Projekt z dnia 31.10.2017 r.

U S T A W A

z dnia …….

o krajowym systemie cyberbezpieczeństwa [1), 2)]

Rozdział 1

Przepisy ogólne

Art. 1. Ustawa określa:

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

Art. 2. Użyte w ustawie określenia oznaczają:

1) CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym;
2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
4) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
5) cyberbezpieczeństwo – stan systemów informacyjnych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne;
6) dostawca usługi cyfrowej – podmiot świadczący usługi cyfrowe, z wyjątkiem podmiotów, o których mowa w art. 104 i art. 105 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności

---

1) Niniejsza ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

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

gospodarczej (Dz. U. z 2016 r. poz. 1829, 1948, 1997 i 2255 oraz z 2017 r. poz. 460 i 819);

7) Grupa Współpracy – grupę, o której mowa w decyzji wykonawczej Komisji 2017/179/UE z dnia 1 lutego 2017 r. ustanawiającej procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 28 z 1.02.2017, str. 73);
8) incydent – incydent krytyczny, poważny, istotny albo zwykły;
9) incydent krytyczny – incydent poważny, incydent istotny lub incydent zwykły, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, zaufania do instytucji publicznych, praw i wolności obywatelskich lub zdrowia publicznego;
10) incydent poważny – incydent zwykły, który powoduje lub może spowodować krytyczne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej albo usługi świadczonej przez podmiot publiczny;
11) incydent zwykły – każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
12) incydent istotny – zdarzenie mające istotny wpływ na świadczenie usługi cyfrowej, o którym mowa w decyzji wykonawczej Komisji Europejskiej 2017/…/UE;
13) internetowa platforma handlowa – usługę, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów z przedsiębiorcami drogą elektroniczną;
14) obsługa incydentu – czynności umożliwiające wykrywanie, klasyfikowanie, analizowanie, priorytetyzację, podejmowanie działań naprawczych oraz ograniczenie skutków incydentu;
15) operator usługi kluczowej – podmiot, w stosunku do którego została wydana decyzja o uznaniu za operatora usługi kluczowej;
16) ryzyko – wielkość charakteryzująca prawdopodobieństwo oraz skutek wystąpienia potencjalnego negatywnego zdarzenia w systemie informacyjnym lub mającego wpływ na system informacyjny, w szczególności służący do świadczenia usług kluczowych lub usług cyfrowych;

17) Sieć CSIRT – sieć składająca się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA);
18) system informacyjny – system teleinformatyczny wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
19) system teleinformatyczny – system, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570);
20) usługa przetwarzania w chmurze – usługę umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników;
21) usługa cyfrowa – usługę świadczoną drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), będącą internetową platformą handlową, wyszukiwarką internetową, lub usługą przetwarzania w chmurze;
22) wyszukiwarka internetowa – usługę, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

Art. 3. 1. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów.

2. Informacje o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4, mogą być przekazywane przez te podmioty w określonym zakresie do publicznej wiadomości w przypadku, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę trwającego incydentu lub w przypadku gdy ujawnienie incydentu z innych względów jest w interesie publicznym, w tym również, jeśli przyczyni się do zwiększenia cyberbezpieczeństwa.

Przekazywanie niezbędnych informacji do publicznej wiadomości nie może naruszać przepisów o ochronie tajemnic oraz o ochronie danych osobowych.

3. Do udostępniania informacji, o których mowa w ust. 2, nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764).

Art. 4. Krajowy system cyberbezpieczeństwa obejmuje:

1) operatorów usług kluczowych i dostawców usług cyfrowych;
2) CSIRT MON;
3) CSIRT NASK;
4) CSIRT GOV;
5) przedsiębiorców telekomunikacyjnych;
6) organy publiczne oraz jednostki je obsługujące;
7) sądy i trybunały;
8) Narodowy Bank Polski;
9) Bank Gospodarstwa Krajowego;
10) Rządowe Centrum Bezpieczeństwa;
11) jednostki podległe i nadzorowane przez organy administracji rządowej;
12) jednostki samorządu terytorialnego oraz ich związki i zrzeszenia;
13) uczelnie publiczne i Polską Akademię Nauk;
14) państwowe osoby prawne, utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego;
15) podmioty świadczące usługi z zakresu cyberbezpieczeństwa;
16) organy właściwe do spraw cyberbezpieczeństwa, o których mowa w art. 38, zwane dalej „organami właściwymi”;
17) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym”.

Rozdział 2

Usługi kluczowe i operatorzy usług kluczowych

Art. 5. 1. Operatorem usługi kluczowej jest podmiot należący do jednego z sektorów, podsektorów oraz rodzajów podmiotów wymienionych w załączniku do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy określony dla danego sektora wydał decyzję o uznaniu za operatora usługi kluczowej.

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

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

3. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 2 pkt 3, określana jest na podstawie progów istotności skutku zakłócającego z uwzględnieniem co najmniej następujących czynników:

1) liczby użytkowników zależnych od usługi świadczonej przez dany podmiot;
2) zależności innych sektorów, o których mowa w załączniku do ustawy, od usługi świadczonej przez ten podmiot;
3) wpływu, jaki incydent – jeżeli chodzi o skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne;
4) udziału podmiotu świadczącego usługę kluczową w rynku;
5) zasięgu geograficznego związanego z obszarem, którego mógłby dotyczyć incydent;
6) znaczenie podmiotu dla utrzymywania wystarczającego poziomu świadczenia usługi przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia.

4. W stosunku do podmiotu, który przestał spełniać warunki, o których mowa w ust. 1 i 2, organ właściwy wydaje decyzję o wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Decyzja może zostać wydana z urzędu lub na wniosek operatora usługi kluczowej.

5. Decyzje, o których mowa w ust. 2 i 4, podlegają natychmiastowemu wykonaniu.

Art. 6. Rada Ministrów określi, w drodze rozporządzenia, wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1, z podziałem na sektory i podsektory wymienione w załączniku do ustawy, kierując się znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej.

Art. 7. 1. Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi oraz dyrektorem Rządowego Centrum Bezpieczeństwa opracuje progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie, określonym w przepisach wydanych na podstawie art. 6, biorąc pod uwagę co najmniej czynniki, o których mowa w art. 5 ust. 3.

2. Minister właściwy do spraw informatyzacji opracowując progi istotności skutku zakłócającego, o których mowa w ust. 1, może uwzględnić czynniki sektorowe.

3. Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały. Do uchwały mają zastosowanie przepisy o ochronie informacji niejawnych.

Art. 8. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz operatorów usług kluczowych, uwzględniający podział na sektory, podsektory i rodzaje podmiotów określone w załączniku do ustawy.

2. Wykaz operatorów usług kluczowych zawiera:

1) nazwę (firmę) operatora usługi kluczowej;
2) sektor, podsektor i rodzaj podmiotu;
3) siedzibę i adres;
4) numer identyfikacji podatkowej NIP, jeżeli został nadany;
5) numer we właściwym rejestrze, jeżeli został nadany;
6) nazwę usługi kluczowej zgodną z wykazem, określonym w przepisach wydanych na podstawie art. 6;
7) datę rozpoczęcia świadczenia usługi kluczowej;
8) datę zakończenia świadczenia usługi kluczowej;
9) datę wykreślenia z wykazu operatorów usług kluczowych.

3. Wpisanie do wykazu operatorów usług kluczowych lub wykreślenie z tego wykazu następuje na wniosek organu właściwego. Wniosek zawiera informacje, o których mowa w ust. 2 pkt 1–8.

4. Wpisanie do wykazu operatorów usług kluczowych oraz wykreślenie z tego wykazu jest czynnością materialno-techniczną.

5. Informacje z wykazu operatorów usług kluczowych minister właściwy do spraw informatyzacji udostępnia na wniosek CSIRT NASK, CSIRT MON, CSIRT GOV i dyrektorowi Rządowego Centrum Bezpieczeństwa.

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

1) organom właściwym;
2) Policji;
3) Żandarmerii Wojskowej;

4) Straży Granicznej;
5) Centralnemu Biuru Antykorupcyjnemu;
6) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
7) Szefowi Agencji Bezpieczeństwa Wewnętrznego;
8) Szefowi Agencji Wywiadu;
9) sądom;
10) prokuraturze;
11) Krajowej Administracji Skarbowej.

Art. 9. 1. Operator usługi kluczowej jest obowiązany informować organ właściwy o każdej zmianie jego danych wpisanych do wykazu operatorów usług kluczowych w terminie 14 dni od zmiany tych danych.

2. Organ właściwy niezwłocznie przekazuje informacje o zmianie danych operatora usługi kluczowej ministrowi właściwemu do spraw informatyzacji.

Art. 10. 1. Operatorzy usług kluczowych zapewniają bezpieczeństwo świadczonych przez nich usług kluczowych oraz ciągłość świadczenia tych usług.

2. Operatorzy usług kluczowych wdrażają system zarządzania bezpieczeństwem, zapewniający w szczególności:

1) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemów informacyjnych wykorzystywanych przez nich do świadczenia usług kluczowych;
2) zarządzanie incydentami, w tym ich identyfikację, klasyfikację i ustalenie priorytetów obsługi incydentów, rejestrację, analizę, wyszukiwanie powiązań, podejmowanie działań naprawczych i usuwanie przyczyn wystąpienia incydentów oraz przekazywanie informacji o incydentach poważnych do właściwego CSIRT;
3) odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu analizowania i zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług kluczowych, uwzględniając najnowszy stan wiedzy oraz zapewniając poziom bezpieczeństwa systemów informacyjnych odpowiedni do istniejącego ryzyka;
4) zarządzanie ryzykiem zakłócenia ciągłości świadczenia usługi kluczowej, w tym prowadzenie jego systematycznego szacowania oraz dokumentowanie;
5) objęcie świadczonych usług kluczowych systemem monitorowania w trybie ciągłym;
6) bezpieczeństwo fizyczne i środowiskowe, w tym kontrolę dostępu;

7) utrzymanie i bezpieczną eksploatacją systemów informacyjnych ;
8) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usług kluczowych, ich dostępność, integralność, niezaprzeczalność oraz poufność;
9) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemów informacyjnych wykorzystywanych przez nich do świadczenia usług kluczowych;
10) stosowanie wewnętrznych procedur zgłaszania i obsługi incydentów;
11) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

3. Minister właściwy do spraw informatyzacji określi w drodze rozporządzenia minimalne wymagania techniczne dla środków łączności, o których mowa w ust. 2 pkt 11, kierując się potrzebą zapewnienia bezpieczeństwa środków łączności na odpowiednim poziomie.

Art. 11. 1. Operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, w ciągu sześciu miesięcy od otrzymania decyzji o uznaniu za operatora usługi kluczowej, oraz przechowują tę dokumentację przez okres 5 lat liczonych od początku roku następującego po roku jej wytworzenia.

2. Do operatorów usług kluczowych będących jednocześnie właścicielami, posiadaczami samoistnymi i zależnymi obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209), przepisów ust. 1 nie stosuje się.

3. Rada Ministrów określi, w drodze rozporządzenia, sposób tworzenia, aktualizacji, oraz zakres informacji zawartych w dokumentacji, o której mowa w ust. 1, uwzględniając potrzebę zapewnienia cyberbezpieczeństwa podczas świadczenia usług kluczowych oraz ciągłości świadczenia tych usług.

Art. 12. 1. Operatorzy usług kluczowych są obowiązani:
1) identyfikować incydent;
2) rejestrować incydenty oraz zapewniać w razie potrzeby dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV;
3) klasyfikować incydent, w tym identyfikować incydent poważny na podstawie progów uznawania incydentu za poważny;

4) zgłaszać incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
5) zapewnić obsługę incydentu zwykłego;
6) zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, w tym poinformować właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV o usunięciu podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu.

2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, nie może narażać operatora usługi kluczowej na zwiększoną odpowiedzialność.

3. W przypadku zakłócenia działania systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą dostępnych środków komunikacji elektronicznej.

4. Rada Ministrów określi w drodze rozporządzenia progi uznania incydentu za poważny w poszczególnych sektorach określonych w załączniku do ustawy, biorąc pod uwagę:

1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej,
2) czas trwania oddziaływania incydentu na świadczoną usługę,
3) zasięg geograficzny związany z obszarem, którego dotyczy incydent

- kierując się potrzebą zapewnienia ochrony przed krytycznym obniżeniem jakości lub przerwaniem ciągłości działania świadczonej usługi kluczowej.

5. Wydając rozporządzenie, o którym mowa w ust. 4, Rada Ministrów może określić progi uznania incydentu za poważny, biorąc pod uwagę także czynniki charakterystyczne dla poszczególnych sektorów, kierując się potrzebą zapewnienia ochrony przed krytycznym obniżeniem jakości lub przerwaniem ciągłości działania świadczonej usługi kluczowej w danym sektorze.

Art. 13. 1. Zgłoszenie incydentu poważnego, o którym mowa w art. 12 ust. 1 pkt 4, zawiera:

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

4) opis wpływu incydentu poważnego na usługi kluczowe, w tym:
   a) usługi kluczowe zgłaszającego, na które incydent poważny wywarł wpływ,
   b) liczbę użytkowników, na których incydent poważny miał wpływ,
   c) czas trwania incydentu poważnego,
   d) zasięg geograficzny, na którym wystąpił incydent poważny,
   e) wpływ incydentu poważnego na usługi kluczowe świadczone przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
   f) przyczynę zaistnienia incydentu poważnego oraz sposób jego przebiegu i skutki jego oddziaływania na systemy informacyjne i usługi kluczowe;
5) informacje umożliwiające właściwemu CSIRT określenie transgranicznego wpływu incydentu;
6) w przypadku incydentu, który mógł mieć wpływ na usługi kluczowe – opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne;
7) informacje o przyczynie i źródle incydentu poważnego, jeśli są znane w chwili zgłaszania;
8) informacje o podjętych działaniach zapobiegawczych;
9) informacje o podjętych środkach naprawczych;
10) inne istotne informacje.

2. W zgłoszeniu operatorzy usług kluczowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

Art. 14. 1. Operatorzy usług kluczowych mogą przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje:

1) o incydencie zwykłym;
2) o zagrożeniach cyberbezpieczeństwa;
3) dotyczące szacowania ryzyka;
4) o podatnościach na incydenty systemów informacyjnych;
5) o wykorzystywanych technologiach informatycznych.

2. Informacje, o których mowa w ust. 1, mogą być przekazywane za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1.

Art. 15. 1. Operatorzy usług kluczowych są obowiązani do:

1) wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych;

2) zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.

2. W celu realizacji zadań, o których mowa w art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1 oraz art. 14, operatorzy usług kluczowych powołują wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawierają umowy z podmiotami świadczącym usługi z zakresu cyberbezpieczeństwa, które:

1) dysponują odpowiednim potencjałem organizacyjno-technicznym pozwalającym na zapewnienie cyberbezpieczeństwa obsługiwanym podmiotom;
2) dysponują pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi;
3) stosują zabezpieczenia w celu zapewnienia dostępności, integralności, poufności i rozliczalności przetwarzanych informacji z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów.

3. Operatorzy usług kluczowych informują organ właściwy i właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV o podmiocie, z którym została zawarta umowa na świadczenie usług z zakresu cyberbezpieczeństwa.

4. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia sposób realizacji wymagań, o których mowa w ust. 2, przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, uwzględniając potrzebę zapewnienia cyberbezpieczeństwa świadczonych usług kluczowych na wysokim poziomie.

Art. 16. 1. Operatorzy usług kluczowych przeprowadzają co najmniej raz na dwa lata audyt bezpieczeństwa teleinformatycznego, zwany dalej „audytem”.

2. Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania.

3. Celem audytu jest potwierdzenie, na podstawie przeprowadzonej analizy ryzyka, że operatorzy usług kluczowych spełniają wymogi określone w ustawie.

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

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

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

6. Organ właściwy na podstawie analizy wyników audytu może wydawać wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych w audycie uchybień. W przypadku, o którym mowa w ust. 5 pkt 2, polecenia wydawane są po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa.

Rozdział 3

Dostawcy usług cyfrowych

Art. 17. 1. Świadczenie usług cyfrowych na terytorium Unii Europejskiej oraz Europejskiego Porozumienia o Wolnym Handlu (EFTA) podlega prawu Rzeczpospolitej Polskiej, jeśli dostawca usług cyfrowych ma główną siedzibę na terytorium Rzeczypospolitej Polskiej.

2. Za główną siedzibę dostawcy usług cyfrowych uznaje się inne niż Rzeczypospolita Polska państwo członkowskie Unii Europejskiej, jeżeli siedziba zarządu tego dostawcy usług cyfrowych znajduje się w tym państwie.

3. Dostawca usług cyfrowych, o ile nie posiada siedziby w jednym z państw, o których mowa w ust. 1, ale oferuje usługi cyfrowe w tych państwach i wyznacza przedstawiciela w Rzeczpospolitej Polskiej, podlega prawu Rzeczypospolitej Polskiej.

4. Jeżeli dostawca usług cyfrowych posiada główną siedzibę lub przedstawiciela na terytorium Rzeczypospolitej Polskiej, ale jego systemy informacyjne są zlokalizowane w jednym lub większej liczbie państw członkowskich Unii Europejskiej, właściwy organ Rzeczypospolitej Polskiej współpracuje z właściwymi organami tych państw członkowskich Unii Europejskiej i udziela im pomocy, odpowiednio do potrzeb.

5. Przepisy ust. 4 stosuje się odpowiednio, jeżeli dostawca usług cyfrowych posiada główną jednostkę organizacyjną lub przedstawiciela w innym państwie członkowskim Unii Europejskiej, ale jego systemy informacyjne są zlokalizowane na terytorium Rzeczypospolitej Polskiej.

Art. 18. 1. Dostawcy usług cyfrowych są odpowiedzialni za zapewnienie cyberbezpieczeństwa świadczonych przez nich usług cyfrowych.

2. Dostawcy usług cyfrowych określają i podejmują odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług cyfrowych. Środki te, uwzględniając najnowszy stan wiedzy, muszą zapewniać poziom bezpieczeństwa systemów informacyjnych odpowiedni do istniejącego ryzyka.

3. Dostawcy usług cyfrowych podejmują środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa ich systemów informacyjnych na usługi cyfrowe, w celu zapewnienia ciągłości tych usług.

Art. 19. 1. Dostawcy usług cyfrowych mają obowiązek informować CSIRT NASK o incydencie istotnym, w tym dotyczącym dwóch lub większej liczby państw członkowskich Unii Europejskiej.

2. Dostawcy usług cyfrowych mają obowiązek przekazywać operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tych dostawców usług cyfrowych, informacje dotyczące incydentu istotnego.

3. Zgłoszenia muszą zawierać informacje umożliwiające CSIRT NASK określenie istotności wpływu transgranicznego incydentu.

4. Zgłoszenie nie może narażać dostawcy usług cyfrowych na zwiększoną odpowiedzialność.

5. Obowiązek zgłoszenia incydentu istotnego ma zastosowanie, gdy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny istotności incydentu.

Art. 20. 1. Dostawcy usług cyfrowych są obowiązani:

1) identyfikować incydent;
2) rejestrować incydenty oraz zapewniać w razie potrzeby dostęp do informacji o rejestrowanych incydentach CSIRT NASK;
3) klasyfikować incydent;
4) zgłaszać incydenty istotne niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, do CSIRT NASK;
5) zapewnić obsługę incydentu istotnego i incydentu krytycznego we współpracy z CSIRT NASK .

2. W przypadku zakłócenia działania systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, dostawcy usług cyfrowych zgłaszają incydenty istotne przy pomocy dostępnych środków komunikacji elektronicznej.

Art. 21. 1. Zgłoszenie incydentu istotnego, o którym mowa w art. 20 ust. 1 pkt 4, zawiera:

1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres;
2) dane osoby składającej zgłoszenie: imię i nazwisko, numer telefonu, adres poczty elektronicznej;
3) dane osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji: imię i nazwisko, numer telefonu, adres poczty elektronicznej;
4) opis wpływu incydentu istotnego na usługi cyfrowe, zawierający informacje pozwalające na zidentyfikowanie incydentu istotnego zgodnie z art. 4 decyzji wykonawczej Komisji Europejskiej 2017/…/UE, w tym określenie istotności wpływu transgranicznego;
5) informacje o przyczynie i źródle incydentu istotnego, jeśli są znane w chwili zgłaszania;
6) informacje o podjętych działaniach zapobiegawczych;
7) informacje o podjętych środkach naprawczych;
8) inne istotne informacje.

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

Art. 22. Dostawcy usług cyfrowych mogą przekazywać do CSIRT NASK informacje, o których mowa w art. 14. Informacje te mogą być przekazywane za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1.

Art. 23. Dostawcy usług cyfrowych mogą zlecić realizację zadań, o których mowa w art. 18-20 i art. 22 oraz zadań określonych w decyzji wykonawczej Komisji Europejskiej 2017/…/UE podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa spełniającym wymogi, o których mowa w art. 15 ust. 2.

Rozdział 4

Obowiązki podmiotów publicznych

Art. 24. 1. Podmioty publiczne, o których mowa w art. 4 pkt 6-14, są obowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług.

2. Jednostki samorządu terytorialnego mogą wyznaczyć jedną osobę odpowiedzialną za cyberbezpieczeństwo usług świadczonych przez ich jednostki organizacyjne.

Art. 25. Podmioty publiczne, o których mowa w art. 4 pkt 6-14, są obowiązane:

1) identyfikować incydent;
2) klasyfikować incydent;
3) dokumentować obsługę incydentu;
4) zgłaszać incydenty poważne niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV;
5) zapewnić obsługę incydentu zwykłego;
6) zapewnić obsługę incydentu poważnego oraz incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV;
7) podejmować działania naprawcze, w tym usuwać skutki incydentu;
8) zapewnić użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Art. 26. Podmioty publiczne, o których mowa w art. 4 pkt 6-14, mogą przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje, o których mowa w art. 14. Informacje te mogą być przekazywane za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1.

Art. 27. Do podmiotu publicznego, o którym mowa w art. 4 pkt 6-14, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 2.

Rozdział 5

Zadania CSIRT

Art. 28. 1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, zapewniając spójny i kompletny system zarządzania ryzykiem w zakresie cyberbezpieczeństwa państwa oraz obsługę zgłoszonych incydentów.

2. CSIRT MON, CSIRT NASK i CSIRT GOV realizują zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniają koordynację obsługi poważnych incydentów. W uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych lub właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić im wsparcie w obsłudze lub obsługę poważnych incydentów.

3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV należy:

1) monitorowanie zagrożeń i incydentów na poziomie krajowym;
2) szacowanie ryzyka związanego z ujawnionym zagrożeniem oraz zaistniałymi incydentami;
3) przekazywanie podmiotom tworzącym krajowy system cyberbezpieczeństwa wczesnych ostrzeżeń;
4) wydawanie ogłoszeń i przekazywanie informacji dotyczących incydentów i ryzyk;
5) klasyfikacja incydentów, jako krytyczne oraz koordynowanie ich obsługi;
6) zapewnienie w razie potrzeby wsparcia w obsłudze incydentu poważnego i krytycznego operatorom usług kluczowych lub dostawcom usług cyfrowych;
7) przekazywanie Pojedynczemu Punktowi Kontaktowemu informacji o incydentach poważnych mających charakter transgraniczny zgłoszonych przez operatorów usług kluczowych lub dostawców usług cyfrowych;
8) przyjmowanie zgłoszeń o incydentach z innych państw, w tym państw członkowskich Unii Europejskiej, i dokonywanie dystrybucji tych informacji do pozostałych CSIRT i do Pojedynczego Punktu Kontaktowego;
9) zmiana klasyfikacji incydentów zwykłych, incydentów poważnych i incydentów istotnych;
10) reagowanie na zgłoszone incydenty;
11) zapewnienie dynamicznej analizy ryzyka i incydentów;
12) przekazywanie informacji technicznych dotyczących danego incydentu do pozostałych CSIRT;
13) udział w Sieci CSIRT.

4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują procedury postępowania w przypadku incydentu i wystąpienia ryzyka.

5. Do zadań CSIRT MON należy obsługa incydentów zgłaszanych przez:

1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane;
2) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, których systemy teleinformatyczne lub sieci teleinformatyczne są wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym;

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

6. Do zadań CSIRT NASK należy:

1) obsługa lub koordynacja obsługi incydentów zgłaszanych przez:
   a) państwowe osoby prawne, utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych w tym przedsiębiorstwa, banki i spółki prawa handlowego, których systemy teleinformatyczne lub sieci teleinformatyczne nie zostały wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym,
   b) agencje wykonawcze,
   c) państwowe instytucje kultury,
   d) jednostki podległe organom administracji rządowej i przez nie nadzorowane,
   e) jednostki samorządu terytorialnego i ich związki,
   f) związki metropolitarne,
   g) samorządowe zakłady budżetowe,
   h) samorządowe jednostki budżetowe,
   i) samorządowe instytucje kultury,
   j) samorządowe kolegia odwoławcze,
   k) regionalne izby obrachunkowe,
   l) uczelnie publiczne,
   m) Polską Akademię Nauk,
   n) dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 7 pkt 12,
   o) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 7 pkt 12,
   p) inne podmioty niż wymienione w lit. a-o oraz ust. 5 i 7,
   r) osoby fizyczne;
2) informowanie innych państw członkowskich Unii Europejskiej o incydentach istotnych, które dotyczą dwóch lub większej liczby państw członkowskich;
3) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności:

a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności technicznych,
b) monitoruje wskaźniki zagrożeń,
c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń,
d) prowadzi analizy strategiczne i opracowuje rekomendacje w zakresie cyberbezpieczeństwa,
e) opracowuje propozycje rozwiązań systemowych w zakresie cyberbezpieczeństwa w postaci standardów, rekomendacji i dobrych praktyk,
f) wspiera uczestników krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,
g) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,
h) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa;

4) wydawanie komunikatów o zidentyfikowanych zagrożeniach;
5) tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach;

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

1) Kancelarię Sejmu, Kancelarię Senatu, Kancelarię Prezydenta Rzeczypospolitej Polskiej;
2) Krajową Radę Radiofonii i Telewizji;
3) Narodowy Bank Polski;
4) Bank Gospodarstwa Krajowego;
5) organy administracji rządowej,
6) sądy i trybunały;
7) prokuraturę;
8) organy kontroli państwowej;
9) Narodowy Fundusz Zdrowia;
10) Zakład Ubezpieczeń Społecznych;
11) Kasę Rolniczego Ubezpieczenia Społecznego;
12) inne niż wymienione w pkt 1-11 oraz ust. 5 pkt 2 i 3 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne są wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o

którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

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

9. Zadania CSIRT NASK są finansowane z części budżetu, której dysponentem jest minister właściwy do spraw informatyzacji na podstawie umowy dotacji podmiotowej.

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

11. Porozumienia, o których mowa w ust. 8, są ogłaszane w przypadku przejęcia zadań realizowanych dotychczasowo przez:

1) CSIRT MON – w Dzienniku Urzędowym Ministra Obrony Narodowej;
2) CSIRT NASK – w Dzienniku Urzędowym ministra właściwego do spraw informatyzacji;
3) CSIRT GOV – w Dzienniku Urzędowym Agencji Bezpieczeństwa Wewnętrznego.

Art. 29. 1. CSIRT GOV jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904 i 1948).

2. W przypadku stwierdzenia, że incydent obsługiwany przez CSIRT MON albo CSIRT NASK jest związany ze zdarzeniami o charakterze terrorystycznym, obsługę takiego incydentu przejmuje CSIRT GOV.

3. CSIRT MON kieruje działaniami związanymi z obsługą incydentów w czasie stanu wojennego, o którym mowa w ustawie z dnia 22 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach naczelnego dowódcy sił zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932).

Art. 30. 1. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV informuje, na podstawie zgłoszenia uzyskanego od operatora usługi kluczowej, inne państwa członkowskie Unii Europejskiej, których dotyczy incydent, jeśli ma on istotny wpływ na ciągłość usług kluczowych świadczonych w tych państwach członkowskich.

2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje, jeśli pozwalają na to okoliczności, zgłaszającemu operatorowi usługi kluczowej informacje dotyczące działań następczych jego zgłoszenia, które mogłyby pomóc w obsłudze incydentu.

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

4. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym operatorem usługi kluczowej, przekazać do publicznej wiadomości informacje o poszczególnych incydentach, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę trwającego incydentu.

Art. 31. 1. CSIRT NASK, w stosownych przypadkach, informuje o incydencie istotnym dotyczącym dwóch lub większej liczby państw członkowskich Unii Europejskiej, państwa członkowskie których dotyczy incydent istotny.

2. CSIRT NASK może, po konsultacji ze zgłaszającym dostawcą usług cyfrowych, przekazać do publicznej wiadomości informacje o poszczególnych incydentach lub zobowiązać do tego dostawcę usług cyfrowych, w przypadku gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.

3. Przekazania informacji, o której mowa w ust. 2, mogą dokonać w stosownych przypadkach organy lub CSIRT innych zainteresowanych państw członkowskich Unii Europejskiej.

Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracują informację zawierającą elementy, o których mowa w art. 5a ust. 3 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, w obszarze zadań realizowanych przez CSIRT zgodnie z art. 24 ust. 2-7.

2. Informacja, o której mowa w ust. 1, jest opracowywana w sposób określony w przepisach wydanych na podstawie art. 5a ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym i przekazywana jako wkład do raportu cząstkowego ministra właściwego do spraw informatyzacji, o którym mowa w tych przepisach.

Art. 33. 1. Podmioty inne niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK.

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

3. Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK. Zgłoszenia takie nie mogą skutkować nałożeniem na zgłaszającego dodatkowych obowiązków.

Art. 34. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługą incydentów poważnych, incydentów krytycznych lub incydentów o charakterze ponadsektorowym i transgranicznym, a także dokonywać analiz i przechowywać niezbędne w tym zakresie dane.

2. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać czynności specjalistyczne, mające na celu likwidację szkód wyrządzonych przez incydenty, w szczególności, jeżeli incydenty mają charakter ponadsektorowy lub transgraniczny.

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

4. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do operatora usługi kluczowej lub dostawcy usługi cyfrowej o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu.

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

6. CSIRT MON, CSIRT NASK i CSIRT GOV obsługując incydenty, które doprowadziły do naruszeń danych osobowych współpracują z organem właściwym w zakresie ochrony danych osobowych.

Art. 35. 1. CSIRT MON, CSIRT GOV i CSIRT NASK, dyrektor Rządowego Centrum Bezpieczeństwa oraz minister właściwy do spraw informatyzacji mogą w zakresie i celu niezbędnym do realizacji zadań wynikających z ustawy przetwarzać dane, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z 4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”.

2. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać się danymi, o których mowa w ust. 1, w zakresie niezbędnym do realizacji zadań określonych w ustawie.

Art. 36. 1. CSIRT MON, CSIRT NASK i CSIRT GOV informują się wzajemnie oraz informują Rządowe Centrum Bezpieczeństwa o incydencie, który może spowodować wystąpienie sytuacji kryzysowej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

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

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

3. Informacja, o której mowa w ust. 1, może zawierać wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 37 ust. 1.

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

5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać do publicznej wiadomości informacje o incydentach oraz o zagrożeniach, w niezbędnym zakresie, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów.

Art. 37. 1. Tworzy się Zespół do spraw Incydentów Krytycznych, zwany dalej „Zespołem”, jako organ pomocniczy w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynujący działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa.

2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa.

3. Obsługę prac Zespołu zapewnia Rządowe Centrum Bezpieczeństwa.

4. CSIRT MON, CSIRT NASK, CSIRT GOV lub dyrektor Rządowego Centrum Bezpieczeństwa mogą zapraszać do udziału w pracach Zespołu, z głosem doradczym, przedstawicieli organów ścigania, wymiaru sprawiedliwości lub służb specjalnych.

5. W przypadku, o którym mowa w art. 36 ust. 3, albo na wniosek innego członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 36 ust. 2, dyrektor Rządowego Centrum Bezpieczeństwa zawiadamia niezwłocznie członków Zespołu o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków porozumiewania się na odległość.

6. Zespół na posiedzeniu:

1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, którego dotyczy informacja, o której mowa w art. 36 ust. 2;
2) określa zadania pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu, którego dotyczy informacja, o której mowa w art. 36 ust. 2;
3) podejmuje decyzję o wystąpieniu z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego;
4) przygotowuje opinię dla Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie wprowadzenia, zmiany lub odwołania stopni alarmowych CRP, o których mowa w ustawie z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych.

7. Prezes Rady Ministrów, niezwłocznie po przekazaniu przez dyrektora Rządowego Centrum Bezpieczeństwa wniosku, o którym mowa w ust. 6 pkt 3, zwołuje posiedzenie Rządowego Zespołu Zarządzania Kryzysowego.

8. Decyzje Zespołu oraz decyzje Rządowego Zespołu Zarządzania Kryzysowego dotyczące obsługi incydentu, którego dotyczy informacja, o której mowa w art. 36 ust. 2, są wiążące.

Rozdział 6

Organy właściwe do spraw cyberbezpieczeństwa

Art. 38. 1. Organami właściwymi są:

1) dla sektora energetycznego – minister właściwy do spraw energii;
2) dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu;
3) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i żeglugi śródlądowej;

4) dla sektora bankowego i infrastruktury rynków finansowych – minister właściwy do spraw instytucji finansowych;
5) dla sektora służby zdrowia – minister właściwy do spraw zdrowia;
6) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw środowiska;
7) dla infrastruktury cyfrowej – minister właściwy do spraw informatyzacji.

2. Organem właściwym dla dostawców usług cyfrowych jest minister właściwy do spraw informatyzacji.

Art. 39. 1. Organy właściwe:

1) prowadzą bieżącą analizę podmiotów w danym sektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
2) wydają decyzje o uznaniu podmiotu za operatora usługi kluczowej lub decyzje o wygaśnięciu decyzji o uznaniu podmiotu za operatora usługi kluczowej;
3) niezwłocznie przekazują wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych lub wykreślenie z wykazu;
4) przygotowują we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
5) monitorują stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych we właściwych im sektorach;
6) mogą prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;
7) przetwarzają informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych oraz operatorów usług kluczowych, w zakresie niezbędnym do realizacji zadań wynikających z ustawy;
8) uczestniczą w ćwiczeniach w zakresie cyberbezpieczeństwa uruchamianych w Rzeczypospolitej Polskiej lub w Unii Europejskiej.

2. Organy właściwe mogą żądać od operatorów usług kluczowych przekazania określonych informacji niezbędnych do oceny bezpieczeństwa ich systemów informacyjnych, w tym dokumentów dotyczących polityki w zakresie cyberbezpieczeństwa, uzasadniając cel ich przekazania, a po dokonaniu ich oceny wydawać wiążące polecenia wprowadzenie środków zaradczych w odniesieniu do stwierdzonych nieprawidłowości.

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

4. Powierzenie następuje na podstawie porozumienia organu właściwego. Porozumienie, wraz ze stanowiącymi jego integralną część załącznikami, podlega ogłoszeniu w dzienniku urzędowym organu właściwego.

5. W porozumieniu, o którym mowa w ust. 3, określa się zasady sprawowania przez organ właściwy kontroli nad prawidłowym wykonywaniem powierzonych zadań.

6. Organy właściwe i Pojedynczy Punkt Kontaktowy w stosownych przypadkach współpracują z organami ścigania i organem właściwym w zakresie ochrony danych osobowych.

Art. 40. 1. Organy właściwe, we współpracy z Pojedynczym Punktem Kontaktowym, na bieżąco rozpoznają potencjalnych transgranicznych operatorów usług kluczowych, badając, czy operatorzy spełniają warunki określone w art. 5 ust. 1 i 2.

2. Operator usługi kluczowej jest uznawany za transgranicznego operatora usługi kluczowej, jeśli świadczy usługę kluczową w dwóch lub większej liczbie państw członkowskich Unii Europejskiej.

3. W celu uznania operatora usługi kluczowej za operatora transgranicznego organ właściwy prowadzi uzgodnienia z organami właściwymi państw członkowskich Unii Europejskiej, na których terytorium operator świadczy usługę kluczową.

4. Organ właściwy w uzgodnieniach, o których mowa w ust. 3, przedstawia stanowisko uzgodnione z Pojedynczym Punktem Kontaktowym.

5. W przypadku, gdy operator zlokalizowany na terytorium innego państwa członkowskiego Unii Europejskiej, który nie został rozpoznany jako transgraniczny operator usługi kluczowej, świadczy usługę kluczową na terytorium Rzeczpospolitej Polskiej, organ właściwy informuje Pojedynczy Punkt Kontaktowy o zamiarze przeprowadzenia uzgodnień na ten temat.

6. Na podstawie uzgodnień, o których mowa w ust. 3, organ właściwy wydaje decyzję dotyczącą uznania danego operatora usługi kluczowej za transgranicznego operatora usługi kluczowej.

Rozdział 7

Zadania ministra właściwego do spraw informatyzacji

Art. 41. Minister właściwy do spraw informatyzacji jest odpowiedzialny za:

1) monitorowanie zagrożeń cyberbezpieczeństwa na poziomie krajowym;

2) monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizacji planów działań na rzecz jej wdrożenia;
3) rekomendowanie obszarów współpracy sektora publicznego z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa Rzeczypospolitej Polskiej poprzez upowszechnianie partnerstwa publiczno-prywatnego;
4) prowadzenie polityki informacyjnej dotyczącej krajowego systemu cyberbezpieczeństwa;
5) opracowywanie rocznych sprawozdań dotyczących:
   a) incydentów poważnych zgłaszanych przez operatorów usług kluczowych, mających wpływ na ciągłość działania świadczonych przez nich usług kluczowych w Rzeczpospolitej Polskiej oraz ciągłość działania usług kluczowych w państwach członkowskich Unii Europejskiej,
   b) zgłaszanych przez dostawców usług cyfrowych incydentów istotnych, w tym incydentów dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej zgodnie z decyzją wykonawczą Komisji Europejskiej 2017/…/UE;
6) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych, w tym:
   a) procedur postępowania w zakresie zarządzania incydentem,
   b) procedur postępowania przy zarządzaniu ryzykiem,
   c) klasyfikacji informacji, ryzyka i incydentów;
7) prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i podnoszenia świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników;
8) gromadzenie informacji o incydentach poważnych, które dotyczą lub mogą dotyczyć innego państwa członkowskiego Unii Europejskiej.

Art. 42. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie systemu teleinformatycznego wykorzystywanego:

1) jako narzędzie wspierające współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
2) do generowania i przekazywania rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
3) do zgłaszania i obsługi incydentów;

4) do szacowania ryzyka na poziomie krajowym;
5) do ostrzegania o zagrożeniach cyberbezpieczeństwa.

2. System, o którym mowa w ust. 1, umożliwia w szczególności:

1) gromadzenie informacji o podatnościach na incydenty i zagrożeniach cyberbezpieczeństwa wywołujących lub mogących wywołać incydenty;
2) rejestrowanie incydentów;
3) gromadzenie informacji o incydentach;
4) zbieranie informacji o poziomie ryzyka wystąpienia incydentu poważnego;
5) agregowanie i korelowanie pozyskiwanych informacji;
6) generowanie ostrzeżeń o zaistniałych incydentach lub możliwości wystąpienia incydentu;
7) opracowanie informacji o poziomie ryzyka dla całego terytorium Rzeczypospolitej Polskiej lub jego części;
8) prognozowanie skutków wystąpienia zagrożeń cyberbezpieczeństwa.

3. Użytkownikami systemu, o którym mowa w ust. 1, są:

1) CSIRT MON, CSIRT NASK i CSIRT GOV;
2) operatorzy usług kluczowych;
3) dostawcy usług cyfrowych w zakresie określonym w decyzji wykonawczej Komisji Europejskiej nr 2017/…/UE;
4) Prezes Urząd Komunikacji Elektronicznej w zakresie określonym w art.175a ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907);
5) Rządowe Centrum Bezpieczeństwa;
6) podmioty publiczne, o których mowa w art. 4 pkt 6-14.

4. CSIRT MON i CSIRT GOV korzystają z systemu teleinformatycznego z uwzględnieniem przepisów odrębnych dotyczących zadań Agencji Bezpieczeństwa Wewnętrznego oraz Ministra Obrony Narodowej i jednostek mu podległych lub przez niego nadzorowanych.

5. Informacje do systemu są przekazywane, jeżeli dotyczą incydentów poważnych, incydentów istotnych lub incydentów krytycznych oraz mogą być przekazywane jeśli dotyczą incydentów zwykłych.

6. Administratorem danych osobowych zgromadzonych w systemie teleinformatycznym jest minister właściwy do spraw informatyzacji.

7. Przetwarzanie danych osobowych zgromadzonych w systemie teleinformatycznym nie wymaga realizacji obowiązków, o których mowa w art. 12-22 rozporządzenia 2016/679.

8. Dane osobowe zgromadzone w systemie teleinformatycznym podlegają zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i są przechowywane wyłącznie przez okres niezbędny do realizacji zadań.

9. Informacje z systemu teleinformatycznego są udostępniane w pełnym zakresie CSIRT NASK, CSIRT MON, CSIRT GOV i dyrektorowi Rządowego Centrum Bezpieczeństwa, a w zakresie przedsiębiorców telekomunikacyjnych, także Prezesowi Urzędu Komunikacji Elektronicznej.

10. Informacje z systemu teleinformatycznego udostępnia się na wniosek, o ile są one niezbędne do realizacji ich ustawowych zadań, następującym podmiotom:

1) Policji;
2) Żandarmerii Wojskowej;
3) Straży Granicznej;
4) Centralnemu Biuru Antykorupcyjnemu;
5) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego;
6) Szefowi Agencji Wywiadu;
7) Szefowi Agencji Bezpieczeństwa Wewnętrznego;
8) Prezesowi Urzędu Komunikacji Elektronicznej;
9) sądom;
10) prokuraturze;
11) Krajowej Administracji Skarbowej.

11. Na wniosek Szefa Biura Bezpieczeństwa Narodowego udostępnia się z systemu teleinformatycznego informacje dotyczące stanu bezpieczeństwa Państwa. Zakres udostępnianych informacji nie obejmuje danych osobowych.

12. Informacje z systemu teleinformatycznego mogą być udostępniane na wniosek w zakresie ich właściwości organom właściwym oraz organowi właściwemu do spraw ochrony danych osobowych.

13. Informacje z systemu teleinformatycznego mogą być udostępniane operatorom usług kluczowych oraz dostawcom usług cyfrowych, posiadającym główną siedzibę na terytorium Rzeczypospolitej Polskiej albo którzy ustanowili w Rzeczypospolitej Polskiej przedstawiciela, w zakresie ich dotyczącym.

14. Minister właściwy do spraw informatyzacji może umożliwić dostęp do systemu teleinformatycznego w celu zgłaszania incydentów za jego pośrednictwem podmiotom

niezobowiązanym do ich zgłaszania, o ile uzna, że jest to niezbędne dla zapewnienia wysokiego poziomu cyberbezpieczeństwa.

15. Minister właściwy do spraw informatyzacji, na wniosek przedsiębiorcy telekomunikacyjnego, może zapewnić dostęp do systemu teleinformatycznego w celu realizacji obowiązków, o których mowa w art. 175a ust. 1 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne.

16. Minister właściwy do spraw informatyzacji określi w drodze rozporządzenia:

1) sposób i tryb zakładania i obsługi konta użytkownika systemu, o którym mowa w ust. 1,
2) zakres uprawień użytkowników systemu, o którym mowa w ust. 1,
3) wymogi bezpieczeństwa teleinformatycznego, które muszą spełnić podmioty krajowego systemu cyberbezpieczeństwa, aby uzyskać dostęp do systemu, o którym mowa w ust. 1

- uwzględniając konieczność zapewnienia sprawnego wykonywania zadań podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, w szczególności zgłaszania i obsługi incydentów, oraz właściwej ochrony systemu, o którym mowa w ust. 1, oraz ochrony danych osobowych zgromadzonych w tym systemie.

Art. 43. 1. Minister właściwy do spraw informatyzacji może realizować zadania, o których mowa w art. 41 i art. 42, na zasadach określonych w przepisach odrębnych, za pomocą właściwych w tym zakresie jednostek podległych lub nadzorowanych przez ministra właściwego do spraw informatyzacji.

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

Art. 44. Minister właściwy do spraw informatyzacji prowadzi Pojedynczy Punkt Kontaktowy, do którego zadań należy:

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

Art. 45. 1. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy:

1) informacje, o których mowa w art. 41 pkt 5;
2) dobre praktyki związane ze zgłaszaniem incydentów, o których mowa w art. 41 pkt 7;

3) propozycje do programu prac Grupy Współpracy;
4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju z zakresu cyberbezpieczeństwa;
5) dobre praktyki w odniesieniu do identyfikowania operatorów usług kluczowych w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.

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

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

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

Art. 46. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej:

1) niezwłocznie informacje:
   a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, o ich zadaniach oraz późniejszych zmianach w tym zakresie,
   b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa;
2) co roku informacje:

a) o liczbie operatorów usług kluczowych w odniesieniu do których prowadzono z pojedynczymi punktami kontaktowymi państw członkowskich Unii Europejskiej rozmowy na temat uznania operatorów usług kluczowych mających siedzibę w innym państwie członkowskim Unii Europejskiej za transgranicznych operatorów usług kluczowych,

b) o zlokalizowanych na terytorium Rzeczypospolitej Polskiej transgranicznych operatorach usług kluczowych, oraz o liczbie państw członkowskich Unii Europejskiej, w których świadczą oni usługi kluczowe;

3) co 2 lata informacje, umożliwiające ocenę wdrażania dyrektywy, obejmujące w szczególności:

a) środki umożliwiające identyfikację operatorów usług kluczowych,

b) wykaz usług kluczowych,

c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora,

d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych, określone w przepisach wydanych na podstawie art. 7.

4) informacje o zakresie kompetencji CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu.

Rozdział 8

Nadzór i kontrola

Art. 47. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują:

1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 15 ust. 2;

2) organy właściwe w zakresie:

a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, związanych ze świadczonymi usługami kluczowymi,

b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych i zgłaszanie incydentów, zgodnie z decyzją wykonawczą Komisji Europejskiej 2017/…/UE.

2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy lub minister właściwy do spraw informatyzacji:

1) prowadzi kontrole w zakresie, o którym mowa w ust. 1;
2) zobowiązuje do usunięcia nieprawidłowości ustalonych w wyniku kontroli;
3) nakłada kary pieniężne.

3. W stosunku do podmiotów, o których mowa w ust. 1 pkt 2 lit. b, podjęcie czynności nadzorczych następuje po uzyskaniu dowodu, że dostawca usług cyfrowych nie spełnia wymogów określonych w decyzji wykonawczej Komisji 2017/…/UE.

Art. 48. 1. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyłączeniem art. 79.

2. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 2 i 3, realizowanej wobec podmiotów:

1) będących przedsiębiorcami, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, z wyłączeniem art. 79;
2) niebędących przedsiębiorcami, stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092), określające zasady i tryb przeprowadzania kontroli.

Art. 49. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do:

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

Art. 50. 1. Kontrolowane podmioty będące przedsiębiorcami zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli,

w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych.

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

Art. 51. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń.

Art. 52. 1. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli.

2. Protokół kontroli powinien zawierać:

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 osoba prowadzącej czynności kontrolne;
4) datę rozpoczęcia i zakończenia czynności kontrolnych;
5) określenie przedmiotu i zakresu kontroli;
6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości;
7) wyszczególnienie załączników.

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

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

5. W razie zgłoszenia zastrzeżeń, o których mowa w ust. 4, osoba prowadząca czynności kontrolne dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne,

a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu.

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

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

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

Art. 53. 1. W toku kontroli, o której mowa w ust. 47 ust. 2 pkt 1, osoba prowadząca czynności kontrolne może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji.

2. Jeżeli dokonanie określonych czynności kontrolnych wymaga wiedzy specjalistycznej podmiot przeprowadzający kontrolę może włączyć do kontroli specjalistów.

Art. 54. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości.

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

Art. 55. 1. Organ właściwy dla dostawców usług cyfrowych sprawuje nadzór w zakresie zgłaszania incydentów mających istotny wpływ na świadczenie usługi cyfrowej oraz wykonywania kontroli następczej w przypadku zaistnienia incydentu, o którym mowa w decyzji wykonawczej Komisji 2017/…/UE.

2. W przypadku, gdy organ właściwy dla dostawców usług cyfrowych uzyska informację, że dostawca usług cyfrowych, który nie posiada głównej siedziby na terytorium Rzeczypospolitej Polskiej, bądź nie ustanowił przedstawiciela na terytorium Rzeczypospolitej Polskiej, nie spełnia wymagań określonych w decyzji wykonawczej Komisji 2017/…/UE, przekazuje informacje do organu właściwego w innym państwie członkowskim Unii Europejskiej, na terytorium którego posiada główną siedzibę bądź został wyznaczony przedstawiciel.

3. W ramach sprawowanego nadzoru, o którym mowa w ust. 1, organ właściwy jest uprawniony do żądania niezwłocznego udostępnienia wszystkich niezbędnych informacji w zakresie:

1) oceny cyberbezpieczeństwa dostawców usług cyfrowych, w tym dokumentów dotyczących polityki w zakresie cyberbezpieczeństwa;
2) eliminowania wszelkich przypadków niespełnienia wymogów określonych w decyzji wykonawczej Komisji Europejskiej nr 2017/…/UE;
3) podjętych działań mających na celu obsługę incydentu.

Rozdział 9

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej

Art. 56. 1. Rada Ministrów przyjmuje, w drodze uchwały, Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zwaną dalej „Strategią”.

2. Strategia określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Strategia obejmuje sektory, o których mowa w załączniku do ustawy oraz usługi cyfrowe.

3. Strategia uwzględnia w szczególności:

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

4. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z ministrami i właściwymi kierownikami urzędów centralnych.

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

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

7. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej Strategię w terminie trzech miesięcy po przyjęciu przez Radę Ministrów.

Rozdział 10

Przepisy o karach pieniężnych

Art. 57. 1. Karze pieniężnej podlega operator usługi kluczowej, który:

1) nie poinformował organu właściwego o zmianie danych, o której mowa w art. 9 ust. 1;
2) nie wdrożył systemu zarządzania bezpieczeństwem, o którym mowa w art. 10 ust. 2;
3) nie opracował dokumentacji, o której mowa w art. 11 ust. 1;
4) nie wykonuje obowiązków wynikających z art. 12 ust. 1;
5) nie wyznaczył osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych, o której mowa w art. 15 ust. 1 pkt 1;
6) nie przeprowadził audytu, o którym mowa w art. 16 ust. 1;
7) nie realizuje wiążących poleceń wprowadzenia środków zaradczych, o których mowa w art. 16 ust. 6;
8) nie usunął w wyznaczonym terminie nieprawidłowości stwierdzonych w wyniku kontroli, o której mowa w art. 47 ust. 2;
9) uniemożliwia lub utrudnia osobie przeprowadzającej czynności kontrolne wykonywanie czynności kontrolnych, o których mowa w art. 47 ust. 2 pkt 1.

2. Wysokość kary pieniężnej, o której mowa w:

1) ust. 1 pkt 1, wynosi do 1 000 zł;
2) ust. 1 pkt 9, wynosi do 5 000 zł;
3) ust. 1 pkt 5, wynosi do 10 000 zł;
4) ust. 1 pkt 3-4, 6-8, wynosi do 50 000 zł;
5) ust. 1 pkt 2, wynosi do 100 000 zł.

3. Jeżeli w wyniku kontroli organ właściwy stwierdzi, że operator usługi kluczowej uporczywie narusza przepisy ustawy powodując:

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

– organ właściwy nakłada karę w wysokości do 200 000 zł.

Art. 58. 1. Karę pieniężną, o której mowa w art. 57, nakłada w drodze decyzji organ właściwy określony dla danego sektora.

2. Przed wszczęciem postępowania w sprawie nałożenia kary pieniężnej, organ właściwy dla danego sektora może wezwać operatora usługi kluczowej do usunięcia naruszenia w wyznaczonym terminie, jeżeli przemawia za tym charakter naruszenia.

Art. 59. W sprawach nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu stosuje się przepisy działu IVa – ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257).

Rozdział 11

Zmiany w przepisach obowiązujących, przepisy przejściowe, dostosowujące i końcowe

Art. 60. W ustawie z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2016 r. poz. 1943, z późn. zm.[3)]) w art. 90u:

a) w ust. 1 pkt 6 otrzymuje brzmienie:

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

b) w ust. 4 pkt 6 otrzymuje brzmienie:

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

Art. 61. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne w art. 175a po ust. 1 dodaje się ust. 1a w brzmieniu:

„1a. Prezes UKE przekazuje informacje, o których mowa w ust. 1, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1 ustawy z dnia …. o

---

[3)] Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2016 r. poz. 1954, 1985 i 2169 oraz z 2017 r. poz. 60, 949 i 1292.

krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego zgodnie z art. 28 ust. 5-7 tej ustawy.

Art. 62. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym wprowadza się następujące zmiany:

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

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

2) w art. 9 w ust 1 po pkt 2 dodaje się pkt 2a w brzmieniu:

„2a) doradzanie w zakresie koordynacji działań CSIRT MON, CSIRT NASK i CSIRT GOV, o których mowa w ustawie z dnia…. o krajowym systemie cyberbezpieczeństwa;”;

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

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

Art. 63. Minister właściwy do spraw informatyzacji, po wejściu w życie ustawy, przekaże Komisji Europejskiej informacje:

1) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym oraz o ich zadaniach;
2) o zakresie kompetencji CSIRT, w tym o głównych elementach procedur postępowania w przypadku incydentu.

Art. 64. Organy właściwe, w terminie 60 dni od dnia wejścia w życie ustawy, przeprowadzą analizę podmiotów w danym sektorze pod kątem ich uznania za operatorów usług kluczowych, wydadzą decyzje o uznaniu za operatorów usług kluczowych oraz przekażą ministrowi właściwemu do spraw informatyzacji wnioski o wpisanie operatorów usług kluczowych do wykazu.

Art. 65. Minister właściwy do spraw informatyzacji w terminie do dnia 9 maja 2018 r. przekaże Komisji Europejskiej informacje o przepisach dotyczących kar pieniężnych przewidzianych w ustawie.

Art. 66. Minister właściwy do spraw informatyzacji w terminie do dnia 9 sierpnia 2018 r. przekaże Grupie Współpracy sprawozdanie podsumowujące na temat:

1) incydentów poważnych zgłaszanych przez operatorów usług kluczowych, mających wpływ na ciągłość działania świadczonych przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość działania usług kluczowych w państwach członkowskich Unii Europejskiej;
2) zgłaszanych przez dostawców usług cyfrowych incydentów istotnych, w tym incydentów dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej zgodnie z decyzją wykonawczą Komisji Europejskiej 2017/…/UE.

Art. 67. Minister właściwy do spraw informatyzacji w terminie do dnia 9 listopada 2018 r. przekaże Komisji Europejskiej informacje o:

1) krajowych środkach umożliwiających identyfikację operatorów usług kluczowych;
2) wykazie usług kluczowych;
3) liczbie zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o którym mowa w załączniku do ustawy, ze wskazaniem ich znaczenia w odniesieniu do tego sektora;
4) progach istotności skutku zakłócającego dla świadczonej usługi kluczowej branych pod uwagę przy kwalifikowaniu podmiotów, jako operatorów usług kluczowych, określonych w przepisach wydanych na podstawie art. 7.

Art. 68. 1. Operatorzy usług kluczowych realizują obowiązki określone w:

1) art. 10 ust. 2 pkt 5 i 8 oraz art. 12 ust. 1 – w terminie sześciu miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej;
2) art. 10 ust. 2 pkt 1-4, pkt 6-7 i pkt 9-11 oraz art. 15 ust. 1 – w terminie trzech miesięcy od dnia otrzymania decyzji o uznaniu za operatora usług kluczowych;

2. Dostawcy usług cyfrowych realizują obowiązki określone w ustawie w terminie od 1 lipca 2019 roku.

Art. 69. 1. Minister właściwy do spraw informatyzacji uruchomi system teleinformatyczny, o którym mowa w art. 42 ust. 1, do dnia 1 stycznia 2021 r.

2. Do czasu uruchomienia systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, operatorzy usług kluczowych, dostawcy usług cyfrowych, CSIRT MON, CSIRT NASK oraz

CSIRT GOV zgłaszają incydenty oraz wymieniają się informacjami przy pomocy dostępnych środków komunikacji elektronicznej oraz przetwarzają informacje w dostępnych systemach teleinformatycznych.

Art. 70. 1. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej zostanie przyjęta do dnia 31 października 2019 r.

2. Do czasu przyjęcia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, o której mowa w art. 55, jej rolę pełni uchwała Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.

Art. 71. 1. Maksymalny limit wydatków z budżetu państwa będących skutkiem finansowym wejścia w życie niniejszej ustawy wynosi:

1) w 2017 r. - 1.920 tys. zł;
2) w 2018 r. - 19.950 tys. zł;
3) w 2019 r. - 16.800 tys. zł;
4) w 2020 r. - 16.010 tys. zł;
5) w 2021 r. - 26.040 tys. zł;
6) w 2022 r. - 26.040 tys. zł;
7) w 2023 r. - 26.040 tys. zł;
8) w 2024 r. - 26.040 tys. zł;
9) w 2025 r. - 26.040 tys. zł;
10) w 2026 r. – 26.040 tys. zł.

2. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, oraz wdraża mechanizmy korygujące, o których mowa w ust. 3.

3. W przypadku, gdy wielkość wydatków po pierwszym półroczu danego roku budżetowego wyniesie więcej niż 65% limitu wydatków przewidzianych na dany rok, dysponent środków obniża wielkość środków przeznaczonych na wydatki w drugim półroczu o kwotę stanowiącą różnicę pomiędzy wielkością tego limitu a kwotą przekroczenia wydatków.

4. W przypadku, gdy wielkość wydatków w poszczególnych miesiącach zgodna jest z planem finansowym przepisu ust. 3 nie stosuje się.

Art. 72. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

Za zgodność pod względem prawnym, legislacyjnym i redakcyjnym

- Katarzyna Prusak-Górniak

Dyrektor Departamentu Prawnego MC

/-podpisano elektronicznie-/

Załącznik do ustawy z dnia …...
(poz. …)

SEKTORY I PODSEKTORY ORAZ PODZAJE PODMIOTÓW

Sektor	Podsektor (jeżeli występuje)	Rodzaj podmiotu
Energetyka	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2017 r. poz. 220, 791, 1089 i 1387), posiadające koncesję na obrót energią elektryczną.
		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 elektroenergetycznego.
		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 elektroenergetycznego.
	Ropa naftowa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na przesyłanie paliw ciekłych.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na dystrybucję paliw ciekłych, na wytwarzanie paliw ciekłych, na magazynowanie lub przeładunek paliw ciekłych, na obrót paliwami ciekłymi lub na obrót paliwami ciekłymi z zagranicą.
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na obrót gazem ziemnym z zagranicą lub na obrót paliwami gazowymi.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 2 pkt 26 ustawy z dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym (Dz. U. z 2017 r. poz. 1210 i 1387).
		Przedsiębiorstwo energetyczne, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lutego 2007 r o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12, 26 i 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadający koncesję na obrót gazem ziemnym z zagranicą lub na obrót paliwami gazowymi, jak również przedsiębiorstwo energetyczne, o którym mowa w art. 2 pkt 26 i 27 ustawy z dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na skraplanie i regazyfikację gazu ziemnego.
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002.
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2017 poz. 959 i 1089).
		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.
		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 2016 r. poz. 1727, 1823, 1920, 1923, 1948 i 2138 oraz z 2017 r. poz. 60, 1089 i 1566), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy.
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym.
		Operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym.
	Transport wodny	Armator morski transportu pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady, z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.
		Armator, o którym mowa w art. 5 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej (Dz. U. z 2013 r. poz. 1458, z 2015 r. poz. 1690 i 1960, z 2016 r. poz. 1954 oraz z 2017 r. poz. 1566).

		Podmiot zarządzający, o których mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz. U. z 2010 r. Nr 33, poz. 179, z 2015 r. poz. 1569 i 1642, z 2016 r. poz. 1954 oraz z 2017 r. poz. 785).
		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 2016 poz. 281 i 1948 oraz z 2017 r. poz. 32, 60, 785 i 1215).
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5, 5a, ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2016 r. poz. 1440, 1920, 1948 i 2255 oraz z 2017 r. poz. 191 i 1089).
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2016 r. poz. 1440, 1920, 1948 i 2255 oraz z 2017 r. poz. 191 i 1089).
		Drogowa spółka specjalnego przeznaczenia w rozumieniu ustawy z dnia 12 stycznia 2007 r. o drogowych spółkach specjalnego przeznaczenia (Dz. U. z 2015 r. poz. 1502 oraz z 2016 r. poz. 2260) wykonująca zadania, o których mowa w art. 13hb ust. 3 ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2016 r. poz. 1440, 1920, 1948 i 2255 oraz z 2017 r. poz. 191 i 1089).
		Operator, o którym mowa w art. 13hd ust. 1 ustawy 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 2016 poz. 1988, 1997 i 2260 oraz z 2017 r. poz. 85, 724, 768, 791,1089 i 1948).
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Instytucja finansowa, o której mowa w art. 4 ust. 1 pkt 7 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.
		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe.
		Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy – Prawo bankowe.
		Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2016 r. poz. 1910, 1948 i 1997 oraz z 2017 r. poz. 60, 85, 245, 768 i 1089).
		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 2016 r. poz. 1636, 1948 i 1997 oraz z 2017 r. poz. 724, 768, 791 i 1089).
		Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.
Służba zdrowia		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z

		2016 r. poz. 1638, 1948 i 2260).
Zaopatrzenie w wodę pitną i jej dystrybucja		Przedsiębiorstwo wodno-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2017 r. poz. 328 i 1566).
Infrastruktura cyfrowa		Podmiot, który świadczy usługi DNS.
		Podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiącego obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego.
		Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).