Prezes
Rady Ministrów

Donald Tusk

Warszawa, dnia /elektroniczny znacznik czasu/

RM-0610-32-25
UC42

Pan Szymon HOŁOWNIA
Marszałek Sejmu

Szanowny Panie Marszałku,

na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej przedstawiam Sejmowi projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa.
Ma on na celu wykonanie prawa Unii Europejskiej.
Do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem
Donald Tusk
/podpisano kwalifikowanym podpisem elektronicznym/

Do wiadomości:
wnioskodawca

tel. +48 (22) 694 75 00
dkpl@kprm.gov.pl
gov.pl/premier

Al. Ujazdowskie 1/3; 00-583
Warszawa

Projekt

U S T A W A

z dnia

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 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)

---

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 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.

(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;

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 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 publiczny, mających

---

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

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 miesięczne 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) 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;

[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.

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;
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 cyberbezpieczeństwa 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;
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) przygotowanie 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 został wydany europejski 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 mające 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 w procesie certyfikacji 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 warunkach wskazanych w umowie 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 mające 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 podmiotu dokonującego certyfikacji oraz wskazanie adresu jego 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. Krajowy certyfikat może zostać przedłużony na wniosek:

1) dostawcy,
2) osoby fizycznej, która poddała swoją wiedzę i swoje umiejętności praktyczne ocenie zgodności,

3) podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności

– 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. Podmiot, o którym mowa w ust. 2, składa wniosek o przedłużenie ważności krajowego certyfikatu w terminie co najmniej 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 osoby fizyczne, o których 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 z zapewnieniem bezpieczeństwa i ochrony tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także zapewnieniem ochrony 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 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 lub osób fizycznych podlegających 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 jednostki 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 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179).

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, przy uwzględnieniu 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) przygotowanie 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 dokonywania 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) opracowanie i walidację procesów badawczych;
7) przygotowanie 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 do 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:

1) przygotowanie 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 dokonywania 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) opracowanie i walidację procesów badawczych;
7) przygotowanie 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 do 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.

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 utrzymanie 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.

5. Minister właściwy do spraw informatyzacji z urzędu, w drodze decyzji, cofa albo zawiesza 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:

1) naruszenie, o którym mowa w ust. 5, nie występowało w ciągu ostatnich 3 lat, nie było związane z popełnieniem przestępstwa ani nie podważa zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa;
2) naruszenie, o którym mowa w ust. 5, jest odwracalne.

7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na czas określony, 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 zgodności certyfikacji z danym europejskim programem 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 otrzymania opinii 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) 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.

9. Minister właściwy do spraw informatyzacji nie ponosi odpowiedzialności za szkody wywołane wydaniem decyzji, o której mowa w ust. 5.

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 skargę do jednostki oceniającej zgodność 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 załatwienia 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 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 i 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 wystąpić do podmiotów, o których mowa w art. 3 ust. 2 pkt 3–6, z wnioskiem o przedstawienie 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, 1222 i 1871 oraz z 2025 r. poz. 222)

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) wielkość 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 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.

3. Decyzję o zawieszeniu europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, wydaje się na czas określony, 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, system zarządzania cyberbezpieczeństwem lub osoba fizyczna, 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 obowiązana, nie przekazuje danych, o których mowa w art. 23 ust. 1, lub przekazuje nieprawdziwe lub niekompletne 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 przeprowadzanie 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 unijna 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 … o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. …).”.

Art. 36. 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… o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. …);”.

Art. 37. 1. Akredytacje udzielone przez Polskie Centrum Akredytacji jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie niniejszej ustawy stają się akredytacjami w rozumieniu niniejszej ustawy.

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

Art. 38. 1. Certyfikaty wydane w ramach akredytacji, o której mowa w art. 37, obowiązują do końca terminu ich ważności. Do tych certyfikatów stosuje się przepisy dotychczasowe.

2. W terminie 14 dni od dnia wejścia w życie niniejszej 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. 39. 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 przekroczenia 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 których mowa w ust. 2, oraz odpowiedzialnym za wdrożenie mechanizmów korygujących, o których mowa w ust. 3, jest minister właściwy do spraw gospodarki.

Art. 40. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

UZASADNIENIE

1. Cel i potrzeba wydania ustawy

Rozporządzenie 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.), zwane dalej „rozporządzeniem 2019/881", ustanowiło europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów. Do tej pory certyfikacja w obszarze cyberbezpieczeństwa była obszarem nieuregulowanym, w którym miały zastosowanie ogólne zasady prawa cywilnego i prawa umów.

Rozporządzenie 2019/881 nakłada na wszystkie państwa członkowskie Unii Europejskiej obowiązek ustanowienia krajowego organu do spraw certyfikacji cyberbezpieczeństwa, który będzie nadzorował rynek i kontrolował prawidłowość działań w zakresie certyfikacji. W celu wdrożenia w Polsce rozwiązań przewidzianych w rozporządzeniu 2019/881 konieczne jest również wprowadzenie do polskiego systemu prawa przepisów związanych z akredytacją podmiotów uprawnionych do wydawania certyfikatów oraz procedur związanych z działaniem tego systemu, regulujących np. kwestie zatwierdzania certyfikatów o poziomie zaufania „wysoki".

Każdy z certyfikatów wydanych w ramach określonego europejskiego programu certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881, będzie automatycznie uznawany w całej Unii Europejskiej. Należy wskazać, że w wielu państwach Europy Środkowej rynek certyfikacji cyberbezpieczeństwa jest mniej rozwinięty niż w Polsce. Przykładem tego może być możliwość uzyskania w Polsce certyfikatów w ramach systemu Common Criteria. W związku z tym wejście w życie projektowanych przepisów może umożliwić polskim przedsiębiorcom przyciągnięcie klientów z regionu.

Ponadto, w ramach uzupełnienia europejskiego systemu certyfikacji, zostaną również wprowadzone krajowe schematy certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. W tym zakresie występuje już

wiele certyfikatów prywatnych, które są wykorzystywane na rynku. Bardzo trudno jest jednak zweryfikować prawdziwą wartość takiego certyfikatu, ponieważ każdorazowo ustala to właściciel takiego „programu certyfikacji". W efekcie często certyfikaty nie realizują swojej funkcji informowania o produktach spełniających określone normy. W związku z tym konieczne jest wprowadzenie oficjalnych schematów certyfikacji cyberbezpieczeństwa, określonych w przepisach, których zasady przyznawania i wymogi będą zawarte w przepisach prawa. Takie regulacje przyjęte w postaci niewiążącej, np. uchwały, nie będą spełniały podobnej roli, gdyż nie będą formalnie różnić się od certyfikatów prywatnych.

Równocześnie należy podkreślić, że krajowe schematy certyfikacji cyberbezpieczeństwa będą nową instytucją prawną. Tak samo ustawa nie wpływa na certyfikaty wydawane obecnie na podstawie różnych prywatnych programów certyfikacyjnych. Pozostają one ważne na zasadach, na jakich zostały wydane. Programy te dalej mogą być stosowane, ale nie będą miały statusu krajowych schematów certyfikacji cyberbezpieczeństwa, a wydane w ich ramach certyfikaty nie będą stanowić krajowych certyfikatów cyberbezpieczeństwa, o których mowa w ustawie. Ponadto również programy certyfikacji realizowane przez podmioty publiczne będą dalej działać na dotychczasowych zasadach.

Krajowe schematy certyfikacji cyberbezpieczeństwa będą mogły również dotyczyć systemów zarządzania cyberbezpieczeństwem oraz wiedzy i umiejętności osób w zakresie cyberbezpieczeństwa. Systemy zarządzania cyberbezpieczeństwem zostały zdefiniowane jako ogół procedur oraz wytycznych służących ochronie zasobów informacyjnych organizacji przed cyberzagrożeniami. Dzięki temu przedsiębiorcy dostaną możliwość uzyskania certyfikatu na cały stosowany u siebie system zarządzania cyberbezpieczeństwem. Z kolei certyfikaty dla poszczególnych osób pozwolą w sposób bezstronny potwierdzić posiadane kompetencje z zakresu cyberbezpieczeństwa oraz wyróżnić się na rynku. Są to szczególnie istotne kwestie, gdyż takie potwierdzenie kompetencji osób czy też organizacji w obszarze cyberbezpieczeństwa pozwoli ich kontrahentom i potencjalnym pracodawcom łatwo określić ich kompetencje i zdecydować, czy chcą z nimi współpracować.

Należy podkreślić, że podmioty prywatne będą również mogły wydawać certyfikaty w ramach krajowych schematów certyfikacji cyberbezpieczeństwa po uzyskaniu akredytacji. W związku z tym rynek certyfikacyjny będzie dostępny dla tych podmiotów.

Takie rozwiązanie jest zgodne z rozporządzeniem 2019/881 w zakresie, w jakim odnosi się ono do krajowych schematów certyfikacji cyberbezpieczeństwa. Rozporządzenie to odnosi się do nich tylko w kontekście programów dotyczących produktów ICT, usług ICT, procesów ICT

i usług zarządzanych w zakresie bezpieczeństwa, które są również objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa. W takim wypadku krajowe schematy certyfikacji cyberbezpieczeństwa odnoszące się do tych produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa przestają działać, a państwo nie może przyjmować nowych programów. W związku z tym wprowadzenie krajowych schematów certyfikacyjnych odnoszących się do osób oraz systemów zarządzania cyberbezpieczeństwem nie będzie w żaden sposób kolidowało z przepisami rozporządzenia 2019/881 w tym zakresie, gdyż będą one dotyczyły innych obszarów merytorycznych.

Wprowadzenie instytucji krajowych schematów certyfikacji cyberbezpieczeństwa pozwoli również podnieść rangę programów certyfikacyjnych tworzonych np. przez państwowe instytuty badawcze, które obecnie funkcjonują jako programy prywatne. Przykładem takiego programu może być program „Firma Bezpieczna Cyfrowo", który jest prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy, zwaną dalej „NASK–PIB". Wprowadzenie krajowych schematów certyfikacji cyberbezpieczeństwa pozwoli podnieść ich rangę i nadać określone ramy prawne. Dzięki przyjęciu programów w formie aktów prawnych będzie również możliwe odwoływanie się do nich w innych przepisach prawa, co pozwoli w szerszym stopniu wykorzystać te certyfikaty na potrzeby administracji.

Dzięki krajowym schematom certyfikacji cyberbezpieczeństwa administracja będzie mogła wpływać na bezpieczeństwo produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa również w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Będzie to również szansa dla rozwoju rynku certyfikacji oraz tworzenie usług dostosowanych ściśle do potrzeb krajowego rynku oraz jego specyfiki.

Krajowy system certyfikacji cyberbezpieczeństwa będzie stanowił zbiór podmiotów, o których mowa w art. 3 ust. 2 (minister właściwy do spraw informatyzacji; Polskie Centrum Akredytacji, zwane dalej „PCA"; jednostki oceniające zgodność; dostawcy, 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; osoby fizyczne, które poddają swoją wiedzę i umiejętności praktyczne ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa; podmioty, które poddają wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach danego

krajowego schematu certyfikacji cyberbezpieczeństwa), 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;
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.

Działając w ramach tego systemu, podmioty będą wspólnie przyczyniać się do poprawy standardów cyberbezpieczeństwa produktów i usług dostępnych na rynku oraz rozwiązań takich jak security by design. Krajowy system certyfikacji cyberbezpieczeństwa będzie cennym uzupełnieniem europejskiego systemu cyberbezpieczeństwa. Stworzy precyzyjny system oceny produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa, dzięki czemu identyfikowane będą produkty spełniające najlepsze standardy w dziedzinie cyberbezpieczeństwa. Projektowane przepisy nie nakładają żadnych dodatkowych obowiązków na podmioty niezainteresowane uczestnictwem w tym systemie. Przyjęty model nie tworzy też barier dostępu do rynku. Przyjęcie przepisów o krajowym systemie certyfikacji cyberbezpieczeństwa będzie miało korzystne skutki dla całego sektora przedsiębiorstw. Obecnie firmy ponoszą coraz większe straty w wyniku działalności cyberprzestępców. Wprowadzenie certyfikacji w dziedzinie cyberbezpieczeństwa sprawi, że firmy uzyskają lepszy dostęp do rozwiązań gwarantujących najwyższy poziom bezpieczeństwa. Ponadto samo zbudowanie systemu certyfikacji cyberbezpieczeństwa przyczyni się do wzrostu świadomości w omawianym obszarze. W efekcie straty ponoszone przez sektor przedsiębiorstw powinny ulec zmniejszeniu.

Projektowane rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne.

Certyfikaty przyczynią się też do wzrostu cyberbezpieczeństwa używanych produktów i usług. Dzięki wizualnemu oznaczeniu certyfikowanych produktów i usług konsumenci otrzymają jasne informacje co do bezpieczeństwa dostępnych na rynku produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa.

Rozporządzenie 2019/881 przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, określające poziom cyberbezpieczeństwa, jaki gwarantuje dany produkt. W odniesieniu do każdego z tych poziomów będą określane odrębne wymagania, jakie musi spełniać produkt, by uzyskać certyfikat danego poziomu. Wymagania dla konkretnych produktów będą zawarte w określonych europejskich programach certyfikacji cyberbezpieczeństwa. Każdy z wydawanych certyfikatów będzie musiał wskazywać, jakiego poziomu dotyczy. Również szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich programach certyfikacji.

Certyfikacja w zakresie cyberbezpieczeństwa będzie procesem całkowicie dobrowolnym i będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku. Projektowana ustawa tworzy ramy, w jakich będzie wykonywana certyfikacja, równocześnie nie nakładając żadnych obowiązków na podmioty działające na rynku. Każdy chętny będzie więc mógł zarówno rozpocząć działalność w tym zakresie, jak i uzyskać certyfikację swojego produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, równocześnie nie będąc do tego zobowiązanym.

W zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179). Stosowne przepisy proceduralne są już wykorzystywane przez podmioty, których dotyczą, a nowym elementem będą jedynie wymagania określane dla każdego z poziomów zaufania.

Podjęcie prac związanych z utworzeniem krajowego systemu certyfikacji cyberbezpieczeństwa wynika z jednej strony z potrzeby dania impulsu do rozwoju rynku w obszarze certyfikacji oraz zapewnienie konsumentom bezpiecznych produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa, a z drugiej strony z konieczności wdrożenia do polskiego porządku prawnego rozporządzenia 2019/881.

Przyjęcie przepisów w zakresie certyfikacji cyberbezpieczeństwa przyczyni się do zwiększenia świadomości znaczenia cyberbezpieczeństwa w sektorze przedsiębiorstw i skłoni przedsiębiorców do stosowania bezpieczniejszych, sprawdzonych rozwiązań. To z kolei, dzięki zwiększeniu zakresu wykorzystania rozwiązań odpornych na cyberataki, będzie służyło podniesieniu poziomu bezpieczeństwa obywateli.

Przepisy rozporządzenia 2018/991 nie pozwalają na inne ukształtowanie roli krajowego organu do spraw certyfikacji cyberbezpieczeństwa, dlatego też w tym zakresie nie ma możliwości zastosowania alternatywnych rozwiązań.

Przyjęte zostały rozwiązania oparte na otwarciu rynku i nie została wyznaczona jedna państwowa jednostka oceniająca zgodność, która wydawałaby certyfikaty odwołujące się do poziomu uzasadnienia zaufania „wysoki". Przyjęcie alternatywnego rozwiązania mogłoby stanowić barierę w rozwoju prywatnych jednostek oceniających zgodność. Alternatywne rozwiązanie w tym zakresie nie pozwala więc osiągnąć wszystkich celów projektowanej ustawy w zakresie rozwoju rynku certyfikacji w Polsce.

Krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował:

- uprawnieniami do nadzoru nad systemem certyfikacji cyberbezpieczeństwa oraz
- narzędziami do usuwania z obiegu prawnego certyfikatów wydanych wbrew przepisom ustawy oraz do kontrolowania podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Projektowana ustawa odnosi się przede wszystkim do produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa. Należy jednak zaznaczyć, że każda z tych trzech kategorii może stanowić wyrób, o którym mowa w przepisach ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. W samych przepisach projektodawca nie posługuje się jednak sformułowaniem „wyrób", gdyż nie zawiera go rozporządzenie 2019/881. Celem projektodawcy jest, aby stosowana w krajowych przepisach terminologia była jak najbardziej zbliżona do europejskiej.

2. Omówienie projektowanych przepisów

Zakres ustawy

Projektowana 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 tego systemu, kontroli działalności tych podmiotów oraz koordynacji ich działalności.

Zakres przedmiotowy projektowanej ustawy wynika ze ścisłego związku tych przepisów z rozporządzeniem 2019/881. Wiele przepisów w zakresie certyfikacji znajduje się w ww. rozporządzeniu i jest bezpośrednio stosowana. Projektowana ustawa skupia się więc na ustanowieniu roli organów państwa w tym obszarze oraz uszczegółowieniu środków kontroli, nadzoru i koordynacji.

Definicje

Projektowana ustawa wprowadza szereg definicji odwołujących się do rozporządzenia 2019/881 oraz innych aktów prawa unijnego. Zapewnia to niezbędną precyzję wykorzystywanych w ustawie sformułowań oraz zapobiega powstaniu wątpliwości interpretacyjnych. Na potrzeby ustawy będzie wykorzystywana nowa definicja cyberbezpieczeństwa, która została zawarta w rozporządzeniu 2019/881. Należy podkreślić, że ta definicja będzie wykorzystywana jedynie na potrzeby niniejszej ustawy, gdyż definiuje ona cyberbezpieczeństwo inaczej niż w podstawowej dla tego obszaru ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), zwanej dalej „uksc". Harmonizacja obu tych obszarów nastąpi w momencie implementacji do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80), tzw. dyrektywy NIS2, co ma zostać dokonane poprzez przyjęcie *ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw* (UC32). Zgodnie z obowiązującą dziś definicją cyberbezpieczeństwa zawartą w art. 2 pkt 4 uksc, cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i niezaprzeczalność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Przyjęte rozwiązanie pozwoli na wprowadzenie przepisów o certyfikacji bez konieczności czekania na wejście w życie innych aktów prawnych.

Projektowana ustawa przewiduje też wprowadzenie pojęcia krajowych schematów certyfikacji cyberbezpieczeństwa, które będą obejmować zarówno krajowe programy certyfikacji zdefiniowane w art. 2 pkt 10 rozporządzenia 2019/881, jak również dokumenty określające wymogi z zakresu cyberbezpieczeństwa na potrzeby certyfikacji osób oraz systemów zarządzania cyberbezpieczeństwem. Wprowadzenie pojęcia „schematu" jest konieczne, aby możliwe było przygotowanie dokumentów analogicznych dla programów certyfikacji dla osób

i systemów zarządzania, a zarazem zachować zgodność z prawem europejskim, które określa, że krajowe programy certyfikacji mogą dotyczyć tylko produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.

Określenie celu krajowego systemu certyfikacji cyberbezpieczeństwa i jego podmiotów

Projekt określa cel krajowego systemu certyfikacji cyberbezpieczeństwa oraz zakres podmiotowy nowego systemu oraz wskazuje organ nadzoru nad jego działaniem. Do systemu będą należały PCA, minister właściwy do spraw informatyzacji, zwany dalej „ministrem", zainteresowane jednostki oceniające zgodność, przedsiębiorcy certyfikujący swoje produkty, osoby fizyczne, które poddadzą swoje kompetencje ocenie zgodności w ramach krajowego schematu certyfikacji cyberbezpieczeństwa oraz podmioty, które poddadzą wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach krajowego schematu certyfikacji cyberbezpieczeństwa. Należy podkreślić, że podmioty prywatne nie będą w żaden sposób zmuszone do dołączenia do tego systemu. Obowiązki z niego wynikające będą więc dotyczyć tylko tych, którzy dobrowolnie się im poddadzą. Tyczy się to zarówno jednostek oceniających zgodność, jak i podmiotów poddających się procesowi certyfikacji.

Dobrowolność certyfikacji

Przepisy projektowanej ustawy wskazują, że certyfikacja produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa będzie odbywać się dobrowolnie, na podstawie umowy zawartej między dostawcą a jednostką oceniającą zgodność. Podstawą dla tej umowy będą wymogi zawarte w odpowiednim krajowym schemacie certyfikacji cyberbezpieczeństwa lub europejskim programie certyfikacji cyberbezpieczeństwa. Ponadto krajowe schematy certyfikacji cyberbezpieczeństwa będą umożliwiały również certyfikację osób fizycznych oraz systemów zarządzania cyberbezpieczeństwem. Umowa będzie podstawą wzajemnych zobowiązań między jednostką oceniającą zgodność a jej klientami, w szczególności będzie określała cenę za usługi jednostki oceniającej zgodność. Równocześnie jednak bardzo wiele elementów samego procesu oceny zgodności będzie określone w konkretnym programie certyfikacji oraz w przepisach go dotyczących. Ponadto w projektowanych przepisach przesądzono jakie kwestie będzie musiała określać umowa o certyfikację. W szczególności umowa będzie musiała regulować zagadnienia związane z ochroną informacji przekazywanych przez klienta, w tym ochronę tajemnic przedsiębiorstwa. Certyfikacja będzie więc procesem dobrowolnym, o rozpoczęciu którego będzie każdorazowo decydował podmiot dysponujący danym produktem ICT, usługą ICT, procesem ICT, usługą

zarządzaną w zakresie bezpieczeństwa, systemem zarządzania cyberbezpieczeństwem czy osoba fizyczna, która chce poddać swoją wiedzę i umiejętności ocenie zgodności. Wskazano również wyraźnie, że ocena zgodności w ramach europejskiego programu certyfikacji cyberbezpieczeństwa będzie dotyczyła wymogów określonych w przewidzianym dla jednego z trzech poziomów uzasadnienia zaufania – podstawowego, istotnego i wysokiego. Poziomy te są zdefiniowane w art. 52 rozporządzenia 2019/881. Im wyższy poziom uzasadnienia zaufania, tym większą gwarancję bezpieczeństwa daje produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa, która została certyfikowana. To, jakiego poziomu będzie dotyczyła certyfikacja, będzie określone w umowie między dostawcą a jednostką oceniającą zgodność. W ramach krajowych schematów certyfikacji cyberbezpieczeństwa nie będzie osobnych poziomów uzasadnienia zaufania. Zamiast nich będą jednolite wymogi dla danych produktów, usług, procesów czy systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych.

Krajowe certyfikaty cyberbezpieczeństwa

Krajowy certyfikat będzie mógł być wydany dla produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa, systemu zarządzania cyberbezpieczeństwem, który zapewnia dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych bądź udostępnianych funkcji lub usług na poziomie odpowiednim do potencjalnych cyberzagrożeń, oraz minimalizuje znane ryzyka w zakresie cyberzagrożeń. W związku z tym posiadanie takiego certyfikatu będzie stanowiło gwarancję odpowiedniego poziomu ochrony.

Z kolei krajowy certyfikat cyberbezpieczeństwa będzie mógł być wydany osobie fizycznej, która posiada wiedzę i praktyczne umiejętności gwarantujące skuteczną realizację zadań z zakresu cyberbezpieczeństwa. Jego posiadacze będą mogli wyróżnić się na rynku pracy, a potencjalni pracodawcy, w tym instytucje publiczne, będą miały dowód ich kompetencji.

Projektowana ustawa określa, że sposób badania spełnienia wymogów będzie każdorazowo dostosowany do przedmiotu danego schematu certyfikacji cyberbezpieczeństwa. Projekt przewiduje, że taką metodą może być: badanie dokumentacji technicznej, audyt, badanie konkretnych właściwości lub analiz funkcjonowania produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa albo systemu zarządzania cyberbezpieczeństwem. Nie wszystkie te metody będą musiały być zastosowane w konkretnym schemacie.

W przypadku krajowych certyfikatów dotyczących osób sprawdzenie ich kompetencji będzie następować w drodze testu wiedzy i umiejętności praktycznych.
Zastosowane metody pozwolą kompleksowo sprawdzić przedmiot certyfikacji i ocenić spełnienie przez niego wymagań określonych w schemacie.
Każdy certyfikat będzie wskazywał dla kogo został wydany, w ramach jakiego schematu certyfikacji cyberbezpieczeństwa, okres, na który został wydany, a także przedmiot certyfikacji oraz datę jego wydania i podpis. Ponadto każdy certyfikat będzie posiadał swoje indywidualne oznaczenie. Każdy certyfikat będzie wydawany na wzorze ustalonym dla danego schematu. Zapewni to transparentność certyfikatów, ułatwi posługiwanie się nimi oraz pozwoli na skuteczną promocję krajowych schematów certyfikacji cyberbezpieczeństwa.
Krajowy certyfikat będzie mógł być wydawany na okres nie krótszy niż 2 lata i nie dłuższy niż 5 lat. Cyberbezpieczeństwo to obszar bardzo szybko rozwijający się, gdzie ciągle pojawiają się nowe technologie i związane z nimi zagrożenia. W związku z tym certyfikat wydany wcześniej może już nie być gwarancją odpowiedniego poziomu cyberbezpieczeństwa. Równocześnie minimalny czas ważności certyfikatu musi być na tyle długi, by miał on znaczenie na rynku. Podmiot, który otrzymał certyfikat, będzie mógł wnioskować o jego przedłużenie. W takim wypadku krajowy schemat certyfikacji cyberbezpieczeństwa będzie przewidywał, jakie czynności są niezbędne do utrzymania certyfikatu. Pozwoli to uniknąć powtarzania całego procesu certyfikacji, co ograniczy koszty i ułatwi działanie przedsiębiorców w tym obszarze.
Dla zapewnienia prawidłowego przebiegu procesu certyfikacji podmiot ubiegający się o certyfikat będzie obowiązany do przekazania jednostce oceniającej zgodność wszystkich niezbędnych informacji związanych z przedmiotem certyfikacji. Jest to niezbędne dla prawidłowego przebiegu procesu certyfikacji oraz monitorowania czy przedmiot certyfikacji spełnia wymogi przez cały okres na jaki został wydany certyfikat.
Projektowana ustawa przewiduje, że dokumentacja techniczna dotycząca przedmiotu certyfikacji będzie musiała być przechowywana przez okres nie dłuższy niż 10 lat od dnia wygaśnięcia certyfikatu. Jest to niezbędne dla potrzeb monitorowania i ewentualnej kontroli prawidłowości działań jednostek oceniających zgodność.

Środki zaradcze

W przypadku wykrycia niezgodności w produkcie ICT, usłudze ICT, procesie ICT, usłudze zarządzanej w zakresie bezpieczeństwa lub systemie zarządzania cyberbezpieczeństwem, dla którego został wydany krajowy certyfikat, posiadacz tego certyfikatu będzie musiał przedstawić w ciągu 14 dni propozycję działań zaradczych, które przywrócą zgodność

z wymogami krajowego schematu certyfikacji cyberbezpieczeństwa. Następnie będzie musiał, we współpracy z jednostką, która wydała certyfikat, przeprowadzić te działania i zapewnić zgodność z wymogami danego krajowego schematu certyfikacji cyberbezpieczeństwa w ciągu 2 miesięcy. W przypadku gdy posiadacz krajowego certyfikatu nie zrealizuje tych obowiązków, jednostka oceniająca zgodność cofa certyfikat. To rozwiązanie gwarantuje, że po wykryciu niezgodności posiadacz certyfikatu nie będzie go od razu tracił, ale będzie mógł przywrócić zgodność z wymogami. Dzięki temu nie będzie musiał przechodzić ponownie całego procesu certyfikacji, co ograniczy koszty, jakie będzie musiał ponieść.

Tworzenie krajowych schematów certyfikacji cyberbezpieczeństwa

Krajowe schematy certyfikacji cyberbezpieczeństwa będą tworzone w drodze rozporządzeń ministra. Przy ich opracowywaniu będzie brany pod uwagę obecny stan wiedzy w dziedzinie techniki oraz kwestia potrzeb rynku w zakresie cyberbezpieczeństwa. Podstawą działania krajowego systemu certyfikacji cyberbezpieczeństwa będą jednak europejskie programy certyfikacji cyberbezpieczeństwa, dlatego też przepis dający ministrowi uprawnienie do tworzenia krajowych schematów certyfikacji cyberbezpieczeństwa został ukształtowany jako fakultatywny. Gwarantuje to zapewnienie zgodności z prawem europejskim. Krajowe schematy certyfikacji cyberbezpieczeństwa będą mogły być wydawane w sytuacji, gdy zostanie to uznane za korzystne dla rozwoju certyfikacji w Polsce. Przygotowanie projektu krajowego schematu certyfikacji cyberbezpieczeństwa będzie zadaniem ministra. Ze względu na konieczność szerokiego wykorzystania wiedzy specjalistycznej w ramach tych prac minister będzie mógł zlecić przygotowanie takiego dokumentu jednostkom przez siebie nadzorowanym, np. instytutom badawczym, takim jak NASK–PIB czy Instytut Łączności – Państwowy Instytut Badawczy. Rozporządzenia te będą wzorowane na rozporządzeniach z art. 9 i art. 10 ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku.

Celem krajowych schematów certyfikacji cyberbezpieczