Bird & Bird

Projekt ustawy

o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw

w wersji dla podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych

22 listopada 2024 r.

3 października 2024 r. został opublikowany projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który ma implementować do polskiego prawa dyrektywę NIS2.

W odniesieniu do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych przepisy projektu zawierają nowy artykuł 8i zawierający listę **24 przepisów, które się stosuje bezpośrednio** do tej kategorii podmiotów i **6 przepisów, które się stosuje odpowiednio**.

Niestety, omawiany przepis jest całkowicie nieczytelny, gdyż uniemożliwia szybkie ustalenie, w jakim konkretnie zakresie przepisy te będą miały zastosowanie do podmiotów z sektora bankowego i infrastruktury rynków finansowych.

Przygotowaliśmy zatem wyciąg z projektu ustawy, który zawiera tylko przepisy, do których odsyła art. 8i, co pozwala łatwo ustalić realny wpływ projektu ustawy i implementacji NIS2 na sektor finansowy.

Mamy nadzieję, że nasz dokument będzie przydatny w Państwa analizach dotyczących dostosowania do nowych wymogów regulacyjnych wynikających z projektu ustawy o krajowym systemie cyberbezpieczeństwa.

Instrukcja przeglądu dokumentu

1. Każdy artykuł, do którego odsyła art. 8i, zawiera hyperlink.
2. **CRTL + kliknięcie** w artykuł powoduje przesunięcie widoku na jego treść.
3. **CRTL + HOME** powoduje przesunięcie widoku na początek dokumentu.
4. Kolorem czerwonym zostały oznaczone fragmenty ustawy, które nie znajdują się w nowelizacji (gdyż projekt nowelizacji ich nie zmienia), a do których odsyła art. 8i.

5 Jeżeli art. 8i odsyła do całej treści artykułu, a podana niżej treść przepisu uwzględnia tylko poszczególne ustępy, oznacza to, że projekt nowelizacji uchyla nieuwzględnione ustępy.

ART. 8I USTAWY O ZMIANIE USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA ORAZ NIEKTÓRYCH INNYCH USTAW

Art. 8i ust. 1

Do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych **nie stosuje się** przepisów ustawy dotyczących systemu zarządzania bezpieczeństwem informacji lub zgłaszania poważnych incydentów, **z wyjątkiem: PRZEPISY WYMIENIONE W TREŚCI ART. 8I**

Art. 3a

Art. 5a ust. 1

Art. 7-7m

art. 8 ust. 1 pkt 1 i pkt 2 lit. j

art. 8h

art. 9

art. 11 ust. 1 pkt 5 i 6

art. 13

art. 15

art. 16

art. 26a ust. 2–4

art. 32

art. 33 ust. 5, 7 i 8

art. 36a

art. 36b

art. 37

art. 43

art. 45 ust. 3

art. 46 ust. 1 pkt 1, 2, 4–7

art. 67a

art. 67c

art. 67d

art. 67g–67i

Art. 8i ust. 2.

Do podmiotów kluczowych i podmiotów ważnych z sektora bankowego i infrastruktury rynków finansowych **stosuje się odpowiednio** przepisy **art. 8c**

art. 8d

art. 8e

art. 8f

art. 12 ust. 7

art. 31 ust. 1

Art. 8i ust. 3

Przepisy rozdziałów 11 [Nadzór i kontrola podmiotów kluczowych i podmiotów ważnych] i 14 [Przepisy o karach pieniężnych] ustawy stosuje się do podmiotów, o których mowa w ust. 1, w zakresie **PRZEPISY WYMIENIONE W TREŚCI ART. 8I**

Art. 3a

Art. 5 ust. 1- 3

Art. 5a ust. 1

Art. 7-7m

art. 8 ust. 1 pkt 1 i pkt 2 lit. j

art. 8h

art. 9

art. 11 ust. 1 pkt 5 i 6

art. 13

art. 15

art. 16

art. 26a ust. 2–4

art. 32

art. 33 ust. 5, 7 i 8

art. 36a

,**art. 36b**

art. 37

art. 43

art. 45 ust. 3

art. 46 ust. 1 pkt 1, 2, 4–7

art. 67a

art. 67c

art. 67d

art. 67g–67i

oraz stosowanych odpowiednio przepisy **art. 8c**

art. 8d

art. 8e

art. 8f

art. 12 ust. 7

art. 31 ust. 1

PRZEPISY WYMIENIONE W TREŚCI ART. 8l

Art. 3a

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

Art. 5 ust. 1- 3

Art. 5.

1. Podmiotem kluczowym jest:

1) osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej wskazana w załączniku nr 1 do ustawy, która przewyższa wymogi dla średniego przedsiębiorstwa określone w art. 2 ust. 1 załącznika I do rozporządzenia Komisji (UE) nr 651/2014 z dnia 17 czerwca 2014 r. uznającego niektóre rodzaje pomocy za zgodne z rynkiem wewnętrznym w zastosowaniu art. 107 i 108 Traktatu (Dz. Urz. UE L 187 z 26.06.2014, str. 1, z późn. zm.[1)]), zwanego dalej „rozporządzeniem 651/2014/UE”;

2) przedsiębiorca komunikacji elektronicznej, który co najmniej spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;

[1)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 329 z 15.12.2025, str. 28, Dz. Urz. UE L 149 z 07.06.2016, str. 10, Dz. Urz. UE L 156 z 20.06.2017, str. 1, Dz. Urz. UE L 26 z 31.01.2018, str. 53, Dz. Urz. UE L 215 z 07.07.2020, str. 3, Dz. Urz. UE L 89 z 16.03.2021, str. 1, Dz. Urz. UE L 270 z 29.07.2021, str. 39, Dz. Urz. UE L 119 z 05.05.2023, str. 159 oraz Dz. Urz. UE L 167 z 30.06.2023, str. 1.

3) dostawca usług zarządzanych w zakresie cyberbezpieczeństwa, który co najmniej spełnia wymogi dla małego albo średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE albo je przewyższa;

4) niezależnie od wielkości podmiotu:

   a) dostawca usług DNS,

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

   c) podmiot krytyczny,

   d) podmiot publiczny,

   e) podmiot zidentyfikowany jako podmiot kluczowy na podstawie art. 7l ust. 2 pkt 1,

   f) państwowa osoba prawna zidentyfikowana jako podmiot kluczowy na podstawie art. 7m,

   g) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 1 do ustawy z nazwy albo poprzez określenie jego rodzaju,

   h) podmiot będący operatorem obiektu energetyki jądrowej, o którym mowa w art. 2 pkt 2 ustawy z dnia 29 czerwca 2011 r. o przygotowaniu i realizacji inwestycji w zakresie obiektów energetyki jądrowej oraz inwestycji towarzyszących (Dz. U. z 2024 r. poz.1410),

   i) 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 2 do ustawy, która spełnia wymogi dla średniego przedsiębiorcy określone w art. 2 ust. 1 załącznika I rozporządzenia 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. 2 i 3 załącznika I do rozporządzenia 651/2014/UE;

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

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

6) podmiot, który nie jest przedsiębiorcą, a jest wskazany w załączniku nr 2 do ustawy z nazwy albo poprzez określenie jego rodzaju.

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

Art. 5a ust. 1

Art. 5a. 1. Podmiot kluczowy i podmiot ważny podlega obowiązkom wynikającym z ustawy, jeżeli posiada jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej.

Art. 7-7m

Art. 7.

1. Minister właściwy do spraw informatyzacji prowadzi wykaz podmiotów kluczowych i podmiotów ważnych, zwany dalej „wykazem”, w celu:

1) identyfikacji podmiotów kluczowych i podmiotów ważnych;

2) zapewnienia wymiany informacji w zakresie cyberbezpieczeństwa, w tym o incydentach, podatnościach i cyberzagrożeniach między podmiotami kluczowymi i podmiotami ważnymi a CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowymi i organami właściwymi do spraw cyberbezpieczeństwa;

3) umożliwienia prowadzenia czynności nadzorczych nad podmiotami kluczowymi i podmiotami ważnymi.

2. Minister właściwy do spraw informatyzacji jest administratorem danych, w tym danych osobowych, gromadzonych w wykazie.

3. Wykaz zawiera:

1) nazwę (firmę) podmiotu kluczowego lub podmiotu ważnego;

2) sektor, podsektor i rodzaj lub rodzaje podmiotu, zgodnie z załącznikiem nr 1 lub 2 do ustawy;

3) siedzibę i adres do korespondencji;

4) adres do doręczeń elektronicznych, jeżeli został wpisany do bazy adresów elektronicznych;

5) adres poczty elektronicznej;

6) numer identyfikacji podatkowej (NIP), jeżeli został nadany;

7) numer identyfikacyjny podmiotu publicznego w krajowym rejestrze urzędowym podmiotów gospodarki narodowej (REGON), jeżeli został nadany;

8) numer we właściwym rejestrze działalności regulowanej, jeżeli został nadany;

9) zakres publicznych adresów IP wykorzystywanych przez podmiot kluczowy lub podmiot ważny w sposób ciągły;

