Projekt z dnia 23 kwietnia 2024

U S T A W A

z dnia … 2024 r.

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

Art. 1. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703) wprowadza się następujące zmiany:

1) w art. 1:
   a) w ust. 1 w pkt 3 kropkę zastępuje się średnikiem i dodaje pkt 4 w brzmieniu:
      „4) zakres Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę.”,
   b) w ust. 2 uchyla się pkt 1 i 2;
2) w art. 2:
   a) po pkt 3 dodaje się pkt 3a–3c w brzmieniu:
      „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) 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 2023 r. poz. 285, 1860 i 2699), wpisany do bazy adresów elektronicznych, o której mowa w art. 25 tej ustawy;
      3c) bezpieczeństwo systemów informacyjnych – odporność systemów informacyjnych na zdarzenia naruszające poufność, integralność, dostępność

[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)] Niniejszą ustawą zmienia się ustawy: ustawię z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych, ustawę z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, ustawę z dnia 6 marca 2018 r. – Prawo przedsiębiorców, ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych oraz ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;”,

b) pkt 4 otrzymuje brzmienie:

„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), zwanym dalej „rozporządzeniem 2019/881”;”,

c) po pkt 4 dodaje się pkt 4a–4k w brzmieniu:

„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 sieci rozproszonych geograficznie serwerów służących zapewnieniu wysokiej i łatwej dostępności treści i usług cyfrowych lub ich szybkiego dostarczania na rzecz użytkowników internetu w imieniu dostawców treści i usług;

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.[3)]), produktu ICT, usługi ICT lub procesu ICT;

4d) dostawca internetowej platformy handlowej – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi, umożliwiające konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową;

---

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

4e) dostawca usług chmurowych – osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która świadczy usługi umożliwiające dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników;

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

4g) dostawca usługi ośrodka 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;

4h) 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 poprzez wsparcie lub aktywną administrację przeprowadzane u usługobiorcy lub zdalnie;

4i) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa – dostawca usług zarządzanych, który świadczy usługi związane z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa lub zapewnia pomoc dla tych działań;

4j) dostawca usług zaufania – dostawca 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”;

4k) 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);”,

d) pkt 5 otrzymuje brzmienie:

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

e) pkt 7 i 8 otrzymują brzmienie:

„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 organizacyjnej nieposiadające osobowości prawnej poprzez wywołanie szkody materialnej lub niematerialnej;

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

f) po pkt 8 dodaje się pkt 8a w brzmieniu:

„8a) kierownik podmiotu kluczowego lub podmiotu ważnego – kierownik jednostki w rozumieniu art. 3 pkt 6 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295 i 1598) kierujący podmiotem kluczowym lub podmiotem ważnym;”,

g) uchyla się pkt 9,

h) po pkt 10 dodaje się pkt 10a w brzmieniu:

„10a) organizacja badawcza – osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która prowadzi 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 2023 r. poz. 742, z późn. zm.[4)]).”,

i) pkt 11 otrzymuje brzmienie:

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

---

[4)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2023 r. poz. 1088, 1234, 1672, 1872 i 2005 oraz z 2024 r. poz. 124 i 227.

j) po pkt 11 dodaje się pkt 11a–11k w brzmieniu:

„11a) platforma sieci usług społecznościowych – usługę świadczoną drogą elektroniczną w rozumieniu przepisów ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), która umożliwia użytkownikom końcowym łączenie się z innymi osobami oraz komunikowanie się i wymianę, udostępnianie i odkrywanie treści za pomocą wielu urządzeń;

11b) podmiot publiczny – podmiot wskazany w załączniku nr 1 do ustawy w sektorze administracji publicznej;

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 uchylająca dyrektywę Rady 2008/114/WE (Dz. Urz. UE L 333 z 27.12.2022, str. 164);

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

11e) potencjalne zdarzenie dla cyberbezpieczeństwa – zdarzenie, które może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych;

11f) przedsiębiorca komunikacji elektronicznej – przedsiębiorcę telekomunikacyjnego lub podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów;

11g) przedsiębiorca telekomunikacyjny - przedsiębiorcę telekomunikacyjnego w rozumieniu art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;

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

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

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

11k) 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;”,

k) pkt 14 otrzymuje brzmienie:

„14) system informacyjny – oznacza to:

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 2024 r. poz. 307) lub

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

– wraz z danymi przetwarzanymi w postaci elektronicznej;”,

l) uchyla się pkt 15–17,

m) w pkt 19 kropkę zastępuje się średnikiem i dodaje się pkt 20 w brzmieniu:

„20) znaczące cyberzagrożenie – cyberzagrożenie, które przez swoje właściwości techniczne może mieć poważny wpływ na bezpieczeństwo systemów informacyjnych poprzez wywołanie szkody materialnej lub niematerialnej.”;

3) po art. 2 dodaje się art. 2a w brzmieniu:

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

4) w art. 3 wyrazy „kluczowych i usług cyfrowych” zastępuje się wyrazami „przez podmioty kluczowe i podmioty ważne”;

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

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

6) w art. 4:

a) pkt 1 i 2 otrzymują brzmienie:

„1) podmioty kluczowe;

2) podmioty ważne;”,

b) pkt 6 otrzymuje brzmienie:

„6) CSIRT sektorowe;”,

c) uchyla się pkt 7–16;

7) w tytule rozdziału 2 wyrazy „operatorów usług kluczowych” zastępuje się wyrazami „podmiotów kluczowych i podmiotów ważnych”;

8) art. 5 otrzymuje brzmienie:

„Art. 5. 1. Podmiotem kluczowym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 i nr 2 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), zwanego dalej „rozporządzeniem 651/2014/UE”;

2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w rozporządzeniu 651/2014/UE;

3) niezależnie od wielkości podmiotu:

a) dostawca usług DNS,

b) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa,

c) kwalifikowany dostawca usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia 910/2014,

d) podmiot krytyczny,

e) podmiot publiczny,

f) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7c ust. 2 pkt 1,

g) rejestr nazw domen najwyższego poziomu (TLD).

2. Podmiotem ważnym jest:

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

2) 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;

3) przedsiębiorca komunikacji elektronicznej będący mikro-, lub małym przedsiębiorcą, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE;
4) podmiot zidentyfikowany jako podmiot ważny na podstawie art. 7c ust. 2 pkt 2.

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

4. Dostawca usług DNS, rejestr nazw domen najwyższego poziomu (TLD), podmiot świadczący usługi rejestracji nazw domen, dostawca usług chmurowych, dostawca usług ośrodka przetwarzania danych, dostawca sieci dostarczania treści, dostawca usług zarządzanych, dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, dostawca internetowych platform handlowych, dostawca wyszukiwarki internetowej oraz dostawca platformy usług sieci społecznościowych świadczący usługi na terytorium Rzeczypospolitej Polskiej podlega obowiązkom wynikającym z ustawy, jeżeli na terytorium Rzeczypospolitej Polskiej:
1) ma siedzibę kierownik podmiotu podejmujący decyzje tego podmiotu w sprawie systemu zarządzania bezpieczeństwem informacji w podmiocie;
2) realizowane są zadania związane z systemem zarządzania bezpieczeństwem informacji w podmiocie, o których mowa w art. 8 ust. 1 lub art. 11 lub
3) podmiot ma największą liczbę pracowników w odniesieniu do innych państw członkowskich Unii Europejskiej.

5. Podmiot wskazany w ust. 4, 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.

6. Przedstawicielem może być osoba fizyczna, osoba prawna lub 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. 4, który nie posiada jednostki organizacyjnej w Unii Europejskiej, do którego organ właściwy do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK lub CSIRT GOV może się zwrócić w związku z obowiązkami podmiotu wynikającymi z ustawy.”;

9) uchyla się art. 6;

10) art. 7 otrzymuje brzmienie:

„Art. 7. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz podmiotów kluczowych i podmiotów ważnych.

2. Wykaz, o którym mowa w ust. 1, zawiera:

1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;
2) sektor, podsektor i rodzaj podmiotu, zgodnie z załącznikiem nr 1 lub nr 2 do ustawy;
3) siedzibę i adres do korespondencji;
4) adres do doręczeń elektronicznych, jeżeli został nadany;
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);
8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany;
9) zakres adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny;
10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny;
11) dane co najmniej 2 osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu oraz adres poczty elektronicznej;
12) numer telefonu przyporządkowany do wykonywanej działalności;
13) deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikroprzedsiębiorcy, małego przedsiębiorcy lub średniego przedsiębiorcy;
14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem wykonywanej działalności;
15) 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 zawierające nazwę (firmę) dostawcy, siedzibę, adres, numer telefonu, adres poczty elektronicznej;
16) informację o ustanowieniu przedstawiciela podmiotu kluczowego lub podmiotu ważnego, o którym mowa w art. 5 ust. 4, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:

a) w przypadku osób fizycznych: imię i nazwisko, adres, numer telefonu oraz adres poczty elektronicznej,

b) w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej: nazwę (firmę) przedstawiciela, siedzibę, adres, numer telefonu, adres poczty elektronicznej;

17) informację o zawarciu przez podmiot kluczowy lubo podmiot ważny porozumienia, o którym mowa w art. 8h ust. 5;

18) informację o uznaniu podmiotu kluczowego lub podmiotu ważnego za podmiot krytyczny;

19) wskazanie organu właściwego do spraw cyberbezpieczeństwa właściwy dla podmiotu kluczowego lub podmiotu ważnego;

20) wskazanie CSIRT sektorowego właściwego dla podmiotu kluczowego lub podmiotu ważnego;

21) wskazanie CSIRT MON, CSIRT NASK lub CSIRT GOV właściwego dla podmiotu kluczowego lub podmiotu ważnego;

22) numer w wykazie;

23) datę wpisu do wykazu;

24) tytuł prawny wpisania do wykazu, o którym mowa w ust. 1;

25) datę wykreślenia z wykazu, o którym mowa w ust. 1.

3. Podmiot kluczowy i podmiot ważny składa wniosek o wpis w wykazie, o którym mowa w ust. 1, w terminie 2 miesięcy od dnia spełnienia wymogów, o których mowa w art. 5 ust. 1 lub ust. 2.

4. 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 ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2023 r. poz. 1524).

5. Dane, o których mowa w ust. 2 pkt 18–25, uzupełnia minister właściwy do spraw informatyzacji.

6. W przypadku:

1) przedsiębiorców telekomunikacyjnych,

2) dostawców usług zaufania,

3) podmiotów publicznych,

4) podmiotów krytycznych

– minister właściwy do spraw informatyzacji wpisuje dane, o których mowa w ust. 2, do wykazu, o którym mowa w ust. 1, dotyczące tych podmiotów w oparciu o dane zawarte w rejestrach publicznych lub przekazane przez właściwe organy nadzorcze.

7. Podmioty, o których mowa w ust. 6, uzupełniają dane w wykazie, o którym mowa w ust. 1, składając wniosek o zmianę wpisu w tym wykazie.

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

9. Wniosek o wpis do wykazu, o którym mowa w ust. 1, zawiera dane, o których mowa w ust. 2 pkt 1–17. Wniosek o zmianę wpisu w wykazie, o którym mowa w ust. 1, zawiera wskazanie danych zmienianych.

10. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu, o którym mowa w ust. 1, zawiera oświadczenie podmiotu kluczowego lub podmiotu ważnego o następującej treści: „Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 Kodeksu karnego 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.

11. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu, o którym mowa w ust. 1, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo kwalifikowaną pieczęcią elektroniczną. Wniosek składa się w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

12. Wpis podmiotu do wykazu, o którym mowa w ust. 1, dokonuje się z chwilą złożenia poprawnego wniosku w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1.

13. Wnioskiem niepoprawnym jest wniosek:

1) niezawierający danych podlegających wpisowi zgodnie z ust. 2 pkt 1–17;
2) złożony przez osobę, wobec której prawomocnie orzeczono zakaz prowadzenia wszelkiej działalności gospodarczej;
3) dotyczący podmiotu kluczowego lub podmiotu ważnego już wpisanego do wykazu;
4) wraz z którym nie złożono oświadczeń, o których mowa w ust. 10;

5) niepodpisany.

14. Wpis, zmiana wpisu oraz wykreślenie wpisu z wykazu, o którym mowa w ust. 1, jest czynnością materialno-techniczną i ma charakter deklaratoryjny.

15. Minister właściwy do spraw informatyzacji przesyła na adres do doręczeń elektronicznych albo na adres poczty elektronicznej zaświadczenie o wpisie podmiotu do wykazu, zmianie wpisu albo jego wykreśleniu.

16. W przypadku podmiotów kluczowych lub podmiotów ważnych, wpisanych do wykazu przez ministra właściwego do spraw informatyzacji, z urzędu, minister ten wzywa podmioty, o których mowa w ust. 6, o uzupełnienie brakujących danych w wykazie, w terminie 14 dni od dnia doręczenia wezwania, pod rygorem kary pieniężnej.

17. Minister właściwy do spraw informatyzacji, co najmniej raz w roku, aktualizuje dane zawarte we wpisach w wykazie, o którym mowa w ust. 1, na podstawie danych pozyskanych z rejestrów publicznych.

18. Minister właściwy do spraw informatyzacji wykreśla podmiot z wykazu, o którym mowa w ust. 1, 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.

19. Podmiot kluczowy i podmiot ważny składa wniosek o zmianę wpisu w wykazie, o którym mowa w ust. 1, w zakresie danych, o których mowa w ust. 2 pkt 1–17, w terminie 14 dni od dnia ich zmiany. Wniosek o zmianę wpisu w wykazie, o którym mowa w ust. 1, zawiera wskazanie zmienianych danych, numer w tym wykazie oraz oświadczenie, o którym mowa w ust. 10.

20. Podmiot kluczowy i podmiot ważny składa wniosek o wykreślenie z wykazu, o którym mowa w ust. 1, jeżeli przestał spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny. Organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek w terminie miesiąca. W przypadku niewyrażenia odmowy w tym terminie organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu.

21. Dane, o których mowa w ust. 2, minister właściwy do spraw informatyzacji udostępnia 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.

22. Dane, o których mowa w ust. 2, w zakresie niezbędnym do realizacji ich ustawowych zadań, minister właściwy do spraw informatyzacji udostępnia, na wniosek, następującym podmiotom:

1) Agencji Bezpieczeństwa Wewnętrznego;
2) Agencji Wywiadu;
3) Centralnemu Biuru Antykorupcyjnemu;
4) dyrektorowi Rządowego Centrum Bezpieczeństwa;
5) organom Krajowej Administracji Skarbowej;
6) Policji;
7) Prezesowi Urzędu Ochrony Danych Osobowych;
8) Prokuratorii Generalnej Rzeczypospolitej Polskiej;
9) prokuraturze;
10) sądom;
11) Służbie Kontrwywiadu Wojskowego;
12) Służbie Ochrony Państwa;
13) Służbie Wywiadu Wojskowego;
14) Straży Granicznej;
15) Żandarmerii Wojskowej.”;

11) po art. 7 dodaje się art. 7a–7c w brzmieniu:

„Art. 7a. 1. Organ właściwy do spraw cyberbezpieczeństwa może wpisać podmiot do wykazu, o którym mowa w art. 7 ust. 1, jeżeli podmiot ten spełnia przesłanki uznania go za podmiot kluczowy albo podmiot ważny oraz podmiot ten nie złożył wniosku, o którym mowa w art. 7 ust. 3.

2. Wpisując podmiot do wykazu, o którym mowa w art. 7 ust. 1, organ właściwy do spraw cyberbezpieczeństwa korzysta z danych zawartych w rejestrach publicznych.

3. Organ właściwy do spraw cyberbezpieczeństwa zawiadamia podmiot o wpisaniu do wykazu na podstawie ust. 1 oraz wzywa ten podmiot do uzupełnienia brakujących danych w wykazie, o którym mowa w art. 7 ust. 1, w terminie 14 dni od dnia otrzymania zawiadomienia, pod rygorem nałożenia kary pieniężnej. Zawiadomienie przekazuje się na adres do doręczeń elektronicznych podmiotu.

4. Wpisanie na podstawie ust. 1 do wykazu, o którym mowa w art. 7 ust. 1, jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

Art. 7b. 1. Organ właściwy do spraw cyberbezpieczeństwa może weryfikować dane zawarte we wpisie w wykazie, o którym mowa w art. 7 ust. 1, ze stanem faktycznym. Weryfikacja odbywa się za pomocą danych zawartych w rejestrach publicznych oraz z innych powszechnie dostępnych źródeł informacji.

2. W przypadku stwierdzenia, że dane w wykazie są niezgodne ze stanem faktycznym organ właściwy do spraw cyberbezpieczeństwa wzywa podmiot do zmiany wpisu do wykazu w terminie 7 dni od doręczenia wezwania, pod rygorem nałożenia kary pieniężnej. Zawiadomienie przekazuje się na adres do doręczeń elektronicznych podmiotu.

3. Organ właściwy do spraw cyberbezpieczeństwa odmawia wykreślenia podmiotu z wykazu, o którym mowa w art. 7 ust. 1, jeżeli podmiot nadal spełnia przesłanki uznania za podmiot kluczowy lub podmiot ważny. Odmowa wykreślenia jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

4. Organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu, o którym mowa w art. 7 ust. 1, jeżeli:

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

Art. 7c. 1. Organ właściwy do spraw cyberbezpieczeństwa, w drodze decyzji, uznaje osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej za podmiot kluczowy lub podmiot ważny jeżeli:

1) prowadzi działalność określoną w załączniku nr 1 lub nr 2 do ustawy;
2) jest mikroprzedsiębiorcą albo małym przedsiębiorcą;
3) spełnia chociaż jedną z poniższych przesłanek:
   a) jako jedyna świadczy usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,
   b) zakłócenie świadczenia usługi przez nią spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub obronności,
   c) zakłócenie świadczenia usługi przez nią spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub

d) świadczenie przez nią usług ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub nr 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 do jakiego został przypisany podmiot;
2) wzywa podmiot do uzupełnienia brakujących danych w wykazie, o którym mowa w art. 7 ust. 1, w terminie 14 dni od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej.

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

5. Organ właściwy do spraw cyberbezpieczeństwa niezwłocznie wpisuje podmiot, wobec którego wydano decyzję, o której mowa w ust. 1, do wykazu, o którym mowa w art. 7 ust. 1.

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

1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy,
2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, w terminie 12 miesięcy

– od dnia doręczenia tej decyzji.”;

12) art. 8 otrzymuje brzmienie:

„Art. 8. 1. Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług 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, w szczególności:

a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
b) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
c) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
d) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
e) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, oraz planów awaryjnych umożliwiających odtworzenie systemu informacyjnego po katastrofie,
f) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
g) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
h) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu, w tym podstawowe zasady cyberhigieny,
i) polityki i procedury stosowania kryptografii, w tym szyfrowania;

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;

6) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa, uwzględniających uwierzytelnianie wieloskładnikowe.

2. Wymagania, o których mowa w ust. 1, uznaje się za spełnione, gdy podmiot kluczowy i podmiot ważny zapewnia system zarzadzania bezpieczeństwem informacji, z uwzględnieniem wymagań określonych w Polskiej Normie PN-EN ISO/IEC 27001 oraz PN-EN ISO/IEC 22301.

3. Minister właściwy do spraw informatyzacji może udostępnić w Biuletynie Informacji Publicznej na swojej stronie podmiotowej mapowanie wymogów Polskich Norm, o których mowa w ust. 2, na obowiązki wynikające z ustawy oraz z przepisów wydanych na podstawie art. 8a.

4. Wdrażając środki, o których mowa w ust. 1 pkt 2 lit. c, podmiot kluczowy i 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”.”;

13) po art. 8 dodaje się art. 8a–8i w brzmieniu:

„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”, skalę działalności wykonywanej przez te

podmioty oraz potrzebę podejmowania przez te podmioty działań zapewniających cyberbezpieczeństwo.

Art. 8b. Podmioty kluczowe z podsektora energii elektrycznej, będące jednocześnie podmiotami realizującymi obowiązki określone w przepisach wydanych na podstawie art. 9 ust. 3 i 4 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2024 r. poz. 266) stosują określone w tych przepisach zasady dotyczące aspektów cyberbezpieczeństwa w transgranicznych przepływach energii elektrycznej, w tym zasady dotyczące wspólnych wymogów minimalnych, planowania, monitorowania, sprawozdawczości i zarządzania kryzysowego odpowiednio.

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. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 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 zostały powierzone innej osobie za jej zgodą.

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

1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania i przeglądu 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 przepisy prawa oraz wewnętrzne regulacje podmiotu w tym zakresie;
5) zapewnia zgodność działania tego podmiotu z przepisami prawa oraz z wewnętrznymi regulacjami podmiotu.

Art. 8e. Kierownik podmiotu kluczowego lub podmiotu ważnego raz w roku kalendarzowym przechodzi szkolenie z zakresu wykonywania obowiązków, o których

mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. Udział w szkoleniu jest udokumentowany.

Art. 8f. 1. Osoba realizująca zadania, o których mowa w art. 8 i art. 11, nie może być skazana prawomocnym wyrokiem sądu za przestępstwa przeciwko ochronie informacji.

2. Weryfikacji niekaralności osób realizujących zadania, o których mowa w art. 8 i art. 11, dokonuje podmiot kluczowy i podmiot ważny.

Art. 8g. Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa 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 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 i podmioty ważne wymieniają między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu, 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 jeśli:

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 zagrożeń, 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 przy wykorzystaniu 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. 5.

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

5. Podmioty kluczowe, podmioty ważne, CSIRT sektorowy lub inne podmioty mogą zawierać porozumienia w sprawie wymiany informacji, o których mowa w ust. 1, określając sposób wymiany informacji i zachowania informacji w poufności pomiędzy stronami porozumienia.

6. Koszty wykonania porozumień, o których mowa w ust. 5, ponoszone są w równych częściach przez wszystkie strony, chyba że w danym porozumieniu postanowiono inaczej.

Art. 8i. Podmioty kluczowe i podmioty ważne z sektora bankowość i infrastruktura rynków finansowych nie stosują przepisów niniejszego rozdziału w zakresie w jakim mają obowiązek stosować rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające 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).”;

14) art. 9 i 10 otrzymują brzmienie:

„Art. 9. Podmiot kluczowy i podmiot ważny:

1) wyznacza dwie osoby odpowiedzialne za utrzymywanie kontaktów z innymi podmiotami kluczowymi i podmiotami ważnymi;

2) zapewnia użytkownikowi usługi dostęp 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) po uzyskaniu wpisu podmiotu do wykazu, o którym mowa w art. 7 ust. 1, rozpoczyna korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w zakresie, o którym mowa w ust. 1 tego przepisu, w terminie 14 dni od dokonania wpisu.

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

2. Do dokumentacji dotyczącej bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi zalicza się:

1) dokumentację normatywną;
2) dokumentację operacyjną.

3. Dokumentację normatywną stanowią:

1) dokumentacja dotycząca systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO/IEC 27001 lub normy jej równoważnej;
2) dokumentacja ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa, obejmująca:
   a) charakterystykę usługi oraz infrastruktury, w której świadczona jest usługa,
   b) szacowanie ryzyka dla obiektów infrastruktury,
   c) ocenę aktualnego stanu ochrony infrastruktury (plan postępowania z ryzykiem),
   d) opis zabezpieczeń technicznych obiektów infrastruktury,
   e) zasady organizacji i wykonywania ochrony fizycznej infrastruktury,
   f) 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 2021 r. poz. 1995.), chroniącej infrastrukturę – jeżeli występuje;
3) dokumentacja systemu zarządzania ciągłością działania usługi wytworzona zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301 lub normy jej równoważnej;
4) dokumentacja techniczna systemu informacyjnego wykorzystywanego do świadczenia usługi;
5) dokumentacja wynikająca ze specyfiki świadczonej usługi w danym sektorze lub podsektorze.

3. Dokumentację operacyjną stanowią zapisy poświadczające wykonywanie czynności wymaganych przez postanowienia zawarte w dokumentacji normatywnej, w tym automatycznie generowane zapisy w dziennikach systemów teleinformatycznych.

4. Dokumentacja, o której mowa w ust. 1, może być prowadzona w postaci papierowej albo w postaci elektronicznej.

5. Podmiot kluczowy lub podmiot ważny jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do 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.

6. Podmiot kluczowy lub podmiot ważny przechowuje dokumentację dotyczącą bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi, liczony od 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).

7. Zniszczenie wycofanej z użytkowania dokumentacji potwierdza się protokołem brakowania zawierającym w szczególności: datę protokołu, oznaczenie niszczonej dokumentacji, dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji są przechowywane w sposób trwały.”;

15) w art. 11:
   a) w ust. 1:
      – wprowadzenie do wyliczenia otrzymuje brzmienie:
        „Podmiot kluczowy i podmiot ważny:”,
      – w pkt 2 po wyrazie „właściwemu” dodaje się wyrazy „CSIRT sektorowemu”,
      – pkt 4 otrzymuje brzmienie:
        „4) zgłasza wczesne ostrzeżenie o incydencie poważnym niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego;”,

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

„4a) zgłasza incydent poważny niezwłocznie, nie później 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, nie później niż w ciągu miesiąca od dnia zgłoszenia, o którym mowa w pkt 4a;”,

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

„1a. Przedsiębiorca komunikacji elektronicznej zgłasza wczesne ostrzeżenie o incydencie poważnym, o którym mowa w ust. 1 pkt 4a, niezwłocznie, nie później niż w ciągu 12 godzin od momentu jego wykrycia, do właściwego CSIRT sektorowego.

1b. Dostawca usług zaufania zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu jego wykrycia do właściwego CSIRT sektorowego.”,

c) ust. 2 otrzymuje brzmienie:

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

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

„2a. W przypadku zaistnienia znaczącego cyberzagrożenia podmiot kluczowy i podmiot ważny informuje swoich użytkowników, na których takie cyberzagrożenie może mieć wpływ, o możliwych środkach zapobiegawczych, które użytkownicy ci mogą podjąć. Podmiot kluczowy i podmiot ważny informuje tych użytkowników o samym znaczącym cyberzagrożeniu, jeżeli nie spowoduje to zwiększenia poziomu ryzyka dla bezpieczeństwa systemów informacyjnych.

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

e) uchyla się ust. 3,

f) w ust. 4:
   – we wprowadzeniu do wyliczenia wyrazy „załączniku nr 1” zastępuje się wyrazami „załącznikach nr 1 oraz nr 2”,
   – w pkt 2 wyrazy „świadczoną usługę kluczową” zastępuje się wyrazami „świadczone usługi”;

16) art. 12 otrzymuje brzmienie:

„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 oraz adres poczty elektronicznej osoby dokonującej zgłoszenia;
3) imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji;
4) wskazanie momentu wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania;
5) wskazanie czy incydent poważny wyczerpuje znamiona przestępstwa;
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 wsparcie techniczne przy obsłudze incydentu. CSIRT sektorowy nie później niż w ciągu 24 godzin przekazuje podmiotowi zgłaszającemu wytyczne dotyczące wdrożenia środków lub udziela 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) usługi zgłaszającego, na które 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,
   e) przyczynę zaistnienia incydentu poważnego i sposób jego przebiegu oraz skutki jego oddziaływania na systemy informacyjne lub świadczone usługi;

2) opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;
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 może zawierać także inne istotne informacje związane z przebiegiem incydentu poważnego lub podjętymi działaniami.

5. Podmiot kluczowy i podmiot ważny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego.

6. Podmiot kluczowy i 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 lub zgłoszenia 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 i podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.”;

17) po art. 12 dodaje się art. 12a i 12b w brzmieniu:

„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) w odpowiednich przypadkach transgraniczne skutki incydentu.

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 i podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie okresowe 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 i podmiot ważny przekazuje właściwemu CSIRT sektorowemu sprawozdanie końcowe nie później niż w ciągu miesiąca od zakończenia obsługi incydentu poważnego.”;

18) art. 13 otrzymuje brzmienie:

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

1) o innych incydentach;
2) o cyberzagrożeniach;
3) dotyczące szacowania ryzyka;
4) o podatnościach;
5) o potencjalnych zdarzeniach dla cyberbezpieczeństwa;
6) o 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 i podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.”;

19) uchyla się art. 14;

20) w art. 15:

a) ust. 1 otrzymuje brzmienie:

„1. Podmiot kluczowy lub podmiot ważny ma obowiązek zapewnić przeprowadzenie, na własny koszt, co najmniej raz na 2 lata, audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi, zwanego dalej „audytem”.”,

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

„1a. Podmiot kluczowy lub podmiot ważny przedstawia w postaci elektronicznej sprawozdanie z przeprowadzonego audytu, o którym mowa w ust. 1, organowi właściwemu, w terminie trzech dni roboczych od dnia jego otrzymania przez podmiot kluczowy lub podmiot ważny.

1b. Organ właściwy do spraw cyberbezpieczeństwa może nakazać, w drodze decyzji, przeprowadzenie audytu, o którym mowa w ust. 1, wraz z określeniem terminu przekazania sprawozdania z przeprowadzonego audytu.”,

c) w ust. 2 w pkt 3 wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowy”,

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

„2a. Audyt nie może być przeprowadzony przez osobę realizującą w podmiocie audytowanym zadania, o których mowa w art. 8 i art. 11, lub która realizowała te zadania w podmiocie audytowanym przez rok przed rozpoczęciem audytu.”,

e) w ust. 3 uchyla się pkt 3,

f) w ust. 5 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi ważnemu”,

g) w ust. 7:

– wprowadzenie do wyliczenia otrzymuje brzmienie:

„Podmiot kluczowy lub podmiot ważny przekazuje kopię sprawozdania z przeprowadzonego audytu na wniosek:”,

– uchyla się pkt 1,

– w pkt 2 wyrazy „operator usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”;

21) art. 16 otrzymuje brzmienie:

„Art. 16. 1. Podmiot kluczowy i podmiot ważny:

1) realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy,

2) zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 12 miesięcy

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

22) po rozdziale 3 dodaje się rozdział 3a w brzmieniu:

„Rozdział 3a

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

Art. 16a. 1. Rejestr nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen zobowiązane są do gromadzenia

i zachowywania z należytą starannością dokładnych i kompletnych danych dotyczących rejestracji nazw domen.

2. Podmioty świadczące usługi rejestracji nazw w konkretnej domenie najwyższego poziomu zobowiązane są do współpracy z rejestrem nazw tej domeny. Baza danych dotycząca rejestracji nazw domen może funkcjonować w szczególności przez umożliwianie rejestratorom 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 zadania 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 rejestratora.

5. Rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen 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) mogą dotyczyć działań weryfikacyjnych 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 4;
4) mogą obejmować 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. 4, w szczególności numeru lub innego oznaczenia identyfikacyjnego abonenta nazwy domeny zawartego w stosownych ewidencjach lub rejestrach państwowych, 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 udostępniają 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 rejestry nazw domen najwyższego poziomu (TLD) i podmioty świadczące usługi rejestracji nazw domen niezwłocznie publikują na stronie internetowej dane dotyczące rejestracji nazwy domeny niebędące danymi osobowymi.

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 kontaktowego adresu poczty elektronicznej abonenta nazwy domeny, wymaga uzyskania zgody, obowiązek jej uzyskania obciąża podmiot przetwarzający te dane jako pierwszy.

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

1) sądu lub prokuratora – w związku z toczącym się postępowaniem,
2) Policji oraz innych upoważnionych organów w postępowaniu karnym, w związku z prowadzonym przez te organy postępowaniem

– udzielają dostępu do konkretnych danych dotyczących rejestracji nazw domen, z zachowaniem przepisów dotyczących ochrony danych osobowych.

2. Rejestry nazw domen najwyższego poziomu (TLD) oraz podmioty świadczące usługi rejestracji nazw domen udzielają odpowiedzi nie później niż w terminie 72 godzin

od dnia otrzymania wniosku o dostęp, w sposób określony w opracowanej przez siebie i podanej do wiadomości publicznej polityce i procedurze ujawniania takich danych. Jeżeli koniec terminu, o którym mowa w zdaniu poprzedzającym, przypada na dzień ustawowo wolny od pracy, za koniec terminu uznaje się koniec następnego dnia powszedniego.”;

23) uchyla się rozdział 4 i 5;

24) użyte w art. 26 w ust. 1, w ust. 3 w pkt 1 i 10, w pkt 14 w lit. b i c oraz w ust. 6 w pkt 2, w art. 35 w ust. 4, w art. 46 w ust. 1 w pkt 5, w art. 51 w pkt 2, 7 i 8, w art. 52 w pkt 2 i 4, w art. 62 w ust. 2 w pkt 3, w art. 73 w ust. 5 w pkt 1 oraz w art. 83, w różnej liczbie i różnym przypadku, wyrazy „zagrożenie cyberbezpieczeństwa” zastępuje się użytym w odpowiedniej liczbie i odpowiednim przypadku wyrazem „cyberzagrożenie”;

25) użyte w art. 26 w ust. 3 w pkt 10, w art. 40, w art. 42 w ust. 1 w pkt 5, w art. 44 w ust. 3 w zdaniu pierwszym i drugim, w art. 49 w ust. 3 we wprowadzeniu do wyliczenia, w art. 64, oraz w art. 93 w ust. 11 w pkt 4 w różnej liczbie i różnym przypadku, wyrazy „sektorowy zespół cyberbezpieczeństwa” zastępuje się użytymi w odpowiedniej liczbie i odpowiednim przypadku wyrazami „CSIRT sektorowy”;

26) w art. 26:

a) ust. 2 otrzymuje brzmienie:

„2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach, na wniosek podmiotów krajowego systemu cyberbezpieczeństwa mogą zapewnić wsparcie tym podmiotom w obsłudze incydentów. O udzieleniu wsparcia jest informowany właściwy CSIRT sektorowy.”,

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

„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

2) CSIRT GOV, za zgodą Szefa Agencji Bezpieczeństwa Wewnętrznego.

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

c) w ust. 3:

– pkt 2–4 otrzymują brzmienie:

„2) szacowanie ryzyka związanego z ujawnionym cyberzagrożeniem oraz zaistniałymi incydentami, w tym zapewnianie podmiotom krajowego systemu cyberbezpieczeństwa 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;”,

– pkt 12 otrzymuje brzmienie:

„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 zdarzeniach dla cyberbezpieczeństwa;”,

– uchyla się pkt 15,

– w pkt 16 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)” zastępuje się wyrazem „ENISA”,

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

„17) w odpowiednich przypadkach gromadzenie i analizowanie danych na potrzeby postepowań karnych;

18) współpraca z sektorowymi i międzysektorowymi społecznościami podmiotów kluczowych i podmiotów ważnych oraz, w odpowiednich przypadkach, wymieniają z nimi informacje;

19) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich, w ramach której mogą wymieniać informacje, w tym dane osobowe zgodnie z unijnymi przepisami o ochronie danych;

20) udział we wdrażaniu bezpiecznych narzędzi wymiany informacji zgodnie z podmiotami kluczowymi i podmiotami ważnymi oraz innymi odpowiednimi zainteresowanymi stronami;

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,
   c) ujawnianiem podatności.”,

d) w ust. 6 w pkt 1:
   – w lit. a wyrazy „11 i 12” zastępuje się wyrazami „10–13”,
   – po lit. c dodaje się lit. ca–cc w brzmieniu:
   „ca) międzynarodowe instytuty badawcze,
   cb) Centrum Łukasiewicz,
   cc) instytuty badawcze Centrum Łukasiewicz, ”,
   – uchyla się lit. e,
   – uchyla się lit. i,
   – lit. j otrzymuje brzmienie:
   „j) podmioty kluczowe i podmioty ważne, z wyjątkiem wymienionych w ust. 5 i 7,”,

e) w ust. 7 po pkt 4 dodaje się pkt 4a–4d w brzmieniu:
   „4a) Polską Agencję Żeglugi Powietrznej;
   4b) Państwowe Gospodarstwo Wodne Wody Polskie;
   4c) 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;
   4d) Urząd Komisji Nadzoru Finansowego;”,

f) po ust. 8 dodaje się ust. 8a w brzmieniu:

„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.”,

g) dodaje się ust. 12 w brzmieniu:

„12. CSIRT MON, CSIRT NASK i CSIRT GOV mogą uczestniczyć w procesie wzajemnej oceny, o którym mowa w art. 19 dyrektywy 2022/2555.”;

27) po art. 26 dodaje się art. 26a w brzmieniu:

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

2. Osoba fizyczna, osobna prawna lub 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 prawną zgłaszającą podatność.

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

1) przyjmuje informacje o wykrytych podatnościach;
2) w razie konieczności, koordynuje komunikację między osobą fizyczną lub prawną zgłaszającą podatność a producentem lub dostawcą potencjalnie podatnych produktów ICT lub usług ICT, w zakresie weryfikacji zgłoszenia i terminu ujawniania podatności;
3) koordynuje proces ujawniania podatności;
4) może publikować informacje o podatnościach;
5) zarządza ujawnionymi informacjami o podatnościach.

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

28) w art. 28:

a) w ust. 1 wyrazy „operatora usługi kluczowej” zastępuje się wyrazami „podmiot kluczowy lub podmiot ważny”,

b) w ust. 2 wyrazy „operatorowi usługi kluczowej” zastępuje się wyrazami „podmiotowi kluczowemu lub podmiotowi ważnemu”;

29) w art. 30:

a) w ust. 1 we wprowadzeniu do wyliczenia wyrazy „operatorzy usług kluczowych i dostawcy usług cyfrowych” zastępuje się wyrazami „podmioty kluczowe i podmioty ważne”,

b) w ust. 2 wyrazy „operatorów usług kluczowych i dostawców usług cyfrowych” zastępuje się wyrazami „podmiotów kluczowych i podmiotów ważnych”;

30) art. 31 i 32 otrzymują brzmienie:

„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 w 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 publikuje 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. W trakcie koordynacji obsługi incydentu poważnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może 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. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do podmiotu kluczowego lub podmiotu ważnego o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub 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.”;

31) w art. 33:

a) w ust. 1wyrazy „urządzenia informatycznego lub oprogramowania” zastępuje się wyrazami „produktu ICT, usługi ICT lub procesu ICT ”,

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

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

1b. CSIRT MON, CSIRT NASK i CSIRT GOV prowadząc badanie, o którym mowa w ust. 1, jest uprawniony do stosowania technik mających na celu: obserwację i analizę pracy urządzenia lub oprogramowania, uzyskanie dostępu do przetwarzanych danych, odtworzenie postaci źródłowej oprogramowania, zwielokrotnienie (powielenie) kodu programowego oraz tłumaczenie (translacja) jego formy, odtworzenie algorytmu przetwarzania danych, identyfikację realizowanych funkcji, usunięcie lub przełamanie zabezpieczeń przed badaniem, identyfikację podatności lub identyfikację nieudokumentowanych funkcji realizowanych przez produkt ICT, usługi ICT lub procesu ICT.

1c. CSIRT MON, CSIRT NASK i CSIRT GOV w czasie prowadzenia badania, o którym mowa w ust. 1, nie jest związany postanowieniami umów, w szczególności umów licencyjnych, badanych produktów ICT, usług ICT lub procesów ICT, które ograniczyłyby możliwość przeprowadzenia badania.

1d. Badanie, o którym mowa w ust. 1:

1) nie narusza autorskich praw osobistych oraz majątkowych, oraz

2) nie wymaga zgody licencjodawcy lub dysponenta produktu ICT, usługi ICT lub procesu ICT.

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

c) ust. 2 otrzymuje brzmienie:

„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, usłudze ICT lub procesie ICT, których badanie dotyczy.”,

d) w ust. 4 i 5–8 wyrazy „urządzeń informatycznych lub oprogramowania” zastępuje się wyrazami „produktów ICT, usług ICT lub procesów ICT”,

e) w ust. 4a wyrazy „zagrożeniu cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniu”,

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

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

g) w ust. 5 wyrazy „otrzymania rekomendacji” zastępuje się wyrazami „udostępnienia rekomendacji na stronie podmiotowej w Biuletynie Informacji Publicznej”,

h) dodaje się ust. 9 w brzmieniu:

„9. CSIRT MON, CSIRT NASK lub CSIRT GOV przeprowadzający badanie może zwrócić się do producenta badanego produktu ICT, usługi ICT lub procesu ICT o przekazanie dokumentacji. Przepis art. 53c stosuje się odpowiednio. O zwróceniu się do producenta, jak również o nie przekazaniu przez producenta dokumentacji w terminie CSIRT przeprowadzający badanie informuje ministra właściwego do spraw informatyzacji.”;

32) w art. 34:

a) ust. 1 otrzymuje brzmienie:

„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.”,

b) dodaje się ust. 3 w brzmieniu:

„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.”;

33) w art. 35:

a) ust. 1 otrzymuje brzmienie:

„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 oraz właściwy CSIRT sektorowy.”,

b) w ust. 2 w pkt 1 w lit. a skreśla się wyrazy „w szczególności jeśli zakłóca świadczenie usługi kluczowej”,

c) w ust. 5:

– wyrazy „zagrożeniach cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniach”,

– wyraz „cyberbezpieczeństwa” zastępuje się wyrazem „bezpieczeństwa”;

34) w art. 36:

a) ust. 3 i 4 otrzymują brzmienie:

„3. Pełnomocnik przewodniczy pracom Zespołu.

4. Obsługę prac Zespołu zapewnia urząd obsługujący Pełnomocnika.”,

b) w ust. 6 wyrazy „dyrektor Rządowego Centrum Bezpieczeństwa” zastępuje się wyrazami „Pełnomocnik”;

35) po rozdziale 6 dodaje się rozdział 6a w brzmieniu:

„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.

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 (Dz. U. 2023 r. poz. 1136, 1834 i 1860);

2) akredytowanych na podstawie art. 48 ustawy z dnia 15 marca 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, 1030 i 1532).

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 za zgodą właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV. 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 lub
2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

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

3. W celu minimalizacji negatywnych następstw oceny bezpieczeństwa 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.

4. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy o może 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 2024 r. poz. 17), 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.

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

6. Informacje uzyskane przez CSIRT MON, CSIRT NASK, CSIRT GOV, 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, CSIRT sektorowe oraz podlegają one niezwłocznemu zniszczeniu, które przeprowadza komisja i które dokumentuje się protokołem zniszczenia tych informacji.

7. Komisja 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.

8. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy sporządza i przekazuje 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, CSIRT GOV.

Art. 36c. Jeżeli wykryta podatność może wystąpić w innych systemach informacyjnych, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy informuje niezwłocznie ministra właściwego do spraw informatyzacji oraz Pełnomocnika

o wykrytej podatności oraz o możliwości jej wystąpienia w innych systemach informacyjnych.

Art. 36d. Rada Ministrów może określić, w drodze rozporządzenia, sposób niszczenia materiałów zawierających informacje, o których mowa w art. 36b ust. 6, i tryb działania komisji, a także wzór protokołu, mając na uwadze rodzaj materiałów podlegających zniszczeniu oraz konieczność zapewnienia efektywności prowadzonych działań.”;

36) w art. 37:

a) ust. 1 otrzymuje brzmienie:

„1. Do udostępniania informacji o podatnościach, incydentach i cyberzagrożeniach oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej oraz ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego.”,

b) w ust. 2 wyrazy „operatorem usługi kluczowej” zastępuje się wyrazami „podmiotem kluczowym lub podmiotem ważnym”,

c) uchyla się ust. 3,

d) ust. 4 skreśla się wyrazy „i 3”;

37) w art. 39:

a) w ust. 1:

– wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

– wyrazy „zagrożeniami cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniami”,

– po wyrazach „art. 9 ust. 1” dodaje się wyrazy „i art. 10”,

b) w ust. 2:

– wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

– po wyrazach „art. 9 ust. 1” dodaje się wyrazy „i art. 10”,

c) w ust. 3:

– we wprowadzeniu do wyliczenia wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

– pkt 3 i 4 otrzymują brzmienie:

„3) gromadzone przez podmioty kluczowe i podmioty ważne w związku ze świadczeniem usług;

4) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1.”,

d) w ust. 4:

– we wprowadzeniu do wyliczenia wyrazy „zagrożeniami cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniami”,

– pkt 1 otrzymuje brzmienie:

„1) gromadzone przez podmioty kluczowe i podmioty ważne w związku ze świadczeniem usług;”,

– uchyla się pkt 2,

e) po ust. 6 dodaje się ust. 6a w brzmieniu:

„6a. Minister właściwy do spraw informatyzacji przetwarza dane osobowe w celu uwierzytelnienia osób fizycznych, które w imieniu podmiotu kluczowego i podmiotu ważnego korzystają z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1.”,

f) ust. 8 otrzymuje brzmienie:

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

g) w ust. 9 we wprowadzeniu do wyliczenia wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

h) dodaje się ust. 10 w brzmieniu:

„10. Dane, o których mowa w ust. 4, są usuwane lub anonimizowane przez ministra właściwego do spraw informatyzacji, dyrektora Rządowego Centrum Bezpieczeństwa, Pełnomocnika oraz organy właściwe do spraw cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne do realizacji zadań wynikających z niniejszej ustawy.”;

38) po art. 39 dodaje się art. 39a w brzmieniu:

„Art. 39a. 1. Minister właściwy do spraw informatyzacji realizując zadania związane z zapewnieniem bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym oraz kształtowaniem polityki państwa w zakresie danych osobowych może, wykorzystując dane pozyskane na podstawie art. 26 ust. 1, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 i art. 10 rozporządzenia 2016/679, tworzyć i udostępniać usługę online polegającą na możliwości sprawdzenia przez użytkownika czy jego dane zostały upublicznione w sieci internet w sposób nieuprawniony.

2. Realizację usługi online, o której mowa w ust. 1, minister właściwy do spraw informatyzacji może powierzyć jednostce mu podległej lub przez niego nadzorowanej. Szczegółowe warunki powierzenia realizacji tej usługi oraz warunki przetwarzania danych określi umowa pomiędzy ministrem właściwym do spraw informatyzacji a jednostką mu podległą lub przez niego nadzorowaną.”;

39) po art. 40 dodaje się art. 40a w brzmieniu:

„Art. 40a. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy, organy właściwe do spraw cyberbezpieczeństwa mogą, w porozumieniu z Pełnomocnikiem, uczestniczyć w procesie oceny wzajemnej, o którym mowa w art. 19 dyrektywy 2022/2555.

2. Ocena wzajemna odbywa się na zasadach określonych w art. 19 ust. 1 dyrektywy 2022/2555.

3. W ramach procesu oceny wzajemnej podmioty wskazane w ust. 1 mogą przekazywać wyznaczonym przez inne państwa członkowskie ekspertom do spraw cyberbezpieczeństwa informacje dotyczące funkcjonowania tych podmiotów z uwzględnieniem przepisów o tajemnicach prawnie chronionych.”;

40) w art. 41:

a) we wprowadzeniu do wyliczenia po wyrazie „cyberbezpieczeństwa” dodaje się wyrazy „dla podmiotów kluczowych”,

b) po pkt 8 dodaje się pkt 8a w brzmieniu:

„8) dla sektora infrastruktury cyfrowej podsektora komunikacji elektronicznej z wyłączeniem podmiotów, o których mowa w art. 26 ust. 5 – Prezes Urzędu Komunikacji Elektronicznej;”,

c) po pkt 9 dodaje się pkt 9a–9g w brzmieniu:

„9a) dla sektora 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 zdrowia;

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;”,

d) uchyla się pkt 10 i 11;

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

„Art. 41a. Organami właściwymi do spraw cyberbezpieczeństwa dla podmiotów ważnych są:

1) dla sektora usług pocztowych – Prezes Urzędu Komunikacji Elektronicznej;

2) dla sektora gospodarowania odpadami – minister właściwy do spraw klimatu;

3) dla sektora dostawców usług cyfrowych – minister właściwy do spraw informatyzacji;

4) dla sektora badań naukowych – minister właściwy do spraw nauki.

Art. 41b. 1. Organem właściwym do spraw cyberbezpieczeństwa w sektorze administracji publicznej dla:

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

2) jednostek podległych Prezesowi Rady Ministrów lub przez niego nadzorowanych,

3) Narodowego Banku Polskiego,

4) Banku Gospodarstwa Krajowego,

5) Polskiej Agencji Żeglugi Powietrznej

– jest Szef Agencji Bezpieczeństwa Wewnętrznego.

2. Organem właściwym do spraw cyberbezpieczeństwa w sektorze administracji publicznej dla:

1) jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 2–6, 10–13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych,
2) jednostek podległym organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych,
3) instytutów badawczych,
4) Urzędu Dozoru Technicznego,
5) Polskiego Centrum Akredytacji,
6) Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkich funduszy ochrony środowiska i gospodarki wodnej,
7) spółek prawa handlowego wykonujących zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej,

– jest minister właściwy do spraw informatyzacji.

3. Organem właściwym w sektorze administracji publicznej dla podmiotów podległych Ministrowi Obrony Narodowej lub przez niego nadzorowanych jest Minister Obrony Narodowej.

4. Minister właściwy do spraw informatyzacji może powierzyć realizację zadań nadzorczych nad podmiotami kluczowymi w sektorze administracji publicznej 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.”;

42) w art. 42:
   a) w ust. 1:
      – pkt 1–3 otrzymuje brzmienie:
         „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 podmiotów kluczowych i podmiotów ważnych, 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. 7c ust. 1;”,

– uchyla się pkt 4,

– pkt 6–8 otrzymują brzmienie:

„6) monitoruje stosowanie przepisów ustawy przez podmioty kluczowe i podmioty ważne;

7) wzywa na wniosek CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego podmioty kluczowe i podmioty ważne do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego lub krytycznego;

8) prowadzi kontrole podmiotów kluczowych i podmiotów ważnych;”,

– pkt 10 otrzymuje brzmienie:

„10) przetwarza informacje, w tym dane osobowe, dotyczące podmiotów kluczowych i podmiotów ważnych oraz świadczonych przez nich usług w zakresie niezbędnym do realizacji zadań wynikających z ustawy;”,

b) uchyla się ust. 2;

c) dodaje się ust. 9 w brzmieniu:

„9. Komisja Nadzoru Finansowego otrzymuje dotację celową na realizację swoich zadań ustawowych z części budżetowej, której dysponentem jest Szef Kancelarii Prezesa Rady Ministrów.”;

43) w art. 43:

a) ust. 1 i 2 otrzymują brzmienie

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

2. Organ właściwy do spraw cyberbezpieczeństwa może zwracać się do organów administracji publicznej prowadzących rejestry publiczne o przekazanie informacji, które umożliwią wstępną ocenę, czy dany podmiot należy uznać za podmiot kluczowy lub podmiot ważny, z zachowaniem przepisów o tajemnicach prawnie chronionych.”,

b) uchyla się ust. 3–5,

c) ust. 6 otrzymuje brzmienie:

„6. Informacje udzielone przez podmiot, o którym mowa w ust. 1, mogą stanowić materiał dowodowy we wszczętym postępowaniu.”;

44) w art. 44:

a) ust. 1 otrzymuje brzmienie:

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

1) przyjmowanie zgłoszeń o incydentach;
2) reagowanie na incydenty;
3) gromadzenie informacji o podatnościach i cyberzagrożeniach;
4) współpraca z podmiotem kluczowym i podmiotem ważnym w zakresie wymiany dobrych praktyk oraz informacji o podatnościach i cyberzagrożeniach, organizacja i uczestniczenie w ćwiczeniach oraz wspieranie inicjatyw szkoleniowych;
5) współpraca z CSIRT MON, CSIRT NASK i CSIRT GOV w koordynowanym przez nie reagowaniu na incydenty, w szczególności w zakresie wymiany informacji o cyberzagrożeniach oraz stosowanych środkach zapobiegających i ograniczających wpływ incydentów;
6) współpraca z innymi CSIRT sektorowymi w zakresie wymiany informacji o podatnościach i cyberzagrożeniach.”,

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

„1a. CSIRT sektorowy przekazuje wczesne ostrzeżenie, o którym mowa w art. 11 ust. 1 pkt 4 oraz zgłoszenie, o którym mowa w art. 11 ust. 1 pkt 4a, niezwłocznie, nie później 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 i podmiotów ważnych danego sektora lub podsektora;

2) wykonywać niezbędne działania techniczne związane z analizą cyberzagrożeń oraz reagowaniem na incydent poważny;
2) koordynować, w ramach sektora lub podsektora, w uzgodnieniu z podmiotami kluczowymi lub podmiotami ważnymi obsługę incydentów, które ich dotyczą;
3) wspierać, w uzgodnieniu z podmiotem kluczowym lub podmiotem ważnym, wykonywanie przez niego obowiązków określonych w art. 11, art. 12 i art. 13;
4) w ramach reagowania na incydent poważny wystąpić do organu właściwego do spraw cyberbezpieczeństwa z wnioskiem o wezwanie podmiotu kluczowego i podmiotu ważnego, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego. CSIRT sektorowy informuje o złożeniu wniosku właściwy CSIRT MON, CSIRT NASK albo CSIRT GOV;
5) prowadzić działania na rzecz podnoszenia poziomu bezpieczeństwa systemów informacyjnych podmiotów kluczowych i 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.

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.”,

c) uchyla się ust. 2,

d) ust. 4 otrzymuje brzmienie:

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

45) po art. 44 dodaje się art. 44a–44f w brzmieniu:

„Art. 44a. 1. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego jednostce jemu podległej albo przez niego nadzorowanej albo organowi przez niego nadzorowanemu.

2. Organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację zadania lub zadań CSIRT sektorowego państwowej osobie prawnej w rozumieniu art. 3 ustawy z dnia 16 grudnia 2016 r. o zasadach zarządzania mieniem państwowym (Dz. U. z 2024 r. poz. 125), 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 w szczególności zakres powierzonych zadań, zasady sprawowania kontroli nad prawidłowym wykonywaniem powierzonych zadań 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. Decyzję ogłasza się w dzienniku urzędowym organu właściwego do spraw cyberbezpieczeństwa.

3. 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 zdaniu drugim zachowuje moc.

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

Art. 44d. 1. Zadania CSIRT sektorowego:

1) są finansowane z części budżetu państwa, której dysponentem jest minister, będący organem właściwym do spraw cyberbezpieczeństwa;
2) mogą być dofinansowywane 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.

4. CSIRT sektorowy dla sektora bankowego i infrastruktury rynków finansowych otrzymuje dotację celową na realizację swoich zadań z części budżetowej, której dysponentem jest Szef Kancelarii Prezesa Rady Ministrów.

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 udostępnia komunikat o zawarciu porozumienia na swojej stronie podmiotowej w Biuletynie 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.”;

46) w art. 45

a) w ust. 1:

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

„1a) monitorowanie wdrażania Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwanego dalej „Krajowym planem”, oraz realizację działań na rzecz jej wdrożenia;

1b) prowadzenie wykazu podmiotów kluczowych i podmiotów ważnych;”,

– pkt 3 otrzymuje brzmienie:

„3) opracowywanie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez podmioty kluczowe i podmioty ważne mających wpływ na ciągłość świadczenia usług przez te podmioty w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług w państwach członkowskich Unii Europejskiej;”,

– pkt 6 otrzymuje brzmienie:

„6) udostępnianie informacji i dobrych praktyk uzyskanych z Grupy Współpracy podmiotom krajowego systemu cyberbezpieczeństwa w celu usprawnienia działań krajowego systemu cyberbezpieczeństwa;”,

– dodaje się pkt 7–12 w brzmieniu:

„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, reagowania kryzysowego i zarządzania kryzysowego, a także koordynacji współpracy w celu ochrony bezpieczeństwa technologii informacyjnej aktywów o krytycznym znaczeniu we współpracy z sektorem prywatnym;

10) współpraca z krajowymi zespołami reagowania na incydenty bezpieczeństwa komputerowego z państw trzecich lub równoważnymi organami państw trzecich oraz wsparcie dla tych zespołów;

11) koordynacja działania organów państwa w przypadku wystąpienie sytuacji kryzysowej w cyberbezpieczeństwie nie dotyczącej obrony państwa oraz Sił Zbrojnych Rzeczpospolitej Polskiej;

12) uczestniczenie w pracach Europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa, o której mowa w art. 16 dyrektywy 2022/2555.”,

b) ust. 2 otrzymuje brzmienie

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

47) po art. 45 dodaje się art. 45a w brzmieniu:

„Art. 45a. Minister właściwy do spraw informatyzacji pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w wymiarze cywilnym.”;

48) w art. 46:

a) w ust. 1 w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6 i 7 w brzmieniu:

„6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;

7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679.”,

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

„1a. W systemie teleinformatycznym prowadzi się wykaz podmiotów kluczowych i podmiotów ważnych.”,

c) ust. 2 otrzymuje brzmienie:

„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.”,

d) uchyla się ust. 3,

e) dodaje się ust. 4–8 w brzmieniu:

„4. Podmioty kluczowe i podmioty ważne, inne niż w ust. 2, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, po uzyskaniu wpisu w wykazie podmiotów kluczowych i podmiotów ważnych.

5. Uwierzytelnienie do systemu teleinformatycznego następuje za pomocą środków określonych w art. 20a ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2024 r. poz. 307).

6. Podmioty kluczowe i podmioty ważne obowiązane są zapewnić zgodność swoich systemów informacyjnych z minimalnymi wymaganiami technicznymi i funkcjonalnymi korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, w terminie 3 miesięcy od udostępnienia tych wymagań.

7. Minister właściwy do spraw informatyzacji udostępnia minimalne wymagania techniczne i funkcjonalne korzystania z systemu teleinformatycznego, o którym mowa w ust. 1, w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.

8. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej wykaz usług świadczonych przez podmioty kluczowe i podmioty ważne stosowany w systemie teleinformatycznym, o którym mowa w ust. 1.”;

49) w art. 47

a) w ust. 1 po wyrazach „ w art. 45 ust. 1” dodaje się wyrazy „ , 1a”,

b) dodaje się ust. 3 w brzmieniu:

„3. Minister właściwy do spraw informatyzacji może udostępniać jednostkom, o których mowa w ust. 1, dane z wykazu podmiotów kluczowych i podmiotów ważnych w zakresie realizacji zadań im powierzonych.”;

50) w art. 48 ust. 1 pkt 1 i 2 otrzymują brzmienie:

„1) odbieranie zgłoszeń incydentu międzysektorowego lub dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowego;

2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV, zgłoszenia incydentu międzysektorowego lub dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej;";

51) w art. 49:

a) w ust. 3 pkt 2 wyrazy „Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA)" zastępuje się wyrazem „ENISA",

b) dodaje się ust. 4–6 w brzmieniu:

„4. Pojedynczy punkt kontaktowy przekazuje ENISA dane z wykazu podmiotów kluczowych i podmiotów ważnych dotyczące dostawców usług DNS, rejestrów nazw domen najwyższego poziomu (TLD), dostawców usług chmurowych, 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.

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 przypisany do wykonywanej działalności;
6) informację o wyznaczeniu przedstawiciela;
7) zakres adresów IP.

6. Pojedynczy punkt kontaktowy, co trzy miesiące, przedkłada ENISA sprawozdanie podsumowujące zawierające dane o:

1) poważnych incydentach;
2) incydentach;
3) cyberzagrożeniach;
4) potencjalnych zdarzeniach dla cyberbezpieczeństwa.";

52) w art. 50 dotychczasową treść oznacza się jako ust. 1 i:

a) w ust. 1 pkt 2 otrzymuje brzmienie:

„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 i podmioty ważne,

d) przepisy, na podstawie których podmioty kluczowe i podmioty ważne zostały wskazane.”,

b) dodaje się ust. 2 w brzmieniu:

„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.”;

53) w art. 51 dotychczasową treść oznacza się jako ust. 1 i:

a) w ust. 1:

– pkt 7 i 8 otrzymują brzmienie:

„7) ocenę cyberzagrożeń w każdym ze stanów gotowości obronnej państwa oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;

8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego i w czasie wojny dotyczących działań obronnych w przypadku cyberzagrożenia;”,

– dodaje się pkt 9 w brzmieniu:

„9) koordynację działania organów państwa w przypadku wystąpienie w przypadku wystąpienia sytuacji kryzysowej w cyberbezpieczeństwie dotyczącej obrony Państwa oraz Sił Zbrojnych Rzeczpospolitej Polskiej.”,

b) dodaje się ust. 2 w brzmieniu:

„2. Minister Obrony Narodowej pełni rolę organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę w sprawach dotyczących obrony Państwa oraz Sił Zbrojnych Rzeczypospolitej Polskiej.”;

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

„Art. 52a. W celu zabezpieczenia realizacji przewidzianych w ustawie zadań CSIRT MON oraz zadań Ministra Obrony Narodowej, Minister Obrony Narodowej, w drodze decyzji niepodlegającej ogłoszeniu, wydzieli z Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz z jednostek podporządkowanych Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni zespoły specjalistów oraz zasoby materiałowe i sprzętowe, które będą podlegać Ministrowi Obrony Narodowej w przypadku mianowania Naczelnego Dowódcy Sił Zbrojnych i przejęcia przez niego dowodzenia Siłami Zbrojnymi.”;

55) tytuł rozdziału 11 otrzymuje brzmienie:

„Nadzór i kontrola podmiotów kluczowych i podmiotów ważnych”;

56) art. 53 otrzymuje brzmienie:

„Art. 53 1. Nadzór w zakresie 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) zobowiązać podmiot, w drodze decyzji, o której mowa w art. 15 ust. 1b, do przeprowadzenia audytu, o którym mowa w art. 15 ust. 1, w szczególności w sytuacji wystąpienia poważnego incydentu lub naruszenia przepisów ustawy przez podmiot kluczowy;
3) zlecić CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowemu, dokonanie oceny bezpieczeństwa systemu informacyjnego podmiotu kluczowego lub podmiotu ważnego;
4) wystąpić z wnioskiem o udzielenie informacji niezbędnych do oceny środków, o których mowa w art. 8 ust. 1 pkt 2 5 i 6, a także zgodności z obowiązkiem przedkładania informacji właściwym organom zgodnie z art. 7;
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 zapobiegnięcia lub zaprzestania naruszania przepisów ustawy.

5. W celu egzekwowania przepisów ustawy organ właściwy do spraw cyberbezpieczeństwa w stosunku do podmiotów kluczowych, 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 realizacji obowiązku zgłaszania incydentu poważnego;
4) nakazać, w drodze decyzji , poinformowanie, w określony przez niego sposób, odbiorców swoich usług, których dotyczy znaczące 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 bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi;
6) wyznaczyć, w drodze decyzji , na określony czas, spośród osób zatrudnionych w urzędzie obsługującym ten organ, urzędnika monitorującego do nadzorowania wykonywania obowiązków, o których mowa w rozdziale 3;
7) nakazać, w drodze decyzji, podanie do wiadomości publicznej informacji o naruszeniach przepisów ustawy;
8) nałożyć, w drodze decyzji , karę pieniężną niezależnie od środków, o których mowa w pkt 1–7 i ostrzeżenia, o którym mowa w ust. 4;

9) nakazać, w drodze decyzji wydanej w postępowaniu uproszczonym, o którym mowa w rozdziale 14 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572), 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. Postępowanie, o którym mowa w ust. 5, jest jednoinstancyjne, a na decyzję organu właściwego do spraw cyberbezpieczeństwa przysługuje skarga do sądu administracyjnego.

8. 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 2–5 lub 6, może zwrócić się do:

1) organu, który udzielił koncesji podmiotu kluczowemu albo podmiotowi ważnemu o jej zawieszenie, ograniczenie jej zakresu albo cofnięcie do czasu gdy podmiot kluczowy albo podmiot ważny podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń;
2) organu, który dokonał wpisu podmiotu kluczowego albo podmiotu ważnego do rejestru działalności regulowanej ,o wykreślenie podmiotu z tego rejestru;
3) organu, który wydał podmiotowi kluczowemu albo podmiotowi ważnemu zezwolenie na prowadzenie działalności gospodarczej, o cofnięcie tego zezwolenia do czasu gdy podmiot kluczowy albo podmiot ważny podejmie działania niezbędne do usunięcia uchybień lub zaprzestania naruszeń;
4) sądu o nałożenie tymczasowego zakazu zajmowania stanowiska przez osoby kierujące podmiotem kluczowym.

9. Środków, o których mowa w ust. 8, nie stosuje się do podmiotów publicznych.

10. Organ właściwy do spraw cyberbezpieczeństwa podejmując działania, o których mowa w ust. 5 i 8, 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.

11. Organ właściwy do spraw cyberbezpieczeństwa przed zastosowaniem środków, o których mowa w ust. 4, 5 i 8, informuje podmiot kluczowy o wstępnych ustaleniach, które mogą prowadzić do wydania decyzji lub podjęcia działań o których mowa w ust. 8.

12. Podmiot kluczowy może przedstawić swoje stanowisko niezwłocznie, nie później niż w terminie 7 dni od dnia poinformowania o wstępnych ustaleniach, o których mowa w ust. 11.

13. 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.

14. 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 8 oraz informuje podmiot o tym fakcie;

2) odrzuca stanowisko tego podmiotu i stosuje środki, o których mowa w ust. 4, 5 lub 8 oraz informuje podmiot o tym fakcie.

15. Organ właściwy do spraw cyberbezpieczeństwa sprawując nadzór w stosunku do podmiotu ważnego stosuje odpowiednio ust. 2 i 4–14, uwzględniając postanowienia określone w ust. 3 pkt 2.”;

57) po art. 53 dodaje się art. 53a–53d w brzmieniu:

„Art. 53a. 1. Organy właściwe do spraw cyberbezpieczeństwa mogą tworzyć, samodzielnie lub wspólnie, metodyki nadzoru określające szczegółowy sposób przeprowadzania nadzoru nad podmiotami kluczowymi i 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 stosowanych metodyk nadzoru w szczególności w oparciu o ocenę efektywności sprawowanego nadzoru.

4. Na podstawie wyników oceny skuteczności, o której mowa w ust. 3, organy właściwe do spraw cyberbezpieczeństwa dokonują zmian w metodach 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 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 i podmiot ważny jest obowiązany do przekazywania na żądanie organu właściwego do spraw cyberbezpieczeństwa danych, informacji i dokumentów niezbędnych 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, powinno być proporcjonalne do celu, jakiemu ma służyć, oraz zawierać:

1) wskazanie podmiotu kluczowego lub podmiotu ważnego do którego skierowane jest żądanie;
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, nie krótszego niż 7 dni;
6) uzasadnienie żądania;
7) pouczenie o zagrożeniu karą, o której mowa w art. 73 ust. 1 pkt 16.

3. Żądanie sporządza się w postaci elektronicznej i przekazuje na adres do doręczeń elektronicznych podmiotu, do którego jest kierowane.

Art. 53d. 1. Urzędnik monitorujący, o którym mowa w art. 53 ust. 5 pkt 7, w zakresie nadzorowania wykonywania przez podmiot kluczowy obowiązków, o których mowa w rozdziale 3, jest uprawniony w szczególności do:

1) swobodnego wstępu i poruszania się po terenie podmiotu kluczowego bez obowiązku uzyskiwania przepustki;
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.

2. Urzędnik monitorujący realizuje powierzone mu zadania z zachowaniem przepisów o tajemnicy prawnie chronionej.”;

58) art. 54 otrzymuje brzmienie:

„Art. 54. 1. 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) nie będących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.

2. Czas trwania kontroli realizowanej wobec podmiotów kluczowych lub podmiotów ważnych będących przedsiębiorcami w jednym roku kalendarzowym nie może przekroczyć 48 dni roboczych.”;

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

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

60) art. 58 otrzymuje brzmienie:

„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, 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 do spraw kontroli dokonuje ich analizy.

7. Kierownik komórki 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 lub w części, lub je oddala.

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

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

10. O nieuwzględnieniu zastrzeżeń do protokołu kontroli w całości lub w części kierownik komórki 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.”;

61) w art. 59:

a) ust. 1 otrzymuje brzmienie:

„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.”,

b) w ust. 3 skreśla się wyrazy „lub ministra właściwego do spraw informatyzacji”;

62) po art. 59 dodaje się art. 59a i 59b w brzmieniu:

„Art. 59a. W przypadku stwierdzenia w toku kontroli podejrzenia naruszenia ochrony danych osobowych, organ właściwy do spraw cyberbezpieczeństwa informuje o tym Prezesa Urzędu Ochrony Danych Osobowych.

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

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 i podmiotami ważnymi, świadczących 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 możliwości organu;
3) organ innego państwa żąda o udostępnienie informacji lub dokumentów, których udostępnienie narusza podstawowy interes bezpieczeństwa państwa, bezpieczeństwa i porządku publiczności 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.”;

63) w art. 61:

a) ust. 3 otrzymuje brzmienie:

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

b) dodaje się ust. 5–8 w brzmieniu:

„5. Pełnomocnik może, w zakresie realizacji jego zadań, zlecać przeprowadzanie badań lub ekspertyz oraz powoływać zespoły doradcze.

6. Pełnomocnik może upoważnić do realizacji swoich zadań pracownika urzędu 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 obowiązane są 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.”;

64) w art. 62:

a) w ust. 1 w pkt 1 wyrazy „i CSIRT GOV” zastępuje się wyrazami „CSIRT GOV i CSIRT sektorowych”,

b) po ust. 2 dodaje się ust. 3 w brzmieniu:

„3. Pełnomocnik może dokonywać zakupów produktów ICT, usług ICT lub procesów ICT z zakresu cyberbezpieczeństwa na rzecz podmiotów publicznych.”;

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

„Art. 62a 1. Przy Pełnomocniku funkcjonuje Połączone Centrum Operacyjne Cyberbezpieczeństwa, zwane dalej „PCOC” będące organem pomocniczym w sprawach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa.

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 Obrony Narodowej,

c) ministra właściwego do spraw informatyzacji,

d) ministra właściwego do spraw zagranicznych,

e) Szefa Kancelarii Prezesa Rady Ministrów,

f) organów właściwych do spraw cyberbezpieczeństwa,

g) CSIRT GOV,

h) CSIRT MON,

i) CSIRT NASK,

j) CSIRT sektorowych,

k) Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni,

l) dyrektora Rządowego Centrum Bezpieczeństwa,

m) Komendanta Centralnego Biura Zwalczania Cyberprzestępczości,

n) Komendanta Głównego Policji,

o) Komendanta Służby Ochrony Państwa,

p) Komendanta Straży Granicznej,

q) Szefa Agencji Wywiadu,

r) Szefa Służby Kontrwywiadu Wojskowego,

s) Szefa Służby Wywiadu Wojskowego.

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

4. Na spotkania PCOC mogą być zapraszani przedstawiciele podmiotów kluczowych lub podmiotów ważnych, jeżeli wymaga tego charakter 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 ujawnionym cyberzagrożeniami oraz zaistniałymi incydentami;
3) wymiana informacji o przeprowadzanych badaniach, o których mowa w art. 33 ust. 1;
4) jednomyślne wyznaczanie roli CSIRT w przypadku incydentów, których obsługa wymaga działań kilku zespołów CSIRT, z wyjątkiem przypadków incydentów krytycznych;
5) wymiana informacji dotyczących sytuacji kryzysowych w cyberprzestrzeni;
6) przygotowywanie bieżących informacji na temat sytuacji w cyberprzestrzeni dla Pełnomocnika.

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 urząd obsługujący Pełnomocnika.

12. Pełnomocnik określi, w drodze zarządzenia, sposób działania PCOC mając na uwadze charakter zadań PCOC oraz konieczność zapewnienia jego sprawnej pracy. Zarządzenie to jest publikowane w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.”;

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

„Art. 64a. 1. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić CSIRT MON, CSIRT NASK 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 lub organy Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz przekazane przez sektor prywatny.

2. Przewodniczący Kolegium, działając z urzędu lub na wniosek innego członka Kolegium, może zlecić 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.”;

67) w art. 65:

a) w ust. 1:

– w pkt 1 wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”,

– w pkt 2:

– – wyrazy „sektorowe zespoły cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowe”,

– – wyrazy „zagrożeniom cyberbezpieczeństwa” zastępuje się wyrazem „cyberzagrożeniom”,

– w pkt 3 wyrazy „i CSIRT NASK” zastępuje się wyrazami „CSIRT NASK i CSIRT sektorowych”,

– w pkt 4 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”,

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

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

b) w ust. 2 wyrazy „Rady Ministrów” zastępuje się wyrazami „Prezesa Rady Ministrów”,

c) dodaje się ust. 3 w brzmieniu:

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

68) w art. 66:

a) w ust. 1 w pkt 4 w lit. g kropkę zastępuje się przecinkiem i dodaje się lit. h w brzmieniu:

„h) organy właściwe do spraw cyberbezpieczeństwa.”,

b) w ust. 4:

– pkt 1 otrzymuje brzmienie:

„1) dyrektor Rządowego Centrum Bezpieczeństwa albo jego zastępca;”,

– w pkt 4 kropkę zastępuje się średnikiem i dodaje się pkt 5–10 w brzmieniu:

„5) Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni albo jego zastępca;

6) Prokurator Generalny albo jego zastępca;

7) Przewodniczący Komisji Nadzoru Finansowego;

8) Szef Agencji Wywiadu albo jego zastępca;

9) Szef Centralnego Biura Antykorupcyjnego albo jego zastępca;

10) Szef Służby Wywiadu Wojskowego albo jego zastępca.”,

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

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

4) może zlecić 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. 64a 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. 64a ust. 2;

6) może wnioskować o wszczęcie postępowania w sprawie uznania dostawcy sprzętu i oprogramowania za dostawcę wysokiego ryzyka, o którym mowa w art. 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 2, wskazując właściwego członka zespołu opiniującego.”,

d) w ust. 7 wyrazy „sektorowych zespołów cyberbezpieczeństwa” zastępuje się wyrazami „CSIRT sektorowych”,

e) po ust. 7 dodaje się ust. 7a i 7b w brzmieniu:

„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.”;

69) po rozdziale 12 dodaje się rozdział 12a w brzmieniu:

„Rozdział 12a

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym”;

70) po art. 67 dodaje się art. 67a–67k w brzmieniu:

„Art. 67a. 1. Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów

informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

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

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. Podmiot krajowego systemu cyberbezpieczeństwa, do którego zostały skierowane rekomendacje uwzględnia je w zarządzaniu ryzykiem.

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 lub
2) przedsiębiorców telekomunikacyjnych, których roczne przychody z tytułu wykonywania działalności telekomunikacyjnej w poprzednim roku obrotowym były wyższe od kwoty 10 milionów złotych

– 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 komunikacji elektronicznej, 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 2023 r. poz. 1251, 1429 i 1672). 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 przed wszczęciem postępowania.

6. Minister właściwy do spraw informatyzacji zawiadamia o wszczęciu postępowania w sprawie uznania za dostawcę wysokiego ryzyka. Zawiadomienie udostępnia się także w Biuletynie Informacji Publicznej na stronie podmiotowej 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) – stronie umowy o Europejskim Obszarze Gospodarczym zawiadomienie, o którym mowa w ust. 6, udostępnia się w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji. Udostępnienie ma skutek doręczenia po upływie 14 dni od dnia jego dokonania.

9. W terminie 14 dni od dnia udostepnienia w Biuletynie Informacji Publicznej zawiadomienia, o którym mowa w ust. 6, izba gospodarcza 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, udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej raport ze złożonych w terminie stanowisk, wskazując w szczególności główne uwagi zawarte w stanowiskach.

10. Przed rozstrzygnięciem sprawy 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, zawiera analizę:

1) zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym oraz zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich, jakie stanowi dostawca sprzętu i oprogramowania, z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów Unii Europejskiej 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.[5)]);
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,

---

[5)] 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 oraz Dz. Urz. UE L 114 z 12.04.2022, str. 60.

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. 64a 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. W przypadku wystąpienia negatywnego sporu co do zakresu właściwości spór rozstrzyga przewodniczący Kolegium wskazując właściwego członka zespołu opiniującego;
3) jeżeli nie zostały wykonane analizy, o których mowa w art. 64a ust. 1 i 2, przewodniczący Kolegium zleca ich wykonanie;
4) zespół opiniujący przedstawia przewodniczącemu Kolegium projekt opinii;
5) uzgodnienie opinii następuje na posiedzeniu Kolegium;
6) uzgodnioną opinię przewodniczący Kolegium przekazuje ministrowi właściwemu do spraw informatyzacji.

14. W zespole opiniującym bierze udział również przedstawiciel Prezesa Urzędu Ochrony Konkurencji i Konsumentów. W posiedzeniu Kolegium, na którym następuje uzgodnienie opinii, bierze udział Prezes lub Wiceprezes Urzędu Ochrony Konkurencji i Konsumentów.

15. Minister właściwy do spraw informatyzacji, w drodze decyzji, uznaje dostawcę sprzętu lub oprogramowania za dostawcę wysokiego ryzyka, jeżeli dostawca ten stanowi

poważne zagrożenie dla obronności, bezpieczeństwa państwa lub bezpieczeństwa i porządku publicznego, lub życia i zdrowia ludzi.

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 udostępnia w Biuletynie Informacji Publicznej na stronie podmiotowej 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 nie później niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15.

2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

3. Do czasu wycofania sprzętu lub oprogramowania, o którym mowa w ust. 1 pkt 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 2023 r. poz. 1605 i 1720), 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 lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia lub udostępnienia informacji o decyzji, o której mowa w art. 67b ust. 15, a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 5 lat.

Art. 67d. 1. Podmioty kluczowe i 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 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, nie krótszego niż 7 dni;
5) uzasadnienie;
6) pouczenie o zagrożeniu karą, o której mowa w art. 73.

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 udostępnia w Biuletynie Informacji Publicznej 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 i podmiotów ważnych.

3. Do postępowania w sprawie o wydanie polecenia zabezpieczającego nie stosuje się art. 10, art. 34, art. 79, art. 81, art. 81a, art. 107 § 1 pkt 3, art. 145 § 1 pkt 4 i art. 156 § 1 pkt 4 oraz rozdziału 8 działu I ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, pozostałe przepisy tej ustawy stosuje się odpowiednio.

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

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

1) istotność cyberzagrożenia;
2) rodzaje ryzyk;
3) przewidywane lub zaistniałe skutki incydentu krytycznego;
4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się.

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

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

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

9. Polecenie zabezpieczające zawiera:

1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy;
2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;
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 i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;
3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT, procesie ICT lub usłudze ICT posiadającym daną podatność;
4) nakaz szczególnej konfiguracji produktu ICT, usługi ICT lub procesu ICT, zabezpieczającej przed wykorzystaniem określonej podatności;
5) nakaz wzmożonego monitorowania zachowania systemu;
6) zakaz korzystania z określonego produktu ICT, usługi ICT lub procesu ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;
7) nakaz wprowadzenia ograniczenia ruchu sieciowego z adresów IP lub adresów URL wchodzącego do infrastruktury podmiotu 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, nie dłużej niż na dwa lata.

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

14. Polecenie zabezpieczające podlega natychmiastowej wykonalności.

15. Minister właściwy do spraw informatyzacji ogłasza polecenie zabezpieczające w dzienniku urzędowym ministra właściwego do spraw informatyzacji. Informacje o poleceniu zabezpieczającym udostępnia się również na stronie internetowej urzędu obsługującego ministra.

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

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

Art. 67h. Podmioty, wobec których zostało skierowane 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 decyzja została ogłoszona w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

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

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

Art. 67j. 1. Do Narodowego Banku Polskiego nie stosuje się przepisów art. 67b oraz art. 67f.

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

2. Powierzając realizację zadań, o których mowa w ust. 1, określa się w szczególności:

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

3. Realizacja zadań, o których mowa w ust. 1, jest dokonywana przez Ministra Obrony Narodowej z wykorzystaniem jednostek mu podległych lub przez niego nadzorowanych, z uwzględnieniem art. 52a.

4. Komunikat o powierzeniu realizacji zadań, o których mowa w ust. 1, ogłasza się w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”. Informacja o komunikacie jest udostępniana na stronach internetowych CSIRT MON, CSIRT NASK, CSIRT GOV lub w Biuletynie Informacji Publicznej na stronie podmiotowej Pełnomocnika.”;

71) art. 69 otrzymuje brzmienie:

„Art. 69. 1. Strategia określa:

1) cele strategiczne oraz środki organizacyjne i regulacyjne, służące ich realizacji;
2) mechanizm służący określeniu istotnych zasobów i szacowanie ryzyka;
3) zasady współpracy między sektorem publicznym i prywatnym;
4) podmioty zaangażowane we wdrażanie i realizację Strategii;
5) środki służące koordynacji i wymiany informacji pomiędzy organami właściwymi w sprawach cyberbezpieczeństwa a właściwymi organami na podstawie dyrektywy (UE) 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.

2. Przy opracowaniu strategii uwzględnia się:

1) rozwiązania dotyczące cyberbezpieczeństwa w łańcuchu dostaw produktów ICT i usług ICT wykorzystywanych przez podmioty do świadczenia usług;
2) rozwiązania dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów ICT i usług 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, 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) zapewnienia 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 załączniku nr 1 i nr 2 do ustawy.

4. Strategia jest realizowana w oparciu o plan działań uwzględniający w szczególności koszty realizacji i źródła finansowania działań określonych w Strategii, który stanowi załącznik do Strategii.”;

72) po art. 70 dodaje się art. 70a w brzmieniu:

„Art. 70a. 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.

2. CSIRT MON, CSIRT NASK i CSIRT GOV, CSIRT sektorowy, organ właściwy do spraw cyberbezpieczeństwa przekazuje ministrowi właściwemu do spraw informatyzacji, w terminie do dnia 30 marca, informacje o realizacji celów Strategii w poprzednim roku.”;

73) po rozdziale 13 dodaje się rozdział 13a w brzmieniu:

„Rozdział 13a

Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę

Art. 72a. Rada Ministrów przyjmuje Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, zwany dalej „Krajowym Planem”, w drodze uchwały.

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 krajowych środków i działań służących w zakresie gotowości;
2) zadania organów zaangażowanych w zarządzanie kryzysowe w cyberbezpieczeństwie;
3) procedury zarządzania kryzysowego w cyberprzestrzeni, w tym ich włączenie do ogólnych krajowych ram zarządzania kryzysowego, oraz kanały wymiany informacji;
4) krajowe środki służące zapewnieniu gotowości na wypadek wystąpienia incydentów na dużą skalę w tym ćwiczenia i szkolenia;
5) zasady współpracy między sektorem publicznym i prywatnym w obszarze zarządzania kryzysowego;
6) rodzaje krytycznej infrastruktury informatycznej;

7) krajowe procedury i ustalenia między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie efektywnego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu incydentami i zarządzaniu kryzysowym w cyberbezpieczeństwie na dużą skalę na poziomie Unii oraz efektywnego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Art. 72c. Podmioty realizujące zadania z zakresu zarządzania kryzysowego zobowiązane są na żądanie ministra właściwego do spraw informatyzacji, przekazać 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 i właściwymi kierownikami urzędów centralnych.

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

Art. 72e. Krajowy Plan podlega aktualizacji nie rzadziej niż raz na dwa lata.

Art. 72f. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej i europejskiej sieci organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa Krajowy Plan, w terminie 3 miesięcy od dnia jego przyjęcia przez Radę Ministrów.”;

74) w art. 73:

a) ust. 1 otrzymuje brzmienie:

„1. Karze pieniężnej podlega podmiot kluczowy lub podmiot ważny, który:

1) nie uzupełnił w terminie brakujących danych w wykazie podmiotów kluczowych i podmiotów ważnych pomimo wezwania, o którym mowa w art. 7 ust. 16 albo art. 7a ust. 3, albo art. 7b ust. 2, albo art. 7c ust. 3 pkt 2;
2) nie przeprowadził systematycznego szacowania ryzyka lub nie zarządził ryzykiem wystąpienia incydentu, o których mowa w art. 8 ust. 1 pkt 1;
3) nie wdrożył systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym do świadczenia usługi albo system ten nie zapewnia funkcjonalności, o których mowa w art. 8 ust. 1;
4) nie wdrożył środków technicznych i organizacyjnych uwzględniających wymagania, o których mowa w art. 8 ust. 1 pkt 2 lit. a–e;
5) nie wykonuje obowiązków, o których mowa w art. 8 ust. 1 pkt 5;

6) nie wykonuje obowiązków, o których mowa w art. 10 ust. 1;
7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1;
8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4;
9) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4a;
10) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4b;
11) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4c;
12) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5;
13) nie usuwa podatności, o których mowa w art. 32 ust. 2;
14) nie przeprowadza audytu w terminie, o którym mowa w art. 15 ust. 1 lub art. 16 ust. 1 pkt 2;
15) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 53 ust.2 pkt 1;
16) nie realizuje obowiązku, o którym mowa w art. 53c;
17) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1;
18) nie korzysta z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w celu realizacji obowiązków, o których mowa w art. 11;
19) nie wykonuje obowiązków, o których mowa w art. 67c ust 1–2 i 4.
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.”,

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

„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. 7 ust. 3, nie złożył wniosku o wpis do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1;
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 5–16, 19 i 20 oraz ust. 1a pkt 2 miało charakter jednorazowy.”,

c) uchyla się ust. 2,

d) ust. 3 otrzymuje brzmienie

„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.”,

e) dodaje się ust. 3a w brzmieniu:

„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.”,

f) ust. 4 otrzymuje brzmienie:

„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.”,

g) ust. 5 otrzymuje brzmienie:

„5. Jeżeli podmiot kluczowy albo podmiot ważny narusza przepisy ustawy, powodując:

1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi;

2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług

– organ właściwy do spraw cyberbezpieczeństwa nakłada karę w wysokości do 100 000 000 zł.”;

75) po art. 73 dodaje się art. 73a w brzmieniu:

„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. 7 ust. 3, 7, 19 lub 20,
2) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 8 ust. 1 i 4,
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. 2,
6) nie wykonuje co najmniej jednego z obowiązków o których mowa w art. 8h ust. 1–5,
7) nie wyznaczył dwóch osób do kontaktu z podmiotami kluczowymi lub podmiotami ważnymi
8) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 10 ust. 1 i 5–7,
9) nie wykonuje co najmniej jednego z obowiązków, o których mowa w art. 11

– jeżeli przemawia za tym czas, zakres lub charakter naruszenia.

2. Karze pieniężnej może także podlegać 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 niedokonanie obowiązków wskazanych w tym przepisie.

4. Kara pieniężna, o której mowa w ust. 1–3, może być wymierzona w kwocie nie większej niż 600% otrzymywanego przez ukaranego wynagrodzenia obliczanego według zasad obowiązujących przy ustalaniu ekwiwalentu pieniężnego za urlop.”;

76) art. 74 otrzymuje brzmienie:

„Art. 74.1. Karę pieniężną, o której mowa w art. 73 i art. 73a, nakłada, w drodze decyzji organ właściwy do spraw cyberbezpieczeństwa.

2. Organ właściwy do spraw cyberbezpieczeństwa może nadać decyzji, o której mowa w ust. 1, rygor natychmiastowej wykonalności w całości lub w części, jeżeli wymaga tego ochrona bezpieczeństwa lub porządku publicznego.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73 i art. 73a, 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.”;

77) uchyla się art. 75;

78) art. 76 otrzymuje brzmienie:

„Art. 76. Kara pieniężna, o której mowa w art. 73 i art. 73a, może zostać nałożona również w przypadku, gdy odpowiednio podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli przemawiają za tym czas trwania, zakres lub skutki naruszenia.”;

79) po art. 76 dodaje się art. 76a–76e w brzmieniu:

„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. 10 oraz wysokość przychodu uzyskanego z działalności gospodarczej w roku obrotowym poprzedzającym wymierzenie kary pieniężnej albo możliwości finansowe kierownika podmiotu kluczowego lub podmiotu ważnego.

2. 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.

3. 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.

4. 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 klauzulą natychmiastowej wykonalności, na odrębny rachunek bankowy wskazany w decyzji organu właściwego do spraw cyberbezpieczeństwa o wymierzeniu kary pieniężnej.

5. Kary pieniężne nieuiszczone w terminie wraz z odsetkami za zwłokę podlegają ściągnięciu w trybie określonym w przepisach o postępowaniu egzekucyjnym w administracji.

6. Organ właściwy do spraw cyberbezpieczeństwa może odstąpić od nałożenia kary pieniężnej, o której mowa w art. 73 i art. 73a, jeżeli waga naruszenia i znaczenie naruszonych przepisów jest znikome, a podmiot albo kierownik podmiotu kluczowego lub podmiotu ważnego zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę.

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:

1) w wykonaniu czynności określonych w ostrzeżeniu wydanym na podstawie art. 53 ust. 4;
2) w wykonaniu decyzji wydanych na podstawie art. 53 ust. 5 pkt 2–7.

2. Okresową karę pieniężną nakłada się, licząc od daty wskazanej w decyzji o nałożeniu tej kary.

3. Do okresowej kary pieniężnej stosuje się przepis art. 74 ust. 2.

Art. 76c. Jeżeli za czyn określony 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 i poprzestaje na pouczeniu. Jeżeli zostało wszczęte postępowanie w sprawie nałożenia kary pieniężnej stosuje się odpowiednio art. 189f ust. 1 pkt 2 ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego.

Art. 76d. Kara pieniężna, o której mowa w art. 73 ust. 1 pkt 3, może być nakładana w sposób określony w art. 14 §1b ustawy z dnia 14 czerwca 1960 r. − Kodeks

postępowania administracyjnego. Do postępowania stosuje się przepisy o postępowaniu uproszczonym.

Art. 76e. W zakresie nieuregulowanym w niniejszym rozdziale stosuje się odpowiednio przepisy działu IVa ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.”;

80) w art. 93 uchyla się ust. 8 i 23;

81) załącznik nr 1 otrzymuje brzmienie określone w załączniku nr 1 do niniejszej ustawy;

82) załącznik nr 2 otrzymuje brzmienie określone w załączniku nr 2 do niniejszej ustawy;

83) dodaje się załącznik nr 3 w brzmieniu określonym w załączniku nr 3 do niniejszej ustawy.

Art. 2. W ustawie z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej (Dz. U. z 2023 r. poz. 960, 1688 i 2029) w art. 27d w ust. 2a wyrazy „usługi przetwarzania w chmurze, o której mowa w załączniku nr 2 do ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863 i 2666),” zastępuje się wyrazami „usługi umożliwiającej dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników”.

Art. 3. W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2023 r. poz. 2383 i 2760) po art. 299h dodaje się art. 299i w brzmieniu:

„Art. 299i. § 1. Szef Krajowej Administracji Skarbowej udostępnia organom właściwym do spraw cyberbezpieczeństwa oraz Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy nieodpłatnie, w drodze teletransmisji bez konieczności składania każdorazowo pisemnych wniosków o udostępnienie, dane w zakresie niezbędnym do dokonania przez te podmioty weryfikacji wielkości przedsiębiorstwa zgodnie z art. 5 ust. 1 i ust. 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 i …).

§ 2. Dane, o których mowa w § 1, obejmują roczne zatrudnienie, a także roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz z operacji finansowych.

§ 3. Sposób udostępniania danych, o których mowa w § 1, określają porozumienia zawarte pomiędzy Szefem Krajowej Administracji Skarbowej a podmiotami, o których mowa w § 1.”.

Art. 4. W ustawie z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych (Dz. U. z 2024 r. poz. 497) w art. 50 dodaje się ust. 28 w brzmieniu:

„28. Zakład udostępnia organom właściwym do spraw cyberbezpieczeństwa i Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego działającemu na poziomie krajowym, prowadzonemu przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy, drogą elektroniczną, dane zgromadzone na koncie płatnika składek, o których mowa w art. 45, obejmujące roczną liczbę pracowników lub roczną liczbę ubezpieczonych, w zakresie niezbędnym do realizacji ich ustawowych zadań.”.

Art. 5. W ustawie z dnia z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2024 r. poz. 34) wprowadza się następujące zmiany:

1) w art. 10 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:

„5a. Do wniosku o wpis do rejestru przekazuje się dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

5b. Prezes UKE, po wpisaniu przedsiębiorcy do rejestru, przekazuje dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, ministrowi właściwemu do spraw informatyzacji do dokonania wpisu, o którym mowa w art 7 ust. 6 tej ustawy. Danych tych nie zamieszcza się w rejestrze.”;

2) uchyla się dział VIIA.

Art. 6. W ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 422) wprowadza się następujące zmiany:

1) w art. 4 po ust. 5 dodaje się ust. 5a i 5b w brzmieniu:

„5a. Do wniosku o wpis dołącza się dane, o których mowa w art. 7 ust. 3 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 i …).

5b. Po wpisie do rejestru, minister właściwy do spraw informatyzacji dane, o których mowa w art. 7 ust. 2 pkt 1–17 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, wpisuje do wykazu podmiotów kluczowych i podmiotów ważnych, o którym mowa w art. 7 ust. 1 tej ustawy. Danych tych nie zamieszcza się w rejestrze.”;

2) w art. 15 w ust. 2 skreśla się wyrazy „oraz informacje o naruszeniach bezpieczeństwa i utracie integralności, o których mowa w art. 19 ust. 2 rozporządzenia 910/2014”;

3) uchyla się art. 39;

4) w art. 46 uchyla się pkt 8.

Art. 7. W ustawie z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236) w art. 61 w pkt 3 kropkę zastępuje się średnikiem i dodaje się pkt 4 w brzmieniu:

„4) w odniesieniu do kontroli, o której mowa w art. 54 ust. 1 pkt 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.”.

Art. 8. W ustawie z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2023 r. poz. 1605 i 1720) w art. 226 w ust. 1:

1) pkt 17 otrzymuje brzmienie:

„17) obejmuje ona produkt ICT, usługę ICT lub proces ICT wskazane w rekomendacji, o której mowa w art. 33 ust. 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913, 1703 i …), stwierdzającej ich negatywny wpływ na bezpieczeństwo publiczne lub bezpieczeństwo narodowe;”;

2) w pkt 18 kropkę zastępuje się średnikiem i dodaje się pkt 19 w brzmieniu:

„19) obejmuje ona produkt ICT, którego typ został określony w decyzji w sprawie uznania dostawcy za dostawcę wysokiego ryzyka, o której mowa w art. 67b ust. 15 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa lub usługę ICT, lub proces ICT, określone w tej decyzji.”.

Art. 9. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 667) wprowadza się następujące zmiany:

1) w art. 2:

a) po ust. 4 dodaje się ust. 4a w brzmieniu:

„4a. Dotacja z budżetu państwa udzielona Funduszowi nie podlega zwrotowi.”,

b) w ust. 8 skreśla się wyrazy: „w drodze porozumienia z ministrem właściwym do spraw finansów publicznych”;

2) w art. 5 pkt 1 otrzymuje brzmienie:

„1) w CSIRT MON, CSIRT NASK, CSIRT GOV, organach właściwych do spraw cyberbezpieczeństwa, CSIRT sektorowych lub w urzędzie obsługującym Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa odpowiednio w art. 26, art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa,”.

Art. 10. 1. Do kontroli operatorów usług kluczowych i dostawców usług cyfrowych wszczętych i niezakończonych do dnia wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

2. Do postępowań o nałożenie kary pieniężnej wszczętych i niezakończonych do dnia wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

3. W przypadku gdy obsługa incydentu została rozpoczęta i nie została zakończona przed dniem wejścia w życie niniejszej ustawy, stosuje się do niej przepisy dotychczasowe.

4. Do badania, o którym mowa w art. 33 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, trwającego i niezakończonego w dniu wejścia w życie niniejszej ustawy stosuje się przepisy w brzmieniu nadanym niniejszą ustawą.

5. Rekomendacje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, o których mowa w art. 33 ust. 4 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, wydane przed dniem wejścia w życia niniejszej ustawy zachowują moc.

Art. 11. Z dniem wejścia w życie niniejszej ustawy operatorzy usług kluczowych stają się podmiotami kluczowymi.

Art. 12. Do audytu, o którym mowa w art. 15 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, niezakończonego w dniu wejścia w życie niniejszej ustawy stosuje się przepisy dotychczasowe.

Art. 13. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 66 ust. 9 ustawy zmienianej w art. 1, nie dłużej jednak niż przez okres 36 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 14. 1. Podmioty, które z dniem wejścia w życie niniejszej ustawy, spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny realizują obowiązki określone w rozdziale 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Podmioty, które z dniem wejścia w życie niniejszej ustawy, spełniają przesłanki uznania ich za podmiot kluczowy albo za podmiot ważny obowiązane są zarejestrować się w wykazie podmiotów kluczowych i podmiotów ważnych zgodnie, z harmonogramem określonym w art. 15 ust. 3 pkt 1 ustawy .

Art. 15. 1. Minister właściwy do spraw informatyzacji uruchomi wykaz podmiotów kluczowych i podmiotów ważnych, w terminie miesiąca od dnia wejścia w życie niniejszej ustawy.

2. Organ właściwy do spraw cyberbezpieczeństwa wpisuje z urzędu do wykazu podmiotów kluczowych i podmiotów ważnych operatorów usług kluczowych wpisanych przed dniem wejścia w życie niniejszej ustawy do wykazu operatorów usług kluczowych.

3. Minister właściwy do spraw informatyzacji ogłasza komunikat określający harmonogram:

1) złożenia wniosków o wpis do wykazu podmiotów kluczowych i podmiotów ważnych przez podmioty kluczowe i podmioty ważne, które w dniu wejścia w życie niniejszej ustawy spełniają przesłanki uznania za podmiot kluczowy lub podmiot ważny;
2) rozpoczęcia korzystania przez podmioty, o których mowa w pkt 1, z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1, w brzmieniu nadanym niniejszą ustawą.

4. W harmonogramie, o którym mowa w ust. 3, wskazuje się terminy dokonywania czynności przez poszczególne rodzaje podmiotów kluczowych i podmiotów ważnych.

5. Wpisy do wykazu podmiotów kluczowych i podmiotów ważnych, o których mowa w ust. 3 pkt 1, trwają do dnia 1 kwietnia 2025 r.

6. Komunikat, o którym mowa w ust. 3, może być zmieniany, jeżeli z powodów technicznych lub organizacyjnych niemożliwe jest dokonanie wpisów i rozpoczęcie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, przez podmioty kluczowe i podmioty ważne w wyznaczonym harmonogramie.

7. Komunikat, o którym mowa w ust. 3, ogłasza się w dzienniku urzędowym ministra właściwego do spraw informatyzacji.

Art. 16. Minister uruchomi funkcjonalności systemu teleinformatycznego**,** o których mowa w art. 46 ust. 1 pkt 6 i 7 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą**,** w terminie roku od dnia wejścia w życie niniejszej ustawy.

Art. 17. Do czasu wdrożenia przez ministra właściwego do spraw informatyzacji rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej doręczenie pism, na elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne w skutkach prawnych z doręczeniem przy

wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego. Jeżeli podmiot nie posiada skrzynki podawczej w ePUAP to organ właściwy do spraw cyberbezpieczeństwa doręcza pisma na adres poczty elektronicznej ujawniony w rejestrze publicznym lub podanym na stronie internetowej podmiotu jako adres do kontaktu.

Art. 18. Podmiot świadczący usługi rejestracji nazw domen:

1) dostosowuje bazy danych dotyczących rejestracji nazw domen do wymagań określonych w art. 16a ustawy zmienianej w art. 1, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy;
2) opracowuje i wdraża polityki i procedury, o których mowa w art. 16a ustawy zmienianej w art. 1, w terminie 6 miesięcy od dnia wejścia w życie niniejszej ustawy.

Art. 19. Minister właściwy do spraw informatyzacji, w terminie do dnia 17 kwietnia 2025 r., przekaże Komisji Europejskiej informacje o:

1) liczbie podmiotów kluczowych w podziale na poszczególne sektory;
2) liczbie podmiotów ważnych w podziale na poszczególne sektory;
3) rodzajach usług świadczone przez podmioty kluczowe i ważne;
4) przepisach na podstawie których podmioty kluczowe i ważne zostały wskazane.

Art. 20. Minister właściwy do spraw informatyzacji, w terminie do dnia 17 kwietnia 2025 r., przekaże Grupie Współpracy informacje o:

1) liczbie podmiotów kluczowych w podziale na poszczególne sektory;
2) liczbie podmiotów ważnych w podziale na poszczególne sektory.

Art. 21. Minister właściwy do spraw informatyzacji, w terminie 3 miesięcy od dnia wejścia w życie ustawy, przekaże Komisji Europejskiej informacje o wyznaczeniu organu do spraw zarządzania kryzysowego w cyberbezpieczeństwie wraz z jego danymi identyfikacyjnymi.

Art. 22. 1. Postanowienia umów obowiązujących w dniu wejścia w życie ustawy, uniemożliwiające przeprowadzenie badania, o którym mowa w art. 33 ust. 1b—1d ustawy zmienianej w art. 1, są nieważne.

2. Porozumienia w sprawie korzystania z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym, zawarte przed dniem wejścia w życie niniejszej ustawy, zachowują ważność do czasu ich wypowiedzenia.

Art. 23. 1. Do czasu wydania komunikatu o osiągnięciu zdolności operacyjnej przez właściwy CSIRT sektorowy podmioty kluczowe i podmioty ważne zgłaszają incydenty poważne do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV.

2. Podmiot kluczowy i podmiot ważny realizuje obowiązki, o których mowa w art. 11 ust. 3 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą od dnia następującego po dniu opublikowania komunikatu o osiągnięciu przez właściwy CSIRT sektorowy zdolności operacyjnej.

3. Przepisów ust. 1 i 2 nie stosuje się w przypadku gdy sektorowy zespół cyberbezpieczeństwa dla danego sektora został powołany przed dniem wejścia w życie ustawy.

Art. 24. CSIRT MON, CSIRT NASK lub CSIRT GOV dostosują w terminie 3 miesięcy od dnia wejścia w życie niniejszej ustawy porozumienia, o których mowa w art. 26 ust. 10 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym do przepisów art. 26 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 25. 1. Organ właściwy do spraw cyberbezpieczeństwa ustanawia CSIRT sektorowy w terminie 18 miesięcy od dnia wejścia w życie niniejszej ustawy.

2. Organ właściwy do spraw cyberbezpieczeństwa ogłasza komunikat o osiągnięciu przez CSIRT sektorowy zdolności operacyjnej w swoim dzienniku urzędowym.

3. Informacja o osiągnieciu zdolności operacyjnej przez CSIRT sektorowy jest również udostępniana na stronach internetowych:

1) urzędu obsługującego Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa,

2) CSIRT MON, CSIRT NASK, CSIRT GOV

– a także jest przekazywana za pomocą systemu teleinformatycznego, o którym mowa w art. 46 ust. 1 ustawy zmienianej w art. 1 w brzmieniu nadanym niniejszą ustawą.

Art. 26. W sprawozdaniu organu właściwego do spraw cyberbezpieczeństwa, o którym mowa w art. 44f ustawy zmienianej w art. 1, które jest sporządzane za rok, w którym został utworzony CSIRT sektorowy, zawiera się informacje dotyczące utworzenia CSIRT sektorowego oraz jego funkcjonowania.

Art. 27. Z dniem wejścia ustawy sektorowy zespół cyberbezpieczeństwa powołany na podstawie art. 44 ustawy zmienianej w art. 1 w brzmieniu dotychczasowym staje się CSIRT sektorowym.

Art. 28. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 16 – Kancelaria Prezesa Rady Ministrów, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 13 059 tys. zł;
3) w 2026 r. – 14 409 tys. zł;
4) w 2027 r. – 15 284 tys. zł;
5) w 2028 r. – 16 217 tys. zł;
6) w 2029 r. – 17 212 tys. zł;
7) w 2030 r. – 18 273 tys. zł;
8) w 2031 r. – 19 405 tys. zł;
9) w 2032 r. – 20 612 tys. zł;
10) w 2033 r. – 21 901 tys. zł.

2. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 20 – gospodarka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 15 302 tys. zł;
3) w 2026 r. – 16 855 tys. zł;
4) w 2027 r. – 17 901 tys. zł;
5) w 2028 r. – 19 017 tys. zł;
6) w 2029 r. – 20 209 tys. zł;
7) w 2030 r. – 21 480 tys. zł;
8) w 2031 r. – 22 837 tys. zł;
9) w 2032 r. – 24 285 tys. zł;
10) w 2033 r. – 25 831 tys. zł.

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

1) w 2024 r. – 0 zł;
2) w 2025 r. – 193 tys. zł;
3) w 2026 r. – 210 tys. zł;
4) w 2027 r. – 225 tys. zł;
5) w 2028 r. – 241 tys. zł;

6) w 2029 r. – 258 tys. zł;
7) w 2030 r. – 276 tys. zł;
8) w 2031 r. – 295 tys. zł;
9) w 2032 r. – 316 tys. zł;
10) w 2033 r. – 338 tys. zł.

4. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 22 – gospodarka wodna, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 11 459 tys. zł;
3) w 2026 r. – 12 656 tys. zł;
4) w 2027 r. – 13 407 tys. zł;
5) w 2028 r. – 14 208 tys. zł;
6) w 2029 r. – 15 063 tys. zł;
7) w 2030 r. – 15 973 tys. zł;
8) w 2031 r. – 16 944 tys. zł;
9) w 2032 r. – 17 979 tys. zł;
10) w 2033 r. – 19 083 tys. zł.

5. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 146 250 tys. zł;
3) w 2026 r. – 147 525 tys. zł;
4) w 2027 r. – 157 081 tys. zł;
5) w 2028 r. – 177 018 tys. zł;
6) w 2029 r. – 199 639 tys. zł;
7) w 2030 r. – 226 882 tys. zł;
8) w 2031 r. – 232 263 tys. zł;
9) w 2032 r. – 260 869 tys. zł;
10) w 2033 r. – 295 808 tys. zł.

6. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 28 – szkolnictwo wyższe i nauka, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;

2) w 2025 r. – 9 345 tys. zł;
3) w 2026 r. – 10 346 tys. zł;
4) w 2027 r. – 10 935 tys. zł;
5) w 2028 r. – 11 564 tys. zł;
6) w 2029 r. – 12 232 tys. zł;
7) w 2030 r. – 12 945 tys. zł;
8) w 2031 r. – 13 703 tys. zł;
9) w 2032 r. – 14 511 tys. zł;
10) w 2033 r. – 15 371 tys. zł.

7. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 32 – rolnictwo, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 15 302 tys. zł;
3) w 2026 r. – 16 855 tys. zł;
4) w 2027 r. – 17 901 tys. zł;
5) w 2028 r. – 19 017 tys. zł;
6) w 2029 r. – 20 209 tys. zł;
7) w 2030 r. – 21 480 tys. zł;
8) w 2031 r. – 22 837 tys. zł;
9) w 2032 r. – 24 285 tys. zł;
10) w 2033 r. – 25 831 tys. zł.

8. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 39 – transport, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 12 035 tys. zł;
3) w 2026 r. – 13 286 tys. zł;
4) w 2027 r. – 14 081 tys. zł;
5) w 2028 r. – 14 930 tys. zł;
6) w 2029 r. – 15 835 tys. zł;
7) w 2030 r. – 16 799 tys. zł;
8) w 2031 r. – 17 828 tys. zł;
9) w 2032 r. – 18 925 tys. zł;
10) w 2033 r. – 20 095 tys. zł.

9. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 46 – zdrowie, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 17 992 tys. zł;
3) w 2026 r. – 19 795 tys. zł;
4) w 2027 r. – 21 047 tys. zł;
5) w 2028 r. – 22 384 tys. zł;
6) w 2029 r. – 23 811 tys. zł;
7) w 2030 r. – 25 335 tys. zł;
8) w 2031 r. – 26 962 tys. zł;
9) w 2032 r. – 28 699 tys. zł;
10) w 2033 r. – 30 554 tys. zł.

10. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 47 – energia, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 11 266 tys. zł;
3) w 2026 r. – 12 446 tys. zł;
4) w 2027 r. – 13 182 tys. zł;
5) w 2028 r. – 13 968 tys. zł;
6) w 2029 r. – 14 805 tys. zł;
7) w 2030 r. – 15 698 tys. zł;
8) w 2031 r. – 16 649 tys. zł;
9) w 2032 r. – 17 664 tys. zł;
10) w 2033 r. – 18 745 tys. zł.

11. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 51 – klimat, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 10 306 tys. zł;
3) w 2026 r. – 11 396 tys. zł;
4) w 2027 r. – 12 059 tys. zł;
5) w 2028 r. – 12 766 tys. zł;
6) w 2029 r. – 13 519 tys. zł;
7) w 2030 r. – 14 321 tys. zł;

8) w 2031 r. – 15 176 tys. zł;
9) w 2032 r. – 16 087 tys. zł;
10) w 2033 r. – 17 058 tys. zł.

12. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 57 – Agencja Bezpieczeństwa Wewnętrznego, będący skutkiem finansowym wejścia w życie niniejszej ustawy, wynosi:

1) w 2024 r. – 0 zł;
2) w 2025 r. – 3 800 tys. zł;
3) w 2026 r. – 4 153 tys. zł;
4) w 2027 r. – 4 444 tys. zł;
5) w 2028 r. – 4 756 tys. zł;
6) w 2029 r. – 5 089 tys. zł;
7) w 2030 r. – 5 446 tys. zł;
8) w 2031 r. – 5 827 tys. zł;
9) w 2032 r. – 6 236 tys. zł;
10) w 2033 r. – 6 673 tys. zł.

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

1) w 2024 r. – 0 zł;
2) w 2025 r. – 17 992 tys. zł;
3) w 2026 r. – 19 795 tys. zł;
4) w 2027 r. – 21 047 tys. zł;
5) w 2028 r. – 22 384 tys. zł;
6) w 2029 r. – 23 811 tys. zł;
7) w 2030 r. – 25 335 tys. zł;
8) w 2031 r. – 26 962 tys. zł;
9) w 2032 r. – 28 699 tys. zł;
10) w 2033 r. – 30 554 tys. zł.

14. Szef Kancelarii Prezesa Rady Ministrów monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok

budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania dotacji celowych dla Urzędu Komisji Nadzoru Finansowego.

15. Minister właściwy do spraw gospodarki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 2, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów produkcji i przestrzeni kosmicznej;
2) CSIRT sektorowego dla sektorów produkcji i przestrzeni kosmicznej.

16. Minister właściwy do spraw gospodarki morskiej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 3, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki morskiej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla podsektora transportu wodnego;
2) CSIRT sektorowego dla podsektora transportu wodnego.

17. Minister właściwy do spraw gospodarki wodnej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 4, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw gospodarki wodnej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków;
2) CSIRT sektorowego dla sektorów zaopatrzenia w wodę pitną i jej dystrybucji oraz ścieków.

18. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 5, i dokonuje oceny wykorzystania tego limitu według stanu

na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw informatyzacji wdraża mechanizm korygujący polegający na ograniczeniu finansowania:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz zarządzania usługami ICT;
2) CSIRT sektorowego dla sektorów dostawców usług cyfrowych, infrastruktury cyfrowej oraz zarządzania usługami ICT;
3) realizacji zadań ministra w obszarze zarządzania kryzysowego w cyberprzestrzeni;
4) dotacji podmiotowej dla CSIRT NASK;
5) dotacji celowych udzielanych jednostkom podległym ministrowi właściwemu do spraw informatyzacji albo przez niego nadzorowanym w związku z powierzeniem realizacji zadań ministra;
5) działalności edukacyjnej w zakresie cyberbezpieczeństwa;
6) realizacji zadań Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

19. Minister właściwy do spraw szkolnictwa wyższego i nauki monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 6, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw szkolnictwa wyższego i nauki wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora badań naukowych;
2) CSIRT sektorowego dla sektora badań naukowych.

20. Minister właściwy do spraw rolnictwa monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 7, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw rolnictwa wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora produkcji, przetwarzania i dystrybucji żywności;
2) CSIRT sektorowego dla sektora produkcji, przetwarzania i dystrybucji żywności.

21. Minister właściwy do spraw transportu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 8, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw transportu wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora transportu;
2) CSIRT sektorowego dla sektora transportu.

22. Minister właściwy do spraw zdrowia monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 9, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw zdrowia wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora ochrony zdrowia, produkcja, wytwarzania i dystrybucji chemikaliów oraz podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro;
2) CSIRT sektorowego dla sektora ochrony zdrowia, produkcja, wytwarzania i dystrybucji chemikaliów oraz podsektora produkcji wyrobów medycznych i wyrobów medycznych do diagnostyki in vitro.

23. Minister właściwy do spraw energii monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 10, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwarty kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków minister właściwy do spraw energii wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności CSIRT sektorowego:

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora energii;
2) CSIRT sektorowego dla sektora energii.

24. Minister właściwy do spraw klimatu monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 11, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok

budżetowy limitu wydatków minister właściwy do spraw klimatu wdraża mechanizm korygujący polegający na ograniczeniu finansowania

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora gospodarowania odpadami;
2) CSIRT sektorowego dla sektora gospodarowania odpadami.

25. Szef Agencji Bezpieczeństwa Wewnętrznego monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 12, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Szef Agencji Bezpieczeństwa Wewnętrznego wdraża mechanizm korygujący polegający na ograniczeniu finansowania czynności nadzorczych wobec podmiotów publicznych w zakresie cyberbezpieczeństwa. Wdrożenie tego mechanizmu korygującego następuje w uzgodnieniu z ministrem – członkiem Rady Ministrów właściwym do spraw koordynowania działalności służb specjalnych albo z Prezesem Rady Ministrów, jeżeli minister– członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został powołany.

26. Prezes Urzędu Komunikacji Elektronicznej monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 13, i dokonuje oceny wykorzystania tego limitu według stanu na koniec każdego kwartału, a w przypadku czwartego kwartału – według stanu na dzień 20 listopada danego roku. W przypadku zagrożenia przekroczenia lub przekroczenia przyjętego na dany rok budżetowy limitu wydatków Prezes Urzędu Komunikacji Elektronicznej wdraża mechanizm korygujący polegający na ograniczeniu finansowania działalności

1) organu właściwego do spraw cyberbezpieczeństwa dla sektora poczty i podsektora komunikacji elektronicznej;
2) CSIRT sektorowego dla sektora poczty i podsektora komunikacji elektronicznej.

Art. 29. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
LEGISLACYJNYM I REDAKCYJNYM
Anna Markowska
Zastępca Dyrektora Departamentu Prawnego
w Ministerstwie Cyfryzacji
/podpisano elektronicznie/

Załączniki do ustawy z dnia …
(Dz. U. poz. …)

Załącznik nr 1

PODMIOTY 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 (Dz. U. z 2023 r. poz. 633, 1688 i 2029).
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9

		czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.
	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, 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.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne świadczący usługę o której mowa w art. 3 pkt. 6f tej ustawy.
		Uczestnicy rynku świadczący usługę, o której mowa w art. 3 pkt 11j 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, prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.
		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.

		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.
	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.
		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 2023 r. poz. 294)
	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.
	Dostawy i usługi dla sektora energii	Dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów kluczowych lub ważnych w sektorze energii.
	Jednostki nadzorowane i podległe	Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane.
		Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.
	Wodór	Operatorzy instalacji służących do produkcji wodoru.
		Operatorzy instalacji służących do magazynowania wodoru.

		Operatorzy instalacji służących do przesyłu wodoru.
		Operatorzy instalacji służących do 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 2023 r. poz. 2110).
		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy, oraz przedsiębiorca, o którym

		mowa w art. 186b ust. 1 pkt 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze, wykonujący dla przewoźników lotniczych zadania związane z kontrolą bezpieczeństwa.
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2023 r. poz. 1786, 1720 i 2029), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c, oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu, oraz operator obiektu infrastruktury

		usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE L 129 z 29.04.2004, str. 6), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2024 r. poz. 395).
		Podmiot zarządzający portem, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach

		morskich (Dz. U. z 2023 r. poz. 1796).
		Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych.
		Podmioty prowadzące na terenie portu działalność wspomagającą transport morski.
		VTS (Służba Kontroli Ruchu Statków) -–aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2023 r. poz. 1666 i 2005).
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5 i 5a ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z

		2024 r. poz. 320).
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.
Bankowość i infrastruktura rynków finansowych		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2023 r. poz. 2488).
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych.
		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 2023 r. poz. 646, 825, 1723 i 1941).
		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.
		Administratorzy kluczowych wskaźników referencyjnych.
Ochrona zdrowia		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej.
		Laboratoria referencyjne UE, o których mowa w art. 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2371.
		Podmioty prowadzące działalność badawczo-rozwojową w zakresie produktów leczniczych zdefiniowanych w art. 1 pkt 2 dyrektywy Parlamentu Europejskiego i Rady

		2001/83/WE.
		Podmioty produkujące podstawowe substancje farmaceutyczne oraz leki i pozostałe wyroby farmaceutyczne, o których mowa w sekcji C dział 21 klasyfikacji NACE Rev. 2.
		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.
		Jednostka podległa ministrowi właściwemu do spraw zdrowia albo przez niego nadzorowana, właściwa w zakresie systemów informacyjnych ochrony zdrowia.
		Narodowy Fundusz Zdrowia.
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni

		farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2022 r. poz. 2301, 605, 650, 1859 i 1938).
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) - stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.
		Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.

		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.
Zaopatrzenie w wodę pitną i jej dystrybucja		Podmiot dostarczający wodę przeznaczoną do spożycia przez ludzi, w tym przedsiębiorstwo wodociągowo-kanalizacyjne oraz podmiot prowadzący hurtową sprzedaż wody, z wyłączeniem podmiotów, dla których dostarczanie wody przeznaczonej do spożycia przez ludzi jest inną niż istotną częścią ich ogólnej działalności.
Ścieki		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.
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 usług chmurowej.
		Dostawca usług ośrodka przetwarzania danych.
		Dostawca sieci dostarczania treści.
		Dostawca usług zaufania.
		Krajowa Izba Rozliczeniowa S.A.
		Podmiot świadczący usługę rejestracji nazw domen.
	Komunikacja elektroniczna	Przedsiębiorca telekomunikacyjny.
		Podmiot świadczący usługę komunikacji interpersonalnej niewykorzystującej numerów.
Zarządzanie usługami ICT		Dostawca usług zarządzanych.
		Dostawca usług zarządzanych w zakresie cyberbezpieczeństwa.
Przestrzeń kosmiczna		Operator infrastruktury naziemnej, który wspiera świadczenie usług kosmicznych, z wyjątkiem przedsiębiorców komunikacji elektronicznej.
Administracja publiczna		jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8 i 10–13

		ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2023 r. poz. 1270, z późn. zm.)
		Instytuty badawcze
		Narodowy Bank Polski
		Bank Gospodarstwa Krajowego
		Urząd Dozoru Technicznego
		Polska Agencja Żeglugi Powietrznej
		Polskie Centrum Akredytacji
		Urząd Komisji Nadzoru Finansowego
		Międzynarodowe instytuty naukowe
		Centrum Łukasiewicz
		Instytuty działające w ramach Sieci Badawczej Łukasiewicz
		Państwowe Gospodarstwo Wodne Wody Polskie, o którym mowa w ustawie z dnia 20 lipca 2017 r. – Prawo wodne
		Polski Fundusz Rozwoju oraz 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.
		Narodowy Fundusz Ochrony Środowiska i Gospodarki

		Wodnej.
		Wojewódzkie fundusze ochrony środowiska i gospodarki wodnej.
		Spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z dnia 20 grudnia 1996 r. o gospodarce komunalnej (Dz. U. z 2021 r. poz. 679).
Produkcja, wytwarzanie i dystrybucja chemikaliów		Przedsiębiorstwo zajmujące się produkcją substancji oraz wytwarzaniem i dystrybucją substancji lub mieszanin, o których mowa w art. 3 pkt 9 i 14 rozporządzenia (WE) nr 1907/2006 Parlamentu Europejskiego i Rady.
		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.
Produkcja, przetwarzanie i dystrybucja żywności		Przedsiębiorstwa spożywcze w rozumieniu art. 3 pkt 2 rozporządzenia (WE) nr 178/2002 Parlamentu Europejskiego i Rady,

		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.
		Podmioty produkujące wyroby medyczne do diagnostyki in vitro w rozumieniu art. 2 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/746, 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.).
	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, gdzie indziej niesklasyfikowana	Przedsiębiorca prowadzący którykolwiek z rodzajów działalności gospodarczej, o których mowa w sekcji C 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.

Załącznik nr 2

PODMIOTY 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.
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, 1597, 1688, 1852 i 2029), polegające na zbieraniu odpadów, zobowiązane do uzyskania wpisu w rejestrze, o którym mowa w art. 49 ust. 1 ustawy 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.
	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 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.
	Dostawy i usługi dla sektora gospodarowania odpadami	Podmioty prowadzące działalność gospodarczą dostaw usług zarządzanych w zakresie cyberbezpieczeństwa dla podmiotów kluczowych lub podmiotów ważnych.
	Jednostki nadzorowane i podległe	Jednostki organizacyjne podległe ministrowi właściwemu do spraw klimatu lub przez niego nadzorowane.
	Zbieranie odpadów	Przedsiębiorstwa świadczące usługi w rozumieniu ustawy z dnia 14 grudnia 2012 r. o odpadach, 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.
Dostawcy usług cyfrowych		Dostawca internetowej platformy handlowej
		dostawca wyszukiwarki internetowej.
		Dostawca platformy sieci usług społecznościowych.
Badania naukowe		Organizacja badawcza.

Załącznik nr 3

KATEGORIE FUNKCJI KRYTYCZNYCH DLA BEZPIECZEŃSTWA SIECI I USŁUG

LP.	OPIS FUNKCJI	IDENTYFIKACJA POWIĄZANEJ FUNKCJI SIECIOWEJ WG STANDARDÓW 3GPP
1.	Uwierzytelnianie urządzeń użytkowników i zarządzanie prawami dostępu.	AMF – Access & Mobility management Function AUSF – Authentication Server Function
2.	Przechowywanie danych kryptograficznych i identyfikacyjnych związanych z użytkownikami końcowymi.	UDM – Unified Data Management
3.	Zarządzanie łącznością z urządzeniami użytkowników i przydzielanie zasobów radiowych.	5G Radio Base Station Baseband Unit oraz inne funkcje
4.	Ruting ruchu sieciowego pomiędzy urządzeniami użytkownika a sieciami i aplikacjami innych firm.	UPF – User Plane Function

5.	Zarządzanie połączeniami ze sprzętem użytkownika i sesjami.	SMF – Session Management Function
6.	Wdrażanie, zarządzanie i monitorowanie polityk dostępu do sieci.	PCF – Policy Control Function
7.	Przydzielanie elementu sieci dla połączeń z urządzeniami użytkowników.	NSSF – Network Slice Selection Function
8.	Rejestrowanie, autoryzacja i utrzymanie ciągłości usług sieciowych.	NRF – Network Repository Function
9.	Zabezpieczenia sieci przed oddziaływaniem aplikacji zewnętrznych.	NEF – Network Exposure Function
10.	Zabezpieczenia połączeń z innymi sieciami.	SEPP – Security Edge Protection Proxy