oraz uchylającego rozporządzenie Rady (EWG) nr 793/93 i rozporządzenie Komisji (WE) nr 1488/94, jak również dyrektywę Rady 76/769/EWG i dyrektywy Komisji 91/155/EWG, 93/67/EWG, 93/105/WE i 2000/21/WE

[7)] Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 136 z 29.05.2007, str. 3, Dz. Urz. UE L 141 z 31.05.2008, str. 22, Dz. Urz. UE L 36 z 05.02.2009, str. 84, Dz. Urz. UE L 118 z 12.05.2010, str. 89, Dz. Urz. UE L 260 z 02.10.2010, str. 22, Dz. Urz. UE L 49 z 24.02.2011, str. 52, Dz. Urz. UE L 136 z 24.05.2011, str. 105, Dz. Urz. UE L 331 z 18.11.2014, str. 41, Dz. Urz. UE L 12 z 17.01.2017, str. 97, Dz. Urz. UE L 102 z 23.04.2018, str. 99, Dz. Urz. UE L 249 z 04.10.2018, str. 19 i 18, Dz. Urz. UE L 141 z 05.05.2020, str. 37, Dz. Urz. UE L 83 z 10.03.2022, str. 64 oraz Dz. Urz. UE L 2025/90479 z 06.06.2025, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 304 z 22.11.2007, str. 1, Dz. Urz. UE L 268 z 09.10.2008, str. 14, Dz. Urz. UE L 353 z 31.12.2008, str. 1, Dz. Urz. UE L 46 z 17.02.2009, str. 3, Dz. Urz. UE L 164 z 26.06.2009, str. 7, Dz. Urz. UE L 86 z 01.04.2010, str. 7, Dz. Urz. UE L 133 z 31.05.2010, str. 1, Dz. Urz. UE L 44 z 18.02.2011, str. 2, Dz. Urz. UE L 58 z 03.03.2011, str. 27, Dz. Urz. UE L 69 z 16.03.2011, str. 3 i 7, Dz. Urz. UE L 101 z 15.04.2011, str. 12, Dz. Urz. UE L 134 z 21.05.2011, str. 2, Dz. Urz. UE L 37 z 10.02.2012, str. 1, Dz. Urz. UE L 41 z 15.02.2012, str. 1, Dz. Urz. UE L 128 z 16.05.2012, str. 1, Dz. Urz. UE L 252 z 19.09.2012, str. 1 i 4, Dz. Urz. UE L 253 z 20.09.2012, str. 1 i 5, Dz. Urz. UE L 43 z 14.02.2013, str. 24, Dz. Urz. UE L 108 z 18.04.2013, str. 1, Dz. Urz. UE L 158 z 10.06.2013, str. 1, Dz. Urz. UE L 328 z 07.12.2013, str. 69, Dz. Urz. UE L 90 z 26.03.2014, str. 1, Dz. Urz. UE L 93 z 28.03.2014, str. 24, Dz. Urz. UE L 136 z 09.05.2014, str. 19, Dz. Urz. UE L 244 z 19.08.2014, str. 6, Dz. Urz. UE L 50 z 21.02.2015, str. 1, Dz. Urz. UE L 58 z 03.03.2015, str. 43, Dz. Urz. UE L 104 z 23.04.2015, str. 2, Dz. Urz. UE L 132 z 29.05.2015, str. 8, Dz. Urz. UE L 233 z 05.09.2015, str. 2, Dz. Urz. UE L 9 z 14.01.2016, str. 1, Dz. Urz. UE L 40 z 17.02.2016, str. 5, Dz. Urz. UE L 144 z 01.06.2016, str. 27, Dz. Urz. UE L 165 z 23.06.2016, str. 4, Dz. Urz. UE L 166 z 24.06.2016, str. 1, Dz. Urz. UE L 255 z 21.09.2016, str. 14, Dz. Urz. UE L 337 z 13.12.2016, str. 3, Dz. Urz. UE L 35 z 10.02.2017, str. 6, Dz. Urz. UE L 104 z 20.04.2017, str. 8, Dz. Urz. UE L 150 z 14.06.2017, str. 7 i 14, Dz. Urz. UE L 224 z 31.08.2017, str. 110, Dz. Urz. UE L 6 z 11.01.2018, str. 45, Dz. Urz. UE L 99 z 19.04.2018, str. 3 i 7, Dz. Urz. UE L 114 z 04.05.2018, str. 4, Dz. Urz. UE L 256 z 12.10.2018, str. 1, Dz. Urz. UE L 308 z 04.12.2018, str. 1, Dz. Urz. UE L 322 z 18.12.2018, str. 14, Dz. Urz. UE L 154 z 12.06.2019, str. 37, Dz. Urz. UE L 186 z 11.07.2019, str. 1, Dz. Urz. UE L 259 z 10.10.2019, str. 9, Dz. Urz. UE L 35 z 07.02.2020, str. 1, Dz. Urz. UE L 110 z 08.04.2020, str. 1, Dz. Urz. UE L 203 z 26.06.2020, str. 28, Dz. Urz. UE L 252 z 04.08.2020, str. 24, Dz. Urz. UE L 423 z 15.12.2020, str. 6, Dz. Urz. UE L 425 z 16.12.2020, str. 3, Dz. Urz. UE L 431 z 21.12.2020, str. 38, Dz. Urz. UE L 24 z 26.01.2021, str. 19, Dz. Urz. UE L 216 z 18.06.2021, str. 121, Dz. Urz. UE L 259 z 21.07.2021, str. 1, Dz. Urz. UE L 282 z 05.08.2021, str. 29, Dz. Urz. UE L 415 z 22.11.2021, str. 16, Dz. Urz. UE L 418 z 24.11.2021, str. 6, Dz. Urz. UE L 446 z 14.12.2021, str. 34, Dz. Urz. UE L 98 z 25.03.2022, str. 38, Dz. Urz. UE L 112 z 11.04.2022, str. 6, Dz. Urz. UE L 123 z 08.05.2023, str. 1, Dz. Urz. UE L 149 z 09.06.2023, str. 49, Dz. Urz. UE L 180 z 17.07.2023, str. 12, Dz. Urz. UE L 238 z 27.09.2023, str. 67, Dz. Urz. UE L 2023/2482 z 14.11.2023, Dz. Urz. UE L 2024/1328 z 17.05.2024, Dz. Urz. UE L 2024/2462 z 20.09.2024, Dz. Urz. UE L 2024/2929 z 28.11.2024, Dz. Urz. UE L 2025/660 z 02.04.2025, Dz. Urz. UE L 2025/1090 z 03.06.2025 oraz Dz. Urz. UE L 2025/1731 z 11.08.2025.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
Produkcja, przetwarzanie i dystrybucja żywności		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady z dnia 28 stycznia 2002 r. ustanawiającego ogólne zasady i wymagania prawa żywnościowego, powołującego Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiającego procedury w zakresie bezpieczeństwa żywności (Dz. Urz. UE L 31 z 01.02.2002, str. 1, z późn. zm.[8)]), zajmujące się dystrybucją hurtową oraz przemysłowymi produkcją i przetwarzaniem
Produkcja	Produkcja wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro	Podmioty produkujące wyroby medyczne w rozumieniu art. 2 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG (Dz. Urz. UE L 117 z 05.05.2017, str. 1, z późn. zm.[9)])
		Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych do diagnostyki *in vitro* oraz uchylenia dyrektywy 98/79/WE i decyzji Komisji 2010/227/UE (Dz. Urz. UE L 117 z 05.05.2017, str. 176, z późn. zm.[10)]), z wyjątkiem podmiotów produkujących wyroby medyczne uznane za mające krytyczne znaczenie podczas danego stanu zagrożenia zdrowia publicznego
	Produkcja komputerów, wyrobów elektronicznych i optycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 26 klasyfikacji NACE Rev. 2, ujętej w załączniku I do rozporządzenia (WE) nr 1893/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie statystycznej klasyfikacji działalności gospodarczej NACE Rev. 2 i zmieniającego rozporządzenie Rady (EWG) nr 3037/90 oraz niektóre rozporządzenia WE w sprawie określonych dziedzin statystycznych (Dz. Urz. UE L 393 z 30.12.2006, str. 1, z późn. zm.[11)])
	Produkcja urządzeń elektrycznych	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 27 klasyfikacji NACE Rev. 2
	Produkcja maszyn i urządzeń,	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C

8) Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 179 z 07.07.2007, str. 59, Dz. Urz. UE L 327 z 12.11.2014, str. 9 oraz Dz. Urz. UE L 37 z 13.02.2015, str. 24, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 245 z 29.09.2003, str. 4, Dz. Urz. UE L 100 z 08.04.2006, str. 3, Dz. Urz. UE L 60 z 05.03.2008, str. 17, L 188 z 18.07.2009, str. 14, Dz. Urz. UE L 189 z 27.06.2014, str. 1, Dz. Urz. UE L 35 z 10.02.2017, str. 10, Dz. Urz. UE L 117 z 05.05.2017, str. 1, Dz. Urz. UE L 198 z 25.07.2019, str. 241, Dz. Urz. UE L 231 z 06.09.2019, str. 1 oraz Dz. Urz. UE L 2024/908 z 20.03.2024.

9) Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 117 z 03.05.2019, str. 9, Dz. Urz. UE L 334 z 27.12.2019, str. 165 oraz Dz. Urz. UE L 241 z 08.07.2021, str. 7, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 130 z 24.04.2020, str. 18, Dz. Urz. UE L 70 z 08.03.2023, str. 1, Dz. Urz. UE L 80 z 20.03.2023, str. 24, Dz. Urz. UE L 2024/568 z 14.02.2024 oraz Dz. Urz. UE L 2024/1860 z 09.07.2024.

10) Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 117 z 03.05.2019, str. 11, Dz. Urz. UE L 334 z 27.12.2019, str. 167 oraz Dz. Urz. UE L 233 z 01.07.2021, str. 9, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 19 z 28.01.2022, str. 3, Dz. Urz. UE L 70 z 08.03.2023, str. 3, Dz. Urz. UE L 80 z 20.03.2023, str. 24 oraz Dz. Urz. UE L 2024/1860 z 09.07.2024.

11) Sprostowanie wymienionego rozporządzenia zostało ogłoszone w Dz. Urz. UE L 2024/90785 z 06.12.2024, zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 97 z 09.04.2008, str. 13, Dz. Urz. UE L 198 z 25.07.2019, str. 241 oraz Dz. Urz. UE L 19 z 20.01.2023, str. 5.

I	II	III
Sektor	Podsektor	Rodzaj podmiotu
	gdzie indziej niesklasyfikowana	dział 28 klasyfikacji NACE Rev. 2
	Produkcja pojazdów samochodowych, przyczep i naczep	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 29 klasyfikacji NACE Rev. 2
	Produkcja pozostałego sprzętu transportowego	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C dział 30 klasyfikacji NACE Rev. 2
Dostawcy usług cyfrowych		Dostawca internetowej platformy handlowej
		Dostawca wyszukiwarki internetowej
		Dostawca platformy sieci usług społecznościowych
Badania naukowe		Organizacja badawcza
		Podmioty, o których mowa w art. 7 ust. 1 pkt 1–4, 6–7 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce
Podmioty publiczne		samorządowe jednostki budżetowe; samorządowe zakłady budżetowe; samorządowe instytucje kultury; spółki wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679)

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 alokacja zasobów radiowych	Radio Base Station Baseband Unit and other features such as Radio Units and antennas
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

Załącznik nr 4

WYMOGI DLA SYSTEMU ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI DLA PODMIOTU WAŻNEGO BĘDĄCEGO PODMIOTEM PUBLICZNYM

I. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym obejmuje co najmniej:

1) inwentaryzację produktów ICT, usług ICT i procesów ICT służących do przetwarzania informacji;

2) kontrolowanie podstawowych wersji używanego produktów ICT lub usług ICT, a jeżeli to możliwe, korzystanie z mechanizmów kontroli instalacji produktów ICT lub usług ICT na urządzeniach, w tym na urządzeniach mobilnych;

3) zapewnienie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, w zakresie:

   a) ochrony fizycznej miejsc, w których jest przetwarzana informacja, w przypadku przetwarzania danych w urządzeniach znajdujących się pod kontrolą podmiotu,

   b) ochrony wykorzystującej oprogramowanie zabezpieczające lub sprzętowe zabezpieczenia, w które są wyposażone urządzenia przetwarzające informacje, albo

   c) udokumentowania mechanizmów zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami w przypadku korzystania z usług dostawcy chmury obliczeniowej lub dostawcy usługi centrum przetwarzania danych;

4) dopuszczenie do informacji wyłącznie osób posiadających stosowne uprawnienia do systemów informacyjnych (w tym systemów operacyjnych, usług sieciowych i aplikacji) oraz zapewnienie środków uniemożliwiających nieautoryzowany dostęp do tych systemów;

5) stosowanie zasad przyznania minimalnych uprawnień niezbędnych dla realizacji zadań;

6) bezzwłoczne cofanie przyznanych uprawnień w przypadku stwierdzenia braku podstawy dostępu do informacji na stałe lub zawieszanie uprawnień w przypadku niewykonywania obowiązków co najmniej przez jeden miesiąc;

7) modyfikację zakresu przyznanych uprawnień, jeżeli jest to zasadne z uwagi na zmianę charakteru wykonywanych zadań i zakresu dostępu do informacji;

8) ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;

9) kontrolę usług poczty elektronicznej wykorzystującej mechanizmy, o których mowa w art. 24 ust. 1 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej;

10) wykonywanie zapasowych kopii danych odseparowanych logicznie i fizycznie od danych przetwarzanych w systemach informacyjnych dla realizacji zadania publicznego;

11) testowanie pod kątem kompletności i możliwości odtworzenia danych zawartych w zapasowych kopiach;

12) przygotowanie i testowanie procedury w przypadku wystąpienia awarii lub incydentu;

13) stosowanie oprogramowania antywirusowego;

14) stosowanie zasad cyberhigieny przez pracowników korzystających z systemów informacyjnych, w tym kierownika podmiotu;

15) monitorowanie częstotliwości wydawania kolejnych wersji produktów ICT, źródeł dystrybucji produktów ICT oraz cyklu życia produktów ICT w celu zapewnienia bezpieczeństwa systemu informacyjnego;

16) stosowanie stabilnych wersji produktów ICT lub usług ICT, w stosunku do których nie występują informacje o krytycznych podatnościach, a w przypadku ich wystąpienia dopuszczalne jest stosowanie tych wersji produktów ICT lub usług ICT, które nie stwarzają istotnego negatywnego wpływu na poziom bezpieczeństwa systemów informacyjnych;

17) stosowanie środków minimalizujących wystąpienie incydentów przez szkolenie osób zaangażowanych w proces przetwarzania informacji, ze szczególnym uwzględnieniem takich zagadnień, jak:

   a) rodzaje cyberzagrożeń,

   b) podstawowe zasady cyberhigieny,

   c) reagowania na wystąpienie incydentu,

   d) świadomość skutków naruszenia zasad bezpieczeństwa informacji;

18) określenie procedur i zasad działania podmiotu na wypadek wystąpienia cyberzagrożenia lub w przypadku wystąpienia incydentu.

II. System zarządzania bezpieczeństwem informacji dla podmiotu ważnego będącego podmiotem publicznym może dodatkowo obejmować:

1) stosowanie środków zapewniających bezpieczeństwo informacji, w tym produktów ICT, usług ICT lub procesów ICT minimalizujących ryzyko błędów ludzkich;

2) stosowanie dedykowanych usług poczty elektronicznej dla podmiotu na podstawie umowy lub w ramach wspólnego wykonywania obowiązków z zakresu cyberbezpieczeństwa przy pomocy jednostki wyznaczonej, o której mowa w art. 16e ust. 1;
3) zapewnienie wysokiej dostępności systemów informacyjnych:
   a) w zakresie określenia czasu dostępu do systemów informacyjnych,
   b) przez zapewnianie zdolności działania systemu informacyjnego i jego dostępności niezależnie od wystąpienia awarii lub incydentu;
4) określanie i kontrolowanie zasad korzystania przez podmiotu publicznego będącego podmiotem ważnym z:
   a) ogólnodostępnych usług dostawców chmury obliczeniowej,
   b) usług ogólnodostępnych dużych generatywnych modeli sztucznej inteligencji;
5) monitorowanie dostępu do informacji oraz stanu działania systemów informacyjnych za pomocą dedykowanego oprogramowania wykorzystywanego przez pracowników albo korzystanie w tym zakresie z usług dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa;
6) testowanie poziomów bezpieczeństwa systemów informacyjnych oraz zasad cyberhigieny przez pracowników;
7) zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa systemów informacyjnych;
8) zapewnienie aktualności wykorzystywanych produktów ICT oraz usług ICT;
9) stosowanie dodatkowych środków technicznych i organizacyjnych, jeżeli jest to konieczne dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów informacyjnych.

III. Podmiot ważny będący podmiotem publicznym dokonuje przeglądu systemu zarządzania bezpieczeństwem informacji:
1) co najmniej raz w roku albo
2) bezzwłocznie w przypadku wydania przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa rekomendacji, w zakresie, w jakim dotyczy ona systemów informacyjnych, produktów ICT lub usług ICT podmiotu, albo
3) bezzwłocznie w przypadku wystąpienia okoliczności, które mogą wpłynąć na ryzyko wystąpienia incydentu poważnego i wymagających ponownego zrealizowania działań opisanych w przyjętym systemie zarządzania bezpieczeństwie informacji lub zmian w samym systemie.

IV. Podmiot ważny będący podmiotem publicznym dokumentuje realizację działań wskazanych do realizacji w systemie zarządzania cyberbezpieczeństwa.