10) domeny internetowe wykorzystywane przez podmiot kluczowy lub podmiot ważny w sposób ciągły;

11) dane osób do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa zawierające: imię i nazwisko, numer telefonu służbowego oraz służbowy adres poczty elektronicznej, a w przypadku osoby, która będzie pełnić rolę administratora konta podmiotu w systemie teleinformatycznym, o którym mowa w art. 46 ust. 1, dodatkowo numer PESEL;

12) numer telefonu przyporządkowany do wykonywanej działalności;

13) deklarację podmiotu kluczowego lub podmiotu ważnego czy spełnia kryteria mikro-przedsiębiorcy, małego przedsiębiorcy, średniego przedsiębiorcy, o którym mowa w art. 2 ust. 1 załącznika I do rozporządzenia 651/2014/UE, albo przekracza te kryteria;

14) informację określającą, w których państwach członkowskich Unii Europejskiej podmiot kluczowy lub podmiot ważny wykonuje działalność wraz z określeniem rodzaju 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 zawierającymi 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. 5a ust. 6, wraz z danymi kontaktowymi do tego przedstawiciela obejmujące:

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

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

17) informację o zawarciu przez podmiot kluczowy lub podmiot ważny porozumienia, o którym mowa w art. 8h ust. 6;

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

19) wskazanie organu właściwego do spraw cyberbezpieczeństwa 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) podstawę prawną wpisania do wykazu;

25) datę wykreślenia z wykazu.

4. Do danych, o których mowa w ust. 3, 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).

Art. 7a.

1. Dane, o których mowa w art. 7 ust. 3 pkt 18–25, uzupełnia minister właściwy do spraw informatyzacji.

2. W przypadku:

1) przedsiębiorców telekomunikacyjnych,

2) dostawców usług zaufania,

3) podmiotów publicznych,

4) podmiotów krytycznych

– minister właściwy do spraw informatyzacji wpisuje dane, o których mowa w art. 7 ust. 3 pkt 1–8 oraz pkt 18–25, do wykazu dotyczące tych podmiotów w oparciu o dane zawarte w rejestrach publicznych, bazie adresów elektronicznych lub przekazane przez właściwe organy nadzorcze.

Art. 7b.

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

2. Minister właściwy do spraw informatyzacji wzywa podmioty kluczowe lub podmioty ważne, o których mowa w art. 7a ust. 2, o uzupełnienie brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia wezwania, pod rygorem nałożenia kary pieniężnej.

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

1) podstawę prawną wpisania do wykazu;

2) numer podmiotu w wykazie;

3) dane podmiotu wpisane do wykazu oraz wskazanie źródła ich pochodzenia;

4) brakujące dane, które podmiot musi uzupełnić.

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

5. Zawiadomienie o wpisie do wykazu, z urzędu, oraz wezwanie, o którym mowa w ust. 2, doręcza się w sposób określony w dziale I rozdziale 8 ustawy z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).

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

Art. 7c.

1. Podmiot kluczowy i podmiot ważny składają wniosek o wpis w wykazie, w terminie 3 miesięcy od dnia spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

2. Wniosek o wpis do wykazu zawiera dane, o których mowa w art. 7 ust. 3 pkt 1–17.

3. Podmiot kluczowy i podmiot ważny składają wniosek o zmianę wpisu w wykazie, o którym mowa w ust. 1, w zakresie danych, o których mowa w art. 7 ust. 3 pkt 1–17, w terminie 14 dni od dnia ich zmiany.

4. Wniosek o zmianę wpisu w wykazie, o którym mowa w ust. 3, zawiera wskazanie zmienianych danych, numer w tym wykazie oraz oświadczenie, o którym mowa w ust. 5.

5. Wniosek o wpis, zmianę wpisu albo o wykreślenie z wykazu zawiera oświadczenie kierownika podmiotu kluczowego lub podmiotu ważnego o następującej treści: „Świadomy odpowiedzialności karnej za złożenie fałszywego oświadczenia wynikającej z art. 233 § 6 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.

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

7. W przypadku działania przez pełnomocnika wniosek zawiera pełnomocnictwo w postaci elektronicznej podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. W przypadku pełnomocnika lub prokurenta podmiotu ujawnionego w Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub w Krajowym Rejestrze Sądowym nie dołącza się pełnomocnictwa. Od pełnomocnictwa, o którym mowa w zdaniu pierwszym, nie pobiera się opłaty skarbowej.

Art. 7d.

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

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

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

1) nie zawiera danych podlegających wpisowi zgodnie z art. 7 ust. 3 pkt 1–17;

2) dotyczy podmiotu kluczowego lub podmiotu ważnego już wpisanego do wykazu;

3) nie zawiera oświadczeń, o których mowa w art. 7c ust. 5;

4) nie został podpisany.

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

1) nie zawiera nazwy podmiotu oraz numeru w wykazie;

2) wskazania danych zmienianych;

3) nie zawiera oświadczeń, o których mowa w art. 7c ust. 5;

4) nie został podpisany.

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

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

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

Art. 7e.

Minister właściwy do spraw informatyzacji, co najmniej raz w roku, aktualizuje dane zawarte we wpisach w wykazie na podstawie danych pozyskanych z publicznie dostępnych rejestrów publicznych.

Art. 7f.

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

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

1) podmiot wpisany do wykazu nie jest podmiotem kluczowym albo podmiotem ważnym;

2) podmiot wpisany do wykazu utracił status podmiotu kluczowego albo podmiotu ważnego po wpisie do wykazu.

3. Podmiot kluczowy i podmiot ważny składa wniosek o wykreślenie z wykazu w zakresie sektora, podsektora lub rodzaju działalności, jeżeli przestał spełniać przesłanki uznania za podmiot kluczowy lub podmiot ważny w tym sektorze lub podsektorze dla określonego rodzaju działalności. Wniosek o wykreślenie z wykazu zawiera uzasadnienie.

4. Organ właściwy do spraw cyberbezpieczeństwa rozpatruje wniosek w terminie miesiąca. Organ właściwy do spraw cyberbezpieczeństwa odmawia wykreślenia podmiotu z wykazu, jeżeli podmiot nadal spełnia przesłanki uznania za podmiot kluczowy lub podmiot ważny.

5. Odmowa wykreślenia jest inną czynnością z zakresu administracji publicznej, na którą przysługuje skarga do sądu administracyjnego.

6. W przypadku niewyrażenia odmowy wykreślenia z wykazu w terminie miesiąca organ właściwy do spraw cyberbezpieczeństwa wykreśla podmiot z wykazu w odpowiednim zakresie.

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

Art. 7g.

1. Dane, o których mowa w art. 7 ust. 3, 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.

2. Dane, o których mowa w art. 7 ust. 3, 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) Najwyższej Izbie Kontroli;

7) Policji;

8) Prezesowi Urzędu Lotnictwa Cywilnego;

9) Prezesowi Urzędu Ochrony Danych Osobowych;

10) Prezesowi Urzędu Transportu Kolejowego;

11) Prokuratorii Generalnej Rzeczypospolitej Polskiej;

12) prokuraturze;

13) sądom;

14) Służbie Kontrwywiadu Wojskowego;

15) Służbie Ochrony Państwa;

16) Służbie Wywiadu Wojskowego;

17) Straży Granicznej;

18) Żandarmerii Wojskowej.

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

4. Informacja o zmianie wpisu w wykazie oraz o wykreśleniu podmiotu z wykazu jest przechowywana przez 5 lat od zaistnienia zdarzenia wraz z określeniem czasu dokonania zmiany i wykreślenia.

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

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

Art. 7j.

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

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

3. Organ właściwy do spraw cyberbezpieczeństwa zawiadamia podmiot o wpisie do wykazu na podstawie ust. 1 oraz wzywa ten podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia otrzymania zawiadomienia, pod rygorem nałożenia kary pieniężnej.

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

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

Art. 7k.

1. Organ właściwy do spraw cyberbezpieczeństwa może weryfikować dane zawarte we wpisie w wykazie ze stanem faktycznym. Weryfikacja odbywa się za pomocą danych zawartych w publicznie dostępnych rejestrach publicznych.

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. Do doręczenia wezwania stosuje się przepis art. 7j ust. 4.

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

Art. 7l.

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, która nie podlega obowiązkom z ustawy zgodnie z art. 5, jeżeli:

1) jest podmiotem określonym w załączniku nr 1 lub 2 do ustawy;

2) spełnia chociaż jedną z poniższych przesłanek:

a) jako jedyna świadczy, za pomocą systemu informacyjnego, usługę, która ma kluczowe znaczenie dla krytycznej działalności społecznej lub gospodarczej,

b) zakłócenie świadczenia, za pomocą systemu informacyjnego, usługi przez nią spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego,

c) zakłócenie świadczenia, za pomocą systemu informacyjnego, usługi przez nią spowoduje ryzyko systemowe zaprzestania świadczenia usług przez podmioty kluczowe lub podmioty ważne lub

d) świadczenie przez nią, za pomocą systemu informacyjnego, usługi ma istotne znaczenie na poziomie krajowym lub województwa lub ma znaczenie dla dwóch lub więcej sektorów określonych w załączniku nr 1 lub 2 do ustawy.

2. Podmiot uznaje się za:

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

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

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

1) określa sektor do jakiego został przypisany podmiot;

2) wzywa podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania, o którym mowa w ust. 3 pkt 2, stosuje się przepis art. 7b ust. 3.

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

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

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

1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 12 miesięcy,

2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.

Art. 7m.

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

1) którego zakłócenie spowoduje poważne zagrożenie dla bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego, obronności lub zdrowia publicznego lub

2) które ma istotne znaczenie na poziomie krajowym.

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

3. Minister wzywa podmiot do uzupełnienia brakujących danych w wykazie, w terminie 2 miesięcy od dnia doręczenia decyzji, pod rygorem nałożenia kary pieniężnej.

4. Do wezwania, o którym mowa w ust. 3, stosuje się przepis art. 7b ust. 3.

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

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

1) realizuje obowiązki, o których mowa w rozdziale 3, w terminie 6 miesięcy,

2) zapewnia przeprowadzenie po raz pierwszy audytu, o którym mowa w art. 15 ust. 1, w terminie 24 miesięcy

– od dnia doręczenia tej decyzji.

---

art. 8 ust. 1 pkt 1 i pkt 2 lit. j

Art. 8.

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

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;

2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności:

j) podstawowe zasady cyberhigieny,

---

art. 8h

Art. 8h.

1. Podmioty kluczowe i podmioty ważne mogą wymieniać między sobą informacje dotyczące cyberbezpieczeństwa, w tym informacje o cyberzagrożeniach, potencjalnych zdarzeniach dla cyberbezpieczeństwa, podatnościach, technikach i procedurach, oznakach naruszenia integralności systemu informacyjnego, wrogich taktykach, a także informacje o grupach przestępczych, ostrzeżenia dotyczące cyberbezpieczeństwa i zalecenia dotyczące konfiguracji narzędzi bezpieczeństwa mających wykrywać cyberataki.

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

1) ma na celu zapobieganie incydentom, ich wykrywanie, reagowanie na nie, przywracanie normalnego działania po incydentach lub łagodzenie ich skutków lub

2) zwiększa poziom cyberbezpieczeństwa, w szczególności przez podnoszenie świadomości na temat cyberzagrożeń, ograniczanie lub utrudnianie ich rozprzestrzeniania się, eliminowanie i ujawnianie podatności, techniki wykrywania cyberzagrożeń, ograniczania ich zasięgu i zapobiegania im, strategie ograniczania ryzyka, etapy reagowania i przywracania normalnego działania lub sprzyjanie współpracy między podmiotami publicznymi i prywatnymi w badaniach nad cyberzagrożeniami.

3. Wymiana informacji, ostrzeżeń i zaleceń, o których mowa w ust. 1, odbywa się 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. 6.

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

6. Podmioty kluczowe, podmioty ważne, CSIRT MON, CSIRT NASK, CSIRT GOV, CSIRT sektorowy lub organizacje społeczne zrzeszające podmioty kluczowe lub podmioty ważne 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.

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

---

art. 9

Art. 9.

1. Podmiot kluczowy i podmiot ważny:

1) wyznacza co najmniej dwie osoby odpowiedzialne za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa;

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) zapewnia użytkownikowi usługi możliwość zgłoszenia cyberzagrożenia, incydentu lub podatności związanych ze świadczoną usługą;

4) po uzyskaniu wpisu podmiotu do wykazu rozpoczyna korzystanie z systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, w zakresie, o którym mowa w ust. 1 tego przepisu, w terminie o którym mowa w art. 46 ust. 4.

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

---

art. 11 ust. 1 pkt 5 i 6

art. 11

1. Podmiot kluczowy i podmiot ważny:

5) współdziała podczas obsługi incydentu poważnego i incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK, CSIRT GOV lub CSIRT sektorowym, przekazując niezbędne dane, w tym dane osobowe

6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy do spraw cyberbezpieczeństwa.

---

art. 13

Art. 13.

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

1) innych incydentach;

2) cyberzagrożeniach;

3) wynikach szacowania ryzyka;

4) podatnościach;

5) potencjalnych zdarzeniach dla cyberbezpieczeństwa;

6) wykorzystywanych technologiach.

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

3. Podmiot kluczowy i podmiot ważny oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.

---

art. 15

Art. 15

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

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

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

2. Audyt może być przeprowadzony przez:

1) jednostkę oceniającą zgodność, akredytowaną zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych;

2) co najmniej dwóch audytorów posiadających:

a) certyfikaty określone w przepisach wydanych na podstawie ust. 8 lub

b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub

c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymujących się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych;

3) CSIRT sektorowy, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2.

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

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

1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego;

2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego;

4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224);

5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2022 r. poz. 623).

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

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

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

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

3) Szefa Agencji Bezpieczeństwa Wewnętrznego.

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

---

art. 16

Art. 16. Podmiot:

1) kluczowy i podmiot ważny realizuje obowiązki, o których mowa w niniejszym rozdziale, w terminie 6 miesięcy,

2) kluczowy zapewnia przeprowadzenie audytu, o którym mowa w art. 15 ust. 1, po raz pierwszy w terminie 24 miesięcy

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

---

art. 26a ust. 2–4

Art. 26a.

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.

---

art. 32

Art. 32.

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

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

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

---

art. 33 ust. 5, 7 i 8

art. 33

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

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

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

---

art. 36a

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;

2) akredytowanych na podstawie art. 48 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2024 r. poz. 632 i 1222).

4. Zespołem właściwym do przeprowadzenia oceny bezpieczeństwa jest:

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

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

3) w przypadku podmiotów, o których mowa w art. 26 ust. 7 pkt 1–4d – CSIRT GOV.

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

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

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

---

art. 36b

Art. 36b.

1. Ocena bezpieczeństwa systemu informacyjnego może być przeprowadzona:

1) za zgodą podmiotu krajowego systemu cyberbezpieczeństwa, wyrażoną w formie pisemnej lub formie elektronicznej pod rygorem nieważności albo

2) na zlecenie organu właściwego do spraw cyberbezpieczeństwa.

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

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

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

5. 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.

6. CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy 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 i 1228), 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.

7. Używając urządzeń lub programów komputerowych, o których mowa w ust. 6, CSIRT MON, CSIRT NASK, CSIRT GOV i CSIRT sektorowy może uzyskać dostęp do informacji dla niego nieprzeznaczonej, przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne zabezpieczenie, lub może uzyskać dostęp do całości lub części tego systemu informacyjnego.

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

9. Materiały zawierające informacje, o których mowa w ust. 8, podlegają niezwłocznemu, trwałemu i nieodwracalnemu, protokolarnemu zniszczeniu, którego dokonuje komisja. Zniszczeniu nie podlegają informacje o czynnościach przeprowadzanych w ramach oceny bezpieczeństwa oraz o wykrytych podatnościach systemu informacyjnego.

10. Komisja, o której mowa w ust. 9, 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.

11. Po przeprowadzeniu oceny bezpieczeństwa systemu informacyjnego CSIRT MON, CSIRT NASK, CSIRT GOV i 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 albo CSIRT GOV.

---

art. 37

Art. 37

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

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

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

---

art. 43

Art. 43

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

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

---

art. 45 ust. 3

art. 45

3. Minister właściwy do spraw informatyzacji może opublikować na swojej stronie podmiotowej Biuletynu Informacji Publicznej zestawienie wymogów dokumentów normalizacyjnych, o których mowa w art. 2 pkt 3 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483), których wykonywanie realizuje obowiązki wynikające z przepisów ustawy oraz z przepisów wydanych na podstawie art. 8a

---

art. 46 ust. 1 pkt 1, 2, 4–7

art. 46

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

1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;

2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;

4) szacowanie ryzyka na poziomie krajowym;

5) ostrzeganie o zagrożeniach cyberbezpieczeństwa;

6) czynności nadzorcze organów właściwych do spraw cyberbezpieczeństwa;

7) dokonywanie zgłoszenia naruszenia ochrony danych osobowych, o którym mowa w art. 33 rozporządzenia 2016/679 i art. 44 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2023 r. poz. 1206) przez podmioty kluczowe i podmioty ważne;

4. Podmioty kluczowe i podmioty ważne, korzystają z systemu teleinformatycznego w zakresie, o którym mowa w ust. 1, w terminie 6 miesięcy od spełnienia przesłanek uznania za podmiot kluczowy lub podmiot ważny.

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

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

---

art. 67a

Rozdział 12a

Szczególne działania na rzecz zapewnienia cyberbezpieczeństwa na poziomie krajowym

Art. 67a.

1. Pełnomocnik może wydać rekomendacje określające środki techniczne i organizacyjne stosowane w celu zwiększania poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa.

2. Rekomendacje Pełnomocnika są publikowane na stronie podmiotowej Biuletynu Informacji Publicznej Pełnomocnika.

3. Pełnomocnik przed wydaniem rekomendacji może zasięgnąć opinii Kolegium.

4. W rekomendacjach Pełnomocnik może wskazać kategorie podmiotów, do których kierowane są rekomendacje.

5.Stosowanie rekomendacji jest dobrowolne.

---

art. 67c

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 w terminie 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski".

2. Przedsiębiorcy telekomunikacyjni, o których mowa w art. 67b ust. 1 pkt 2, wycofują w ciągu 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15 typy produktów ICT, rodzaje usług ICT, konkretne procesy ICT wskazane w decyzji i określone w wykazie kategorii funkcji krytycznych dla bezpieczeństwa sieci i usług w załączniku nr 3 do ustawy.

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

4. Podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320), nie mogą nabywać typów produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT określonych w decyzji, o której mowa w art. 67b ust. 15.

5. W przypadku gdy podmioty, o których mowa w art. 67b ust. 1, do których stosuje się ustawę z dnia 11 września 2019 r. – Prawo zamówień publicznych, nabyły, w drodze zamówienia publicznego, przed dniem ogłoszenia decyzji, o której mowa w art. 67b ust. 15, produkt ICT, usługę ICT lub proces ICT określone w tej decyzji, mogą korzystać z tych produktów, usług lub procesów nie dłużej niż 7 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski", a w przypadku produktów ICT, usług ICT lub procesów ICT wykorzystywanych do wykonywania funkcji krytycznych określonych w załączniku nr 3 do ustawy, nie dłużej niż 4 lat od dnia ogłoszenia decyzji, o której mowa w art. 67b ust. 15,

---

art. 67d

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, o którym mowa w ust. 1, zawiera:

1) wskazanie podmiotu obowiązanego do przekazania informacji;

2) datę wydania decyzji, o której mowa w art. 67b ust. 15;

3) wskazanie zakresu żądanych informacji;

4) wskazanie terminu przekazania informacji adekwatnego do zakresu tego żądania, 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. 67g–67i

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 oraz podmiotów finansowych, z wyłączeniem podmiotów określonych w art. 16 rozporządzenia 2022/2554.

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

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

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

1) istotność cyberzagrożenia związanego z incydentem krytycznym;

2) szacowanie ryzyka związane z zaistniałym incydentem krytycznym;

3) przewidywane lub zaistniałe skutki incydentu krytycznego;

4) skuteczność obowiązku określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;

5) ocenę stopnia dotkliwości wprowadzanych obowiązków dla podmiotów objętych poleceniem zabezpieczającym oraz proporcjonalności tych obowiązków do celu ich wprowadzania.

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

7. Pełnomocnik, dyrektor Rządowego Centrum Bezpieczeństwa, Szef Agencji Bezpieczeństwa Wewnętrznego oraz minister właściwy do spraw informatyzacji, może wzywać podmioty, o których mowa w ust. 2, lub organy administracji publicznej do udzielenia informacji niezbędnych do przeprowadzenia analizy. Organy administracji publicznej udzielają informacji, o których mowa w zdaniu pierwszym, niezwłocznie, nie później niż w ciągu 72 godzin od otrzymania wezwania.

8. Przedstawiciele podmiotów, o których mowa w ust. 2, organizacji społecznych zrzeszających podmioty, o których mowa w ust. 2, lub organów administracji publicznej mogą być zapraszani przez Pełnomocnika do udziału w pracach Zespołu, o którym mowa w art. 35 ust. 3, lub w jego posiedzeniach w związku z przygotowywaniem analizy, o której mowa w ust. 5.

9. Polecenie zabezpieczające zawiera:

1) wskazanie rodzaju lub rodzajów podmiotów, których dotyczy;

2) obowiązek określonego zachowania zmniejszającego skutki incydentu krytycznego lub zapobiegającego jego rozprzestrzenianiu się;

3) termin jego wdrożenia.

10. Obowiązkiem określonego zachowania, o którym mowa w ust. 9 pkt 2, jest:

1) nakaz przeprowadzenia szacowania ryzyka związanego ze stosowaniem określonego produktu ICT, usługi ICT lub procesu ICT i wprowadzenie środków ochrony proporcjonalnych do zidentyfikowanych ryzyk;

2) nakaz przeglądu planów ciągłości działania, planów awaryjnych i planów odtworzenia działalności pod kątem ryzyka wystąpienia incydentu krytycznego związanego z daną podatnością;

3) nakaz zastosowania określonej poprawki bezpieczeństwa w produkcie ICT lub usłudze ICT posiadającym daną podatność;

4) nakaz szczególnej konfiguracji produktu ICT lub usługi ICT, zabezpieczającej przed wykorzystaniem określonej podatności;

5) nakaz wzmożonego monitorowania zachowania systemu informacyjnego;

6) zakaz korzystania z określonego produktu ICT lub usługi ICT, które posiada podatność, która przyczyniła się do zaistnienia incydentu krytycznego;

7) nakaz wprowadzenia ograniczenia ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, który skutkując zakłóceniem usług świadczonych przez ten podmiot został sklasyfikowany przez CSIRT MON, CSIRT NASK lub CSIRT GOV jako przyczyna trwającego incydentu krytycznego;

8) nakaz wstrzymania dystrybucji lub zakaz instalacji określonej wersji oprogramowania;

9) nakaz zabezpieczenia określonych informacji, w tym dzienników systemowych;

10) nakaz wytworzenia obrazów stanu określonych urządzeń zainfekowanych złośliwym oprogramowaniem.

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

12. Polecenie zabezpieczające wydaje się na czas koordynacji obsługi incydentu krytycznego lub na czas oznaczony, 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.

---

art. 8c

Art. 8c.

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

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

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

---

art. 8d

Art. 8d.

Kierownik podmiotu kluczowego lub podmiotu ważnego:

1) podejmuje decyzje w zakresie przygotowania, wdrażania, stosowania, przeglądu i nadzoru systemu zarządzania bezpieczeństwem informacji w podmiocie;

2) planuje adekwatne środki finansowe na realizację obowiązków z zakresu cyberbezpieczeństwa;

3) przydziela zadania z zakresu cyberbezpieczeństwa w tym podmiocie i nadzoruje ich wykonanie;

4) zapewnia, że personel podmiotu jest świadomy obowiązków z zakresu cyberbezpieczeństwa i zna wewnętrzne regulacje podmiotu w tym zakresie;

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

---

art. 8e

Art. 8e. Kierownik podmiotu kluczowego lub podmiotu ważnego oraz osoba, której powierzono obowiązki kierownika w zakresie cyberbezpieczeństwa raz w roku kalendarzowym przechodzi szkolenie z zakresu wykonywania obowiązków, o których mowa w art. 7b ust. 4, art. 7c, art. 7f ust. 3, art. 8, art. 8d, art. 8e, art. 8f ust. 2 i 3, art. 9–12b, art. 14 i art. 15. Udział w szkoleniu jest udokumentowany.

---

art. 8f

Art. 8f.

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

2. Przed rozpoczęciem realizacji zadań, o których mowa w art. 8 lub art. 11, osoba przedstawia podmiotowi kluczowemu lub podmiotowi ważnemu zaświadczenie o niekaralności za przestępstwa przeciwko ochronie informacji. Kierownik podmiotu kluczowego lub podmiotu ważnego dopuszcza osobę do realizacji zadań, o których mowa w art. 8 lub art. 11, po otrzymaniu zaświadczenia, o którym mowa w zdaniu pierwszym.

3. Podmiot kluczowy lub podmiot ważny wzywa osobę realizującą zadania, o których mowa w art. 8 lub art. 11, do ponownego przedstawienia zaświadczenia o niekaralności za przestępstwa przeciwko ochronie informacji, jeżeli poweźmie uzasadnione podejrzenie, że osoba ta została skazana za przestępstwo przeciwko ochronie informacji.

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

---

art. 12 ust. 7

Art. 12

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

---

art. 31 ust. 1

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.

Tomasz Zalewski

Partner

+48225837946
tomasz.zalewski@twobirds.com

Kuba Ruiz

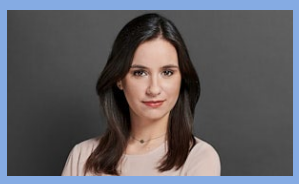
Senior Counsel

+48 693 663 683
kuba.ruiz@twobirds.com

Aleksandra Cywińska

Senior Associate

+48 538 182 792
aleksandra.cywinska@twobirds.com



Karolina Kacprzak

Associate

+48 883 379 631
karolina.kacprzak@twobirds.com

Michał Śmiechowski

Associate

+48 532 406 780
michal.smiechowski@twobirds.com

twobirds.com

Abu Zabi • Amsterdam • Bratysława • Bruksela • Budapeszt • Casablanca • Dubaj • Dublin • Düsseldorf • Frankfurt • Haga • Hamburg • Helsinki • Hong Kong • Kopenhaga • Londyn • Lyon • Madryt • Mediolan • Monachium • Paryż • Pekin • Praga • Rzym • San Francisco • Shenzhen • Singapur • Sydney • Szanghaj • Sztokholm • Tokio • Warszawa