Warszawa, dnia 28 lipca 2025 r.

Poz. 1017

USTAWA

z dnia 25 czerwca 2025 r.

o krajowym systemie certyfikacji cyberbezpieczeństwa[1), 2)]

Art. 1. Ustawa określa organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, w tym sposób sprawowania nadzoru nad działalnością podmiotów wchodzących w skład tego systemu, kontroli działalności tych podmiotów oraz koordynacji ich działalności.

Art. 2. Użyte w ustawie określenia oznaczają:

1) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30, z późn. zm.[3)]), zwanego dalej „rozporządzeniem 765/2008”;

2) certyfikacja – potwierdzenie, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, osoba fizyczna lub system zarządzania cyberbezpieczeństwem spełniają wymogi określone w europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym schemacie certyfikacji cyberbezpieczeństwa, które skutkuje wydaniem certyfikatu potwierdzającego zgodność z tymi wymogami;

3) cyberbezpieczeństwo – cyberbezpieczeństwo, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15, z późn. zm.[4)]), zwanego dalej „rozporządzeniem 2019/881”;

4) cyberzagrożenie – cyberzagrożenie, o którym mowa w art. 2 pkt 8 rozporządzenia 2019/881;

5) deklaracja zgodności – unijną deklarację zgodności, o której mowa w art. 53 ust. 2 rozporządzenia 2019/881;

6) dokument odzwierciedlający stan wiedzy – dokument, który określa metody, techniki i narzędzia oceny mające zastosowanie do certyfikacji produktów ICT lub wymogi bezpieczeństwa generycznej kategorii produktów ICT lub jakiekolwiek inne wymogi niezbędne do certyfikacji produktów ICT, stosowane w celu harmonizacji oceny, w szczególności w odniesieniu do domen technicznych lub profili zabezpieczeń;

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

---

1) Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15 oraz Dz. Urz. UE L 2025/37 z 15.01.2025).

2) Niniejszą ustawą zmienia się ustawę z dnia 30 kwietnia 2010 r. o instytutach badawczych, ustawę z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz ustawę z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

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

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

8) europejski certyfikat – europejski certyfikat cyberbezpieczeństwa, o którym mowa w art. 2 pkt 11 rozporządzenia 2019/881;

9) europejski program certyfikacji cyberbezpieczeństwa – europejski program certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881;

10) instytut badawczy – instytut badawczy, o którym mowa w art. 1 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534);

11) jednostka oceniająca zgodność – jednostkę prowadzącą ocenę zgodności w zakresie cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem lub wiedzy i umiejętności praktycznych osób fizycznych;

12) krajowy certyfikat – dokument poświadczający, że dany produkt ICT, dana usługa ICT, dany proces ICT, dana usługa zarządzana w zakresie bezpieczeństwa, dany system zarządzania cyberbezpieczeństwem lub dana osoba fizyczna zostały ocenione pod względem zgodności ze szczegółowymi wymogami określonymi w krajowym schemacie certyfikacji cyberbezpieczeństwa;

13) krajowy schemat certyfikacji cyberbezpieczeństwa – krajowy program certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 10 rozporządzenia 2019/881, oraz kompleksowy zbiór regulacji przyjętych przez krajowy organ do spraw certyfikacji cyberbezpieczeństwa, mających zastosowanie do certyfikacji systemów zarządzania cyberbezpieczeństwem albo osób fizycznych w zakresie cyberbezpieczeństwa;

14) norma – normę, o której mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniającego dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylającego decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12, z późn. zm.[5)]);

15) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;

16) państwowy instytut badawczy – instytut badawczy, o którym mowa w art. 21 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych;

17) proces ICT – proces ICT, o którym mowa w art. 2 pkt 14 rozporządzenia 2019/881;

18) produkt ICT – produkt ICT, o którym mowa w art. 2 pkt 12 rozporządzenia 2019/881;

19) przeciętne wynagrodzenie – przeciętne wynagrodzenie w gospodarce narodowej, ogłaszane przez Prezesa Głównego Urzędu Statystycznego w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" na podstawie art. 20 pkt 1 lit. a ustawy z dnia 17 grudnia 1998 r. o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2024 r. poz. 1631 i 1674 oraz z 2025 r. poz. 718 i 769) za rok poprzedzający rok nałożenia kary pieniężnej, o której mowa w art. 33;

20) specyfikacja techniczna – specyfikację techniczną, o której mowa w art. 2 pkt 20 rozporządzenia 2019/881;

21) system zarządzania cyberbezpieczeństwem – przyjęte w danej organizacji procedury oraz wytyczne służące ochronie jej zasobów informacyjnych przed cyberzagrożeniami, polegające na systematycznym ustanawianiu, wdrażaniu, obsłudze, monitorowaniu rozwiązań zapewniających bezpieczeństwo sieci i systemów informatycznych organizacji oraz przeglądach tych sieci i systemów;

22) usługa ICT – usługę ICT, o której mowa w art. 2 pkt 13 rozporządzenia 2019/881;

23) usługa zarządzana w zakresie bezpieczeństwa – usługę zarządzaną w zakresie bezpieczeństwa, o której mowa w art. 2 pkt 14a rozporządzenia 2019/881.

Art. 3. 1. Krajowy system certyfikacji cyberbezpieczeństwa stanowi zbiór podmiotów, o których mowa w ust. 2, oraz procedur związanych z certyfikacją produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w ramach europejskich programów certyfikacji cyberbezpieczeństwa albo krajowych schematów certyfikacji cyberbezpieczeństwa oraz procedur w zakresie certyfikacji systemów certyfikacji cyberbezpieczeństwa lub osób fizycznych w ramach krajowych schematów certyfikacji cyberbezpieczeństwa, wspierających:

1) wytwarzanie wysokiej jakości produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa;

2) budowę systemów zarządzania cyberbezpieczeństwem;

[5)] Zmiany wymienionego rozporządzenia zostały ogłoszone w Dz. Urz. UE L 96 z 29.03.2014, str. 1, 45, 107, 149, 251 i 309, Dz. Urz. UE L 241 z 17.09.2015, str. 1, Dz. Urz. UE L 323 z 19.12.2022, str. 1 oraz Dz. Urz. UE L 135 z 23.05.2023, str. 1.

3) zapewnienie:

a) wykwalifikowanych specjalistów w obszarze cyberbezpieczeństwa,

b) spełniania przez produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa wymogów w zakresie ochrony dostępności, autentyczności, integralności i poufności przetwarzanych danych,

c) bezpieczeństwa oferowanych lub dostępnych produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa w trakcie ich całego cyklu życia oraz powiązanych z nimi funkcji.

2. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:

1) ministra właściwego do spraw informatyzacji;

2) Polskie Centrum Akredytacji;

3) jednostki oceniające zgodność;

4) dostawców, którzy poddają swoje produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa ocenie zgodności w ramach danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa;

5) osoby fizyczne, które poddają swoją wiedzę i umiejętności praktyczne ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa;

6) podmioty, które poddają wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa.

Art. 4. 1. Minister właściwy do spraw informatyzacji jest krajowym organem do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881.

2. Do zadań ministra właściwego do spraw informatyzacji należy:

1) sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3–6;

2) przeprowadzanie kontroli podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3, 4 i 6;

3) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;

4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji;

5) wyrażanie zgody na wydanie europejskich certyfikatów o poziomie uzasadnienia zaufania „wysoki”, o którym mowa w art. 52 ust. 7 rozporządzenia 2019/881;

6) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań w ramach europejskich programów certyfikacji cyberbezpieczeństwa;

7) prowadzenie postępowań w sprawie zezwoleń, o których mowa w art. 19 ust. 2;

8) przekazywanie Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b–d oraz ust. 8 rozporządzenia 2019/881;

9) uczestniczenie w pracach Europejskiej Grupy do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) na podstawie art. 58 ust. 6 rozporządzenia 2019/881;

10) wyrażanie zgody na rezygnację z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy, jeżeli dany europejski program certyfikacji cyberbezpieczeństwa to przewiduje;

11) ustalanie zmian w metodyce oceny, która ma być stosowana, w przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa to przewiduje;

12) przygotowywanie krajowych schematów certyfikacji cyberbezpieczeństwa;

13) nadzorowanie stosowania określonych w europejskich programach certyfikacji cyberbezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa z wymogami europejskich certyfikatów;

14) monitorowanie spełniania przez jednostki oceniające zgodność wymogów określonych w załączniku do rozporządzenia 2019/881;

15) przeprowadzanie lub zlecanie badań produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, dla których zostały wydane europejski certyfikat albo krajowy certyfikat albo deklaracja zgodności, lub systemu zarządzania cyberbezpieczeństwem, dla którego został wydany krajowy certyfikat.

3. Minister właściwy do spraw informatyzacji jest administratorem danych osobowych przetwarzanych w celu realizacji jego zadań, obowiązków lub uprawnień wynikających z ustawy.

4. Zadania ministra właściwego do spraw informatyzacji, o których mowa w ust. 2, oraz zadania ministra właściwego do spraw informatyzacji z zakresu nadzoru nad państwowymi instytutami badawczymi nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra.

Art. 5. 1. Produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa mogą być poddane ocenie zgodności zgodnie z danym europejskim programem certyfikacji cyberbezpieczeństwa na podstawie umowy zawartej przez dostawcę i jednostkę oceniającą zgodność.

2. Ocena zgodności, o której mowa w ust. 1, odnosi się do jednego z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881.

3. Umowa, o której mowa w ust. 1, określa w szczególności produkt ICT, usługę ICT, proces ICT lub usługę zarządzaną w zakresie bezpieczeństwa, które mają zostać poddane ocenie zgodności, zakres certyfikacji, europejski program certyfikacji cyberbezpieczeństwa, w ramach którego ma być wydany europejski certyfikat, poziom uzasadnienia zaufania, do którego ma odwoływać się ten certyfikat, obowiązki stron związane z certyfikacją oraz obowiązki związane z ochroną informacji przekazywanych jednostce oceniającej zgodność, a zwłaszcza sposób ochrony tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także ochrony praw własności intelektualnej.

Art. 6. 1. Produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub wiedza i umiejętności praktyczne osoby fizycznej z zakresu cyberbezpieczeństwa mogą być poddane ocenie zgodności zgodnie z danym krajowym schematem certyfikacji cyberbezpieczeństwa.

2. Produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa w ramach oceny zgodności, o której mowa w ust. 1, podlegają ocenie zgodności ze szczegółowymi wymogami określonymi w danym krajowym schemacie certyfikacji cyberbezpieczeństwa na podstawie umowy zawartej przez dostawcę i jednostkę oceniającą zgodność.

3. System zarządzania cyberbezpieczeństwem w ramach oceny zgodności, o której mowa w ust. 1, podlega ocenie zgodności ze szczegółowymi wymogami określonymi w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, na podstawie umowy zawartej przez podmiot, o którym mowa w art. 3 ust. 2 pkt 6, i jednostkę oceniającą zgodność.

4. Wiedza i umiejętności praktyczne osoby fizycznej z zakresu cyberbezpieczeństwa w ramach oceny zgodności, o której mowa w ust. 1, podlegają ocenie zgodności ze szczegółowymi wymogami określonymi w danym krajowym schemacie certyfikacji cyberbezpieczeństwa na podstawie umowy zawartej przez tę osobę i jednostkę oceniającą zgodność.

5. Umowa, o której mowa w ust. 2–4, określa w szczególności produkt ICT, usługę ICT, proces ICT, usługę zarządzaną w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osobę fizyczną, które mają zostać poddane ocenie zgodności, zakres certyfikacji, krajowy schemat certyfikacji cyberbezpieczeństwa, w ramach którego ma być wydany krajowy certyfikat, obowiązki stron związane z certyfikacją oraz obowiązki związane z ochroną informacji przekazywanych jednostce oceniającej zgodność, a zwłaszcza sposób ochrony tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także ochrony praw własności intelektualnej.

Art. 7. 1. Krajowy certyfikat może zostać wydany dla produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem, które zapewniają dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub udostępnianych funkcji lub usług na poziomie odpowiednim do potencjalnych cyberzagrożeń oraz minimalizują znane ryzyka w zakresie cyberzagrożeń.

2. Krajowy certyfikat może zostać wydany osobie fizycznej, która posiada wiedzę i umiejętności praktyczne gwarantujące realizację zadań z zakresu cyberbezpieczeństwa.

Art. 8. 1. W celu wykazania, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa lub system zarządzania cyberbezpieczeństwem spełniają szczegółowe wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, przeprowadza się ocenę polegającą na badaniu dokumentacji technicznej, audycie, badaniu konkretnych właściwości produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa albo systemu zarządzania cyberbezpieczeństwem lub analizie ich funkcjonowania.

2. W celu wykazania, że wiedza i umiejętności praktyczne osoby fizycznej ubiegającej się o uzyskanie krajowego certyfikatu spełniają szczegółowe wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, przeprowadza się test wiedzy i umiejętności praktycznych z zakresu cyberbezpieczeństwa.

Art. 9. 1. Krajowy certyfikat zawiera:

1) oznaczenie podmiotu, który otrzymał krajowy certyfikat, a w przypadku osoby fizycznej – imię i nazwisko tej osoby;
2) nazwę jednostki oceniającej zgodność, która wydała krajowy certyfikat, oraz wskazanie adresu jej siedziby;
3) oznaczenie produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem podlegających certyfikacji, a w przypadku osoby fizycznej – wskazanie zakresu certyfikacji;
4) numer lub oznaczenie krajowego certyfikatu;
5) oznaczenie krajowego schematu certyfikacji cyberbezpieczeństwa, w ramach którego został wydany krajowy certyfikat;
6) okres, na jaki został wydany krajowy certyfikat;
7) datę wydania krajowego certyfikatu i podpis osoby reprezentującej podmiot dokonujący certyfikacji.

2. Krajowy certyfikat wydawany jest według wzoru określonego w przepisach wydanych na podstawie art. 15 ust. 1.

Art. 10. 1. Krajowy certyfikat jest wydawany na okres nie krótszy niż 2 lata i nie dłuższy niż 5 lat.

2. Ważność krajowego certyfikatu może zostać przedłużona na wniosek:

1) dostawcy, któremu wydano certyfikat,
2) osoby fizycznej, której wydano certyfikat,
3) podmiotu, któremu wydano certyfikat

– w przypadku gdy produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna nadal spełniają wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa.

3. Podmioty, o których mowa w ust. 2, składają wniosek o przedłużenie ważności krajowego certyfikatu nie później niż w terminie miesiąca przed upływem jego ważności.

4. Do wniosku, o którym mowa w ust. 2, dołącza się dokumentację potwierdzającą spełnianie przez produkt ICT, usługę ICT, proces ICT, usługę zarządzaną w zakresie bezpieczeństwa lub system zarządzania cyberbezpieczeństwem szczegółowych wymogów określonych w danym krajowym schemacie certyfikacji cyberbezpieczeństwa.

5. Potwierdzenie spełnienia wymagań przez osobę fizyczną, o której mowa w ust. 2 pkt 2, następuje na podstawie powtórnego sprawdzenia wiedzy i umiejętności praktycznych zgodnie z metodami określonymi w przepisach wydanych na podstawie art. 15 ust. 1.

Art. 11. Produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna, dla których wydano krajowy certyfikat, spełniają szczegółowe wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa przez cały okres, na jaki został wydany krajowy certyfikat.

Art. 12. 1. Posiadacz krajowego certyfikatu przekazuje informacje istotne z punktu widzenia spełniania szczegółowych wymogów określonych w danym krajowym schemacie certyfikacji cyberbezpieczeństwa do jednostki oceniającej zgodność, która wydała ten certyfikat, w szczególności informuje jednostkę oceniającą zgodność o wykryciu podatności w produkcie ICT, usłudze ICT, procesie ICT lub usłudze zarządzanej w zakresie bezpieczeństwa, dla których został wydany krajowy certyfikat.

2. Jednostka oceniająca zgodność może żądać od posiadacza krajowego certyfikatu informacji i dokumentów potwierdzających, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna nadal spełniają szczegółowe wymogi określone w krajowym schemacie certyfikacji cyberbezpieczeństwa, w ramach którego został wydany krajowy certyfikat.

Art. 13. 1. Dokumentacja techniczna dotycząca certyfikacji zawierająca opis wytwarzania i działania produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem jest przechowywana przez jednostkę oceniającą zgodność przez okres nie dłuższy niż 10 lat od dnia wygaśnięcia krajowego certyfikatu. Po upływie okresu przechowywania dokumentacja ta podlega zniszczeniu w sposób uniemożliwiający odtworzenie jej treści.

2. Dokumentacja techniczna, o której mowa w ust. 1, jest przechowywana w sposób zapewniający jej dostępność, autentyczność, integralność i poufność, bezpieczeństwo i ochronę tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także ochronę praw własności intelektualnej.

3. Zniszczenie dokumentacji, o której mowa w ust. 1, potwierdza się protokołem brakowania zawierającym w szczególności datę sporządzenia protokołu, datę zniszczenia dokumentacji, oznaczenie niszczonej dokumentacji, opis sposobu zniszczenia dokumentacji i dane osoby zatwierdzającej protokół. Protokoły brakowania dokumentacji są przechowywane przez jednostki oceniające zgodność.

Art. 14. 1. W przypadku stwierdzenia przez jednostkę oceniającą zgodność, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa lub system zarządzania cyberbezpieczeństwem, dla których wydany został krajowy certyfikat, przestały spełniać wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, jednostka oceniająca zgodność informuje posiadacza krajowego certyfikatu o stwierdzonej niezgodności i zwraca się do niego o przedstawienie propozycji działań zaradczych. Posiadacz krajowego certyfikatu przedstawia jednostce oceniającej zgodność propozycję działań zaradczych w terminie 14 dni od dnia otrzymania informacji o stwierdzonej niezgodności.

2. W przypadku akceptacji propozycji działań zaradczych przez jednostkę oceniającą zgodność posiadacz krajowego certyfikatu usuwa niezgodność zgodnie z zaproponowanymi działaniami zaradczymi w terminie 2 miesięcy od akceptacji tych propozycji przez jednostkę oceniającą zgodność.

3. Jednostka oceniająca zgodność weryfikuje, czy wykonane działania zaradcze doprowadziły do usunięcia niezgodności, o której mowa w ust. 1.

4. W przypadku gdy posiadacz krajowego certyfikatu nie przedstawi propozycji działań zaradczych, nie usunie niezgodności, o której mowa w ust. 1, w terminie, o którym mowa w ust. 2, lub uniemożliwia weryfikację, o której mowa w ust. 3, jednostka oceniająca zgodność cofa wydany krajowy certyfikat.

5. Jednostka oceniająca zgodność powiadamia ministra właściwego do spraw informatyzacji o cofnięciu krajowego certyfikatu.

Art. 15. 1. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzenia, krajowy schemat certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem lub osób fizycznych, zawierający:

1) szczegółowe wymogi dla produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem podlegających ocenie zgodności lub osób fizycznych, których wiedza i umiejętności praktyczne z zakresu cyberbezpieczeństwa podlegają ocenie zgodności;

2) szczegółowe metody stosowane w celu wykazania, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna spełniają wymogi, o których mowa w pkt 1;

3) szczegółowe warunki wydawania, utrzymywania i przedłużania ważności krajowych certyfikatów;

4) szczegółowy sposób monitorowania zgodności produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem lub osób fizycznych z wymogami, o których mowa w pkt 1, w tym mechanizmy służące wykazaniu zgodności z tymi wymogami;

5) szczegółowy zakres dokumentacji technicznej dotyczącej certyfikacji oraz sposób przechowywania i niszczenia tej dokumentacji;

6) okres przechowywania dokumentacji technicznej dotyczącej certyfikacji;

7) okres, na jaki jest wydawany krajowy certyfikat;

8) wzór krajowego certyfikatu.

2. W przypadku rozporządzenia określającego krajowy schemat certyfikacji cyberbezpieczeństwa dotyczący produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa minister właściwy do spraw informatyzacji bierze pod uwagę ich funkcje, wpływ na funkcjonowanie systemów teleinformatycznych, cyberzagrożenia, które ich dotyczą, procesy, w jakich mogą być wykorzystywane, rozwój technologii w obszarze cyberbezpieczeństwa, a także konieczność zapewnienia odpowiedniej transparentności certyfikacji, odpowiedniego sposobu dokumentowania, ewidencjonowania i przechowywania dokumentacji, zapewnienia informacji niezbędnych do oceny, czy spełnione są wymogi, oraz zapewnienia odpowiedniej rozpoznawalności krajowych certyfikatów.

3. W przypadku rozporządzenia określającego krajowy schemat certyfikacji cyberbezpieczeństwa dotyczący systemów zarządzania cyberbezpieczeństwem minister właściwy do spraw informatyzacji bierze pod uwagę konieczność zapewnienia odpowiedniego poziomu cyberbezpieczeństwa systemów teleinformatycznych i danych przetwarzanych w tych systemach, zapewnienia przejrzystych i skutecznych procedur zarządzania cyberbezpieczeństwem, rozwój technologii w obszarze cyberbezpieczeństwa, a także konieczność zapewnienia odpowiedniej transparentności certyfikacji, odpowiedniego sposobu dokumentowania, ewidencjonowania i przechowywania dokumentacji, zapewnienia informacji niezbędnych do oceny, czy spełnione są wymogi, oraz zapewnienia odpowiedniej rozpoznawalności krajowych certyfikatów.

4. W przypadku rozporządzenia określającego krajowy schemat certyfikacji cyberbezpieczeństwa dotyczący osób fizycznych minister właściwy do spraw informatyzacji bierze pod uwagę konieczność odpowiedniego przygotowania osób fizycznych do wykonywania zadań z zakresu cyberbezpieczeństwa oraz wskazania zakresu wiedzy niezbędnej do skutecznej realizacji tych zadań, rozwój technologii w obszarze cyberbezpieczeństwa, a także konieczność zapewnienia odpowiedniej transparentności certyfikacji, odpowiedniego sposobu dokumentowania, ewidencjonowania oraz przechowywania dokumentacji, zapewnienia informacji niezbędnych do oceny, czy spełnione są wymogi, oraz zapewnienia odpowiedniej rozpoznawalności krajowych certyfikatów.

Art. 16. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację w zakresie odnoszącym się do danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa.

Art. 17. 1. Akredytacji jednostce oceniającej zgodność udziela Polskie Centrum Akredytacji.

2. Do akredytacji jednostki oceniającej zgodność stosuje się odpowiednio przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568).

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

4. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji, nie później niż w terminie 14 dni od dnia udzielenia akredytacji, o udzieleniu akredytacji w zakresie odnoszącym się do danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa.

5. Informacja o udzieleniu akredytacji, o której mowa w ust. 3, zawiera:

1) oznaczenie jednostki oceniającej zgodność, której udzielono akredytacji;

2) wskazanie zakresu udzielonej akredytacji, daty udzielenia akredytacji oraz okresu ważności udzielonej akredytacji;

3) numer i oznaczenie certyfikatu akredytacji.

6. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o odmowie udzielenia, cofnięciu, zawieszeniu lub ograniczeniu zakresu akredytacji jednostce oceniającej zgodność nie później niż w terminie 14 dni od dnia podjęcia danego rozstrzygnięcia.

7. Polskie Centrum Akredytacji sprawuje nadzór w zakresie udzielonej akredytacji nad jednostkami oceniającymi zgodność w obszarze objętym danym europejskim programem certyfikacji cyberbezpieczeństwa albo danym krajowym schematem certyfikacji cyberbezpieczeństwa, z uwzględnieniem wymagań, o których mowa w art. 22 ust. 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku, oraz wymogów określonych w:

1) załączniku do rozporządzenia 2019/881;

2) europejskich programach certyfikacji cyberbezpieczeństwa;

3) krajowych schematach certyfikacji cyberbezpieczeństwa.

Art. 18. 1. Państwowe instytuty badawcze nadzorowane przez ministra właściwego do spraw informatyzacji wspierają tego ministra, w zakresie swoich kompetencji, w realizacji zadań, o których mowa w art. 4 ust. 2, przez:

1) przygotowywanie opinii, ekspertyz i analiz;

2) weryfikację dokumentów pochodzących od podmiotów, o których mowa w art. 3 ust. 2 pkt 3–6, pod kątem zgodności tych dokumentów z wymogami określonymi w rozporządzeniu 2019/881, ustawie oraz danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa;

3) przeprowadzanie badań produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa lub systemów zarządzania cyberbezpieczeństwem, w tym dokonywanie określonych czynności z zakresu oceny zgodności;

4) publikację wykazów specyfikacji technicznych, norm i standardów;

5) udział w pracach międzynarodowych grup normalizacyjnych z zakresu cyberbezpieczeństwa zgodnie z zasadami normalizacji krajowej i międzynarodowej;

6) opracowywanie i walidację procesów badawczych;

7) przygotowywanie projektów krajowych schematów certyfikacji cyberbezpieczeństwa;

8) organizowanie porównań międzylaboratoryjnych lub badań biegłości w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa;

9) weryfikację, czy dana osoba fizyczna posiada:

a) kwalifikacje techniczne i zawodowe obejmujące wszystkie czynności z zakresu cyberbezpieczeństwa lub oceny zgodności,

b) odpowiednie doświadczenie w realizacji zadań z zakresu oceny zgodności,

c) wiedzę z zakresu cyberbezpieczeństwa, w szczególności w zakresie wymagań wynikających z danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa,

d) uprawnienia do przeprowadzania oceny zgodności w ramach danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa.

2. Państwowe instytuty badawcze, które nie są nadzorowane przez ministra właściwego do spraw informatyzacji, mogą, w zakresie swoich kompetencji, za zgodą organu nadzorującego dany instytut, wspierać tego ministra w realizacji zadań, o których mowa w art. 4 ust. 2, przez prowadzenie działań, o których mowa w ust. 1.

3. Minister właściwy do spraw informatyzacji może udzielić państwowemu instytutowi badawczemu, o którym mowa w ust. 1 i 2, wspierającemu go w realizacji zadań, o których mowa w art. 4 ust. 2, dotacji celowej z części budżetu państwa, której jest dysponentem.

4. Państwowe instytuty badawcze, o których mowa w ust. 1 i 2, wspierające ministra właściwego do spraw informatyzacji w realizacji zadań, o których mowa w art. 4 ust. 2, rozwijają potencjał badawczo-rozwojowy oraz zdolności w obszarze oceny zgodności i certyfikacji, w szczególności przez:

1) utrzymywanie stałej sprawności operacyjnej;

2) pozyskiwanie i utrzymywanie ekspertów.

5. W uzasadnionych przypadkach minister właściwy do spraw informatyzacji może, na podstawie umowy, zlecić podmiotom innym niż państwowe instytuty badawcze, o których mowa w ust. 1 i 2, dysponującym wiedzą i kompetencjami w zakresie technologii produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem lub określonych zagadnień z zakresu cyberbezpieczeństwa wykonanie określonych usług związanych z realizacją zadań, o których mowa w art. 4 ust. 2, w szczególności zlecić przygotowanie opinii, ekspertyz i analiz, oraz zlecić weryfikację dokumentów pochodzących od podmiotów, o których mowa w art. 3 ust. 2 pkt 3–6.

6. Państwowy instytut badawczy nie realizuje zadań, o których mowa w ust. 1 i 2, w przypadku gdy uczestniczył w procesie certyfikacji, którego te zadania dotyczą.

7. Jednostki organizacyjne podległe Ministrowi Obrony Narodowej mogą, w zakresie swoich kompetencji, za zgodą tego ministra, wspierać ministra właściwego do spraw informatyzacji w realizacji zadań, o których mowa w art. 4 ust. 2. Przepisy ust. 2, 3 i 6 stosuje się odpowiednio.

Art. 19. 1. W przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa zawiera szczegółowe lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, czynności w ramach oceny zgodności dokonywanej na jego podstawie wykonuje jednostka oceniająca zgodność posiadająca zezwolenie ministra właściwego do spraw informatyzacji.

2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie przez jednostkę oceniającą zgodność czynności w ramach danego europejskiego programu certyfikacji cyberbezpieczeństwa na wniosek jednostki oceniającej zgodność, która spełniła wymogi określone w tym programie oraz posiada akredytację w zakresie odnoszącym się do danego europejskiego programu certyfikacji cyberbezpieczeństwa.

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

1) nazwę (firmę) wnioskodawcy;

2) adres i siedzibę wnioskodawcy;

3) wskazanie europejskiego programu certyfikacji cyberbezpieczeństwa, którego dotyczy wniosek;

4) oświadczenie o spełnieniu szczegółowych lub dodatkowych wymogów, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, określonych w europejskim programie certyfikacji cyberbezpieczeństwa, o którym mowa w pkt 3.

4. Do wniosku dołącza się dokumenty potwierdzające spełnienie szczegółowych lub dodatkowych wymogów, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881, określonych w europejskim programie certyfikacji cyberbezpieczeństwa, o którym mowa w ust. 3 pkt 3.

5. Minister właściwy do spraw informatyzacji z urzędu, w drodze decyzji, zawiesza albo cofa zezwolenie, o którym mowa w ust. 2, jeżeli jednostka oceniająca zgodność naruszyła przepisy rozporządzenia 2019/881, ustawy lub danego europejskiego programu certyfikacji cyberbezpieczeństwa.

6. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się, jeżeli naruszenie, o którym mowa w ust. 5:

1) nie występowało w ciągu ostatnich 3 lat, nie było związane z popełnieniem przestępstwa ani nie podważa zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa;

2) jest odwracalne.

7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na okres nie dłuższy niż 2 lata.

8. W przypadku gdy naruszenie, o którym mowa w ust. 5, ustało, minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2.

9. Minister właściwy do spraw informatyzacji cofa decyzję o zezwoleniu, o którym mowa w ust. 2, jeżeli:

1) naruszenie, o którym mowa w ust. 5, występowało w ciągu ostatnich 3 lat, było związane z popełnieniem przestępstwa i podważa zaufanie do krajowego systemu certyfikacji cyberbezpieczeństwa;

2) naruszenie, o którym mowa w ust. 5, jest nieodwracalne;

3) upłynął okres, na który wydano decyzję, o której mowa w ust. 6, oraz nie ustało naruszenie, o którym mowa w ust. 5.

10. Minister właściwy do spraw informatyzacji przed wydaniem decyzji o zezwoleniu, o którym mowa w ust. 2, decyzji o jego zawieszeniu albo decyzji o jego cofnięciu może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w zakresie spełnienia wymagań określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa.

11. Podmiot, do którego wystąpiono o opinię, przekazuje ją w terminie miesiąca od dnia otrzymania wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572 oraz z 2025 r. poz. 769) nie stosuje się.

12. Decyzja o zezwoleniu, o którym mowa w ust. 2, wygasa w przypadku, gdy jednostce oceniającej zgodność cofnięto akredytację w zakresie odnoszącym się do danego europejskiego programu certyfikacji cyberbezpieczeństwa.

13. Do postępowań w sprawie wydania decyzji, o których mowa w ust. 2 i 5, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 20. 1. W przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa przewiduje możliwość zrezygnowania z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy w procesie oceny zgodności, jednostka oceniająca zgodność składa do ministra właściwego do spraw informatyzacji wniosek o zgodę na taką rezygnację wraz z uzasadnieniem.

2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na zrezygnowanie z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy w przypadku, gdy taka rezygnacja jest uzasadniona charakterem danego produktu ICT, danej usługi ICT, danego procesu ICT lub danej usługi zarządzanej w zakresie bezpieczeństwa.

3. Minister właściwy do spraw informatyzacji przed wydaniem decyzji o zezwoleniu, o którym mowa w ust. 2, może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w ramach oceny zgodności z danym europejskim programem certyfikacji cyberbezpieczeństwa.

4. Podmiot, do którego wystąpiono o opinię, przekazuje ją w terminie miesiąca od dnia otrzymania wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

5. Do postępowań w sprawie wydania decyzji, o której mowa w ust. 2, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 21. 1. W przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa przewiduje możliwość wprowadzenia zmian w metodyce oceny, która ma być stosowana przez jednostkę oceniającą zgodność, jednostka ta może wystąpić do ministra właściwego do spraw informatyzacji z wnioskiem o wprowadzenie zmian w tej metodyce. Wniosek zawiera propozycję zmian w metodyce oceny, która ma być stosowana przez jednostkę oceniającą zgodność, wraz z ich uzasadnieniem.

2. Minister właściwy do spraw informatyzacji ustala, w drodze decyzji, jakie zmiany w metodyce oceny, o której mowa w ust. 1, mogą być wprowadzone, aby zapewnić prawidłowy przebieg procesu oceny zgodności. Ustalając zmiany w metodyce oceny, minister właściwy do spraw informatyzacji nie jest związany wnioskiem, o którym mowa w ust. 1.

3. Minister właściwy do spraw informatyzacji przed wydaniem decyzji, o której mowa w ust. 2, może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w zakresie zgodności z danym europejskim programem certyfikacji cyberbezpieczeństwa.

4. Podmiot, do którego wystąpiono o opinię, przekazuje ją w terminie miesiąca od dnia otrzymania wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

5. Do postępowań w sprawie wydania decyzji, o której mowa w ust. 2, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 22. 1. Po zakończeniu certyfikacji jednostka oceniająca zgodność, nie później niż w terminie 14 dni od dnia zakończenia certyfikacji, przesyła do ministra właściwego do spraw informatyzacji drogą elektroniczną wniosek o zgodę na wydanie europejskiego certyfikatu, jeżeli dany certyfikat odwołuje się do poziomu uzasadnienia zaufania „wysoki", o którym mowa w art. 52 ust. 7 rozporządzenia 2019/881.

2. Minister właściwy do spraw informatyzacji:

1) wydaje, w drodze decyzji, zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1;

2) odmawia wydania, w drodze decyzji, zgody na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, jeżeli w ramach certyfikacji zostały naruszone przepisy rozporządzenia 2019/881, ustawy lub danego europejskiego programu certyfikacji cyberbezpieczeństwa.

3. We wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, wskazuje się:

1) produkt ICT, usługę ICT, proces ICT albo usługę zarządzaną w zakresie bezpieczeństwa, które podlegały certyfikacji;

2) europejski program certyfikacji cyberbezpieczeństwa, w ramach którego przeprowadzono certyfikację.

4. Do wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, dołącza się raport z certyfikacji.

5. Minister właściwy do spraw informatyzacji cofa, w drodze decyzji, europejski certyfikat, o którym mowa w ust. 1, jeżeli został on wydany niezgodnie z przepisami rozporządzenia 2019/881, ustawy lub danego europejskiego programu certyfikacji cyberbezpieczeństwa lub jeżeli produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa, dla których wydany został ten certyfikat, nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa.

6. Minister właściwy do spraw informatyzacji przed wydaniem decyzji, o których mowa w ust. 2 i 5, może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w zakresie zgodności certyfikacji z danym europejskim programem certyfikacji cyberbezpieczeństwa.

7. Podmiot, do którego wystąpiono o opinię, przekazuje ją w terminie miesiąca od dnia otrzymania wystąpienia o opinię. Okresu od dnia wystąpienia o opinię do dnia jej otrzymania nie wlicza się do terminu załatwienia sprawy. Przepisu art. 106 § 5 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego nie stosuje się.

8. Do postępowań w sprawie wydania decyzji, o których mowa w ust. 2 i 5, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 23. 1. Jednostka oceniająca zgodność nie później niż w terminie 14 dni od dnia podjęcia danego rozstrzygnięcia przekazuje ministrowi właściwemu do spraw informatyzacji dane dostawcy, osoby fizycznej, która poddała swoją wiedzę i umiejętności praktyczne ocenie zgodności, albo podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności:

1) którym wydano albo przedłużono europejski certyfikat albo krajowy certyfikat, wraz z kopią tego certyfikatu;

2) którym cofnięto europejski certyfikat albo krajowy certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia;

3) którym odmówiono wydania europejskiego certyfikatu albo krajowego certyfikatu, wraz ze wskazaniem przyczyn odmowy.

2. Dane, o których mowa w ust. 1, obejmują:

1) w przypadku osoby prawnej:

   a) nazwę (firmę),

   b) adres i siedzibę,

   c) numer we właściwym rejestrze, o ile taki numer został nadany, oraz numer identyfikacji podatkowej (NIP);

2) w przypadku osoby fizycznej:

   a) imię i nazwisko,

   b) numer PESEL.

3. Dane, o których mowa w ust. 1, jednostka oceniająca zgodność przekazuje drogą elektroniczną ministrowi właściwemu do spraw informatyzacji.

4. Kopie europejskiego certyfikatu albo krajowego certyfikatu są przechowywane przez ministra właściwego do spraw informatyzacji przez cały okres ważności certyfikatu oraz przez 5 lat po jego wygaśnięciu.

5. W przypadku gdy jednostka oceniająca zgodność przekazuje niepełne dane, o których mowa w ust. 1, minister właściwy do spraw informatyzacji wzywa tę jednostkę do ich uzupełnienia w terminie 14 dni od dnia otrzymania wezwania.

Art. 24. 1. Każdy może złożyć do jednostki oceniającej zgodność skargę na działania tej jednostki podjęte podczas oceny zgodności.

2. Jednostka oceniająca zgodność rozpatruje skargę w terminie nie dłuższym niż 2 miesiące od dnia złożenia skargi.

3. Skargę rozpatrują osoby, które nie brały udziału w działaniach, których dotyczy skarga.

4. Jednostka oceniająca zgodność publikuje na swojej stronie internetowej informacje o postępowaniu ze skargami, o których mowa w art. 63 rozporządzenia 2019/881, w tym termin rozpatrzenia skargi.

Art. 25. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:

1) dostawcę, który wydał deklarację zgodności, jeżeli produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa, których deklaracja dotyczy, nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa;

2) jednostkę oceniającą zgodność prowadzącą ocenę produktów ICT, usług ICT, procesów ICT, osób fizycznych, systemów zarządzania cyberbezpieczeństwem lub usług zarządzanych w zakresie bezpieczeństwa w zakresie cyberbezpieczeństwa.

2. Minister właściwy do spraw informatyzacji rozpatruje skargi, o których mowa w ust. 1, w sposób określony w danym europejskim programie certyfikacji cyberbezpieczeństwa i na zasadach w nim określonych, a w przypadku gdy dany europejski program certyfikacji cyberbezpieczeństwa nie określa sposobu ani zasad rozpatrywania skarg, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

3. Rozpatrzenie skargi, o której mowa w ust. 1, następuje nie później niż w terminie 2 miesięcy od dnia jej złożenia.

Art. 26. Każdemu, czyj interes prawny lub czyje uprawnienie zostały naruszone przez bezczynność w sprawie rozpatrzenia skargi, o której mowa w art. 25 ust. 1, przysługuje prawo wniesienia skargi na bezczynność organu do sądu administracyjnego.

Art. 27. 1. Minister właściwy do spraw informatyzacji w ramach nadzoru, o którym mowa w art. 4 ust. 2 pkt 1, może wezwać podmioty, o których mowa w art. 3 ust. 2 pkt 3–6, do przedstawienia informacji dotyczących:

1) produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, dla których zostały wydane europejski certyfikat lub deklaracja zgodności – w zakresie objętym danym europejskim programem certyfikacji cyberbezpieczeństwa;

2) produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa, systemu zarządzania cyberbezpieczeństwem lub osoby fizycznej, dla których został wydany krajowy certyfikat – w zakresie objętym danym krajowym schematem certyfikacji cyberbezpieczeństwa;

3) liczby wydanych europejskich certyfikatów albo krajowych certyfikatów wraz ze wskazaniem europejskich programów certyfikacji cyberbezpieczeństwa albo krajowych schematów certyfikacji cyberbezpieczeństwa, w ramach których te certyfikaty zostały wydane, oraz poziomów uzasadnienia zaufania, o których mowa w art. 52 rozporządzenia 2019/881, do których te certyfikaty się odwoływały;

4) liczby wydanych deklaracji zgodności wraz ze wskazaniem europejskich programów certyfikacji cyberbezpieczeństwa, w ramach których te deklaracje zostały wydane;

5) innych kwestii istotnych dla funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa.

2. Informacje, o których mowa w ust. 1, przekazuje się ministrowi właściwemu do spraw informatyzacji w terminie 21 dni od dnia otrzymania wniosku o przedstawienie informacji.

Art. 28. 1. Minister właściwy do spraw informatyzacji w ramach nadzoru, o którym mowa w art. 4 ust. 2 pkt 1, prowadzi kontrole jednostek oceniających zgodność, dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa oraz podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności.

2. Do kontroli, o której mowa w ust. 1, przeprowadzonej wobec dostawców:

1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, z późn. zm.[6)]) oraz przepisy art. 55–59 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222);

2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224).

Art. 29. 1. Minister właściwy do spraw informatyzacji w ramach przeprowadzanej kontroli, o której mowa w art. 28 ust. 1, może poddać produkt ICT, usługę ICT, proces ICT lub usługę zarządzaną w zakresie bezpieczeństwa, dla których został wydany europejski certyfikat albo krajowy certyfikat albo została wydana deklaracja zgodności, lub system zarządzania cyberbezpieczeństwem, dla którego został wydany krajowy certyfikat, badaniom lub zlecić ich przeprowadzenie w celu ustalenia, czy są spełnione wymogi określone w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa.

2. Koszty badań, o których mowa w ust. 1, ponosi dostawca produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa lub podmiot, który poddał wykorzystywany przez siebie system zarządzania cyberbezpieczeństwem ocenie zgodności.

Art. 30. 1. Badanie, o którym mowa w art. 29 ust. 1, może zostać przeprowadzone na próbkach produktu ICT.

2. Próbką produktu ICT jest pojedynczy produkt ICT danego rodzaju albo jego określony element.

3. Dostawca produktu ICT na wezwanie ministra właściwego do spraw informatyzacji przekazuje osobom prowadzącym czynności kontrolne wskazaną przez te osoby próbkę produktu ICT. Z przekazania próbki produktu ICT sporządza się protokół.

4. Protokół, o którym mowa w ust. 3, zawiera:

1) nazwę produktu ICT;

2) oznaczenie europejskiego certyfikatu albo krajowego certyfikatu wydanego dla produktu ICT lub deklaracji zgodności wydanej dla produktu ICT;

3) określenie wielkości próbki produktu ICT przekazanej do badania;

4) dane identyfikujące produkt ICT, w szczególności numer seryjny przekazanego jako próbka egzemplarza produktu ICT;

5) imię i nazwisko osoby przekazującej próbkę produktu ICT;

6) imię i nazwisko osoby odbierającej próbkę produktu ICT;

7) datę przekazania próbki produktu ICT;

8) podpis osoby sporządzającej protokół.

Art. 31. 1. Jeżeli badanie, o którym mowa w art. 29 ust. 1, wykaże, że produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości na swojej stronie podmiotowej w Biuletynie Informacji Publicznej informację o niespełnianiu przez produkt ICT, usługę ICT, proces ICT lub usługę zarządzaną w zakresie bezpieczeństwa wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa.

2. W przypadku europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, minister właściwy do spraw informatyzacji:

1) cofa certyfikat, jeżeli wykryte nieprawidłowości:

   a) mają znaczący wpływ na dostępność, autentyczność, integralność lub poufność danych, sieci i systemów informatycznych danego podmiotu wykorzystującego system zarządzania cyberbezpieczeństwem lub

   b) mają znaczący wpływ na użytkownika produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, lub

   c) są nieodwracalne;

2) zawiesza certyfikat, jeżeli wykryte nieprawidłowości nie mają znaczącego wpływu, o którym mowa w pkt 1 lit. a i b, oraz są odwracalne.

---

6) Zmiany tekstu jednolitego wymienionej ustawy zostały ogłoszone w Dz. U. z 2024 r. poz. 1222 i 1871 oraz z 2025 r. poz. 222, 621, 622 i 769.

3. Decyzję o zawieszeniu europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, wydaje się na okres nie dłuższy niż 6 miesięcy.

4. W przypadku przywrócenia zgodności z wymogami określonymi w danym europejskim programie certyfikacji cyberbezpieczeństwa minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu europejskiego certyfikatu, o którym mowa w art. 22 ust. 1.

5. Cofnięcie albo zawieszenie europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, następuje w drodze decyzji ministra właściwego do spraw informatyzacji.

Art. 32. Minister właściwy do spraw informatyzacji w przypadku uzasadnionego podejrzenia, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, dla których wydano europejski certyfikat albo krajowy certyfikat, nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa, a w przypadku systemu zarządzania cyberbezpieczeństwem lub osób fizycznych – nie spełniają wymogów określonych w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, informuje o tym podejrzeniu jednostkę oceniającą zgodność, która wydała europejski certyfikat albo krajowy certyfikat.

Art. 33. 1. Jednostka oceniająca zgodność, która będąc do tego obowiązaną, nie przekazuje danych, o których mowa w art. 23 ust. 1, lub przekazuje nieprawdziwe lub niepełne dane, podlega karze pieniężnej w wysokości dziesięciokrotności przeciętnego wynagrodzenia.

2. Jednostka oceniająca zgodność, która wydaje europejski certyfikat albo krajowy certyfikat, działając bez wymaganej akredytacji, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

3. Dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, podmiot, który otrzymał krajowy certyfikat dla wykorzystywanego przez siebie systemu zarządzania cyberbezpieczeństwem, albo jednostka oceniająca zgodność produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, którzy uniemożliwiają lub utrudniają ministrowi właściwemu do spraw informatyzacji przeprowadzenie kontroli, o której mowa w art. 28, podlegają karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

4. Dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, który nie wykonuje obowiązku określonego w art. 53 ust. 3 rozporządzenia 2019/881, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

5. Dostawca produktów ICT, który nie wykonuje obowiązku, o którym mowa w art. 30 ust. 3, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

6. Dostawca certyfikowanych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa w ramach europejskich programów certyfikacji cyberbezpieczeństwa lub dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w przypadku których wydana została deklaracja zgodności, którzy nie realizują obowiązków, o których mowa w art. 55 rozporządzenia 2019/881, podlegają karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

7. Podmiot, o którym mowa w art. 3 ust. 2 pkt 3–6, który nie przekazuje informacji, o których mowa w art. 27 ust. 1 pkt 1–3, w terminie, o którym mowa w art. 27 ust. 2, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.

Art. 34. 1. Kary pieniężne, o których mowa w art. 33, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

2. Ustalając wysokość kar pieniężnych, o których mowa w art. 33, minister właściwy do spraw informatyzacji uwzględnia zakres lub charakter naruszenia oraz dotychczasową działalność kontrolowanego podmiotu.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 33, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662).

4. Kary pieniężne, o których mowa w art. 33, uiszcza się na rachunek Funduszu Cyberbezpieczeństwa w terminie 14 dni od dnia uprawomocnienia się decyzji ministra właściwego do spraw informatyzacji w sprawie nałożenia kary pieniężnej.

5. Od decyzji ministra właściwego do spraw informatyzacji w sprawie nałożenia kary pieniężnej, o której mowa w art. 33, przysługuje skarga do sądu administracyjnego.

6. Kary pieniężne, o których mowa w art. 33, podlegają egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym.

Art. 35. W ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534) w art. 2 w ust. 2 w pkt 8 kropkę zastępuje się średnikiem i dodaje się pkt 9 w brzmieniu:

„9) wspierać ministra właściwego do spraw informatyzacji w wykonywaniu zadań, o których mowa w art. 4 ust. 2 ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. 1017).”.

Art. 36. W ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222) w art. 93 w ust. 3 pkt 8 i 9 otrzymują brzmienie:

„8) w 2025 r. – 80 300 tys. zł;

9) w 2026 r. – 91 400 tys. zł;”.

Art. 37. W ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662) w art. 2 w ust. 4 po pkt 1 dodaje się pkt 1a w brzmieniu:

„1a) wpływy z kar pieniężnych, o których mowa w art. 33 ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. 1017);”.

Art. 38. 1. Akredytacje udzielone przez Polskie Centrum Akredytacji jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie ustawy stają się akredytacjami w rozumieniu ustawy.

2. W terminie 14 dni od dnia wejścia w życie ustawy Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonych akredytacjach, o których mowa w ust. 1.

Art. 39. 1. Certyfikaty wydane w ramach akredytacji, o której mowa w art. 38, obowiązują do końca terminu ich ważności. Do tych certyfikatów stosuje się przepisy dotychczasowe.

2. W terminie 14 dni od dnia wejścia w życie ustawy jednostki oceniające zgodność informują ministra właściwego do spraw informatyzacji o wydanych certyfikatach, o których mowa w ust. 1, zgodnie z zasadami określonymi w art. 23.

Art. 40. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie ustawy, wynosi:

1) w 2025 r. – 9 720 tys. zł;

2) w 2026 r. – 11 600 tys. zł;

3) w 2027 r. – 11 880 tys. zł;

4) w 2028 r. – 12 190 tys. zł;

5) w 2029 r. – 12 500 tys. zł;

6) w 2030 r. – 12 820 tys. zł;

7) w 2031 r. – 13 150 tys. zł;

8) w 2032 r. – 13 490 tys. zł;

9) w 2033 r. – 13 840 tys. zł;

10) w 2034 r. – 14 200 tys. zł.

2. Maksymalny limit wydatków Polskiego Centrum Akredytacji, będący skutkiem finansowym wejścia w życie ustawy, wynosi:

1) w 2025 r. – 300 tys. zł;

2) w 2026 r. – 310 tys. zł;

3) w 2027 r. – 320 tys. zł;

4) w 2028 r. – 330 tys. zł;

5) w 2029 r. – 340 tys. zł;

6) w 2030 r. – 350 tys. zł;

7) w 2031 r. – 360 tys. zł;

8) w 2032 r. – 360 tys. zł;

9) w 2033 r. – 370 tys. zł;

10) w 2034 r. – 380 tys. zł.

3. W przypadku zagrożenia przekroczeniem lub przekroczenia przyjętego na dany rok budżetowy maksymalnego limitu wydatków, o którym mowa w ust. 1 i 2, zostanie zastosowany mechanizm korygujący polegający na ograniczeniu wydatków związanych z realizacją zadań określonych w ustawie.

4. Minister właściwy do spraw informatyzacji monitoruje wykorzystanie limitu wydatków, o którym mowa w ust. 1, i przynajmniej dwa razy do roku dokonuje, według stanu na koniec danego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia mechanizmów korygujących, o których mowa w ust. 3, dokonuje minister właściwy do spraw informatyzacji.

5. Organem właściwym do monitorowania wykorzystania limitu wydatków, o którym mowa w ust. 2, oraz odpowiedzialnym za wdrożenie mechanizmów korygujących, o których mowa w ust. 3, jest minister właściwy do spraw gospodarki.

Art. 41. Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia.

Prezydent Rzeczypospolitej Polskiej: *A. Duda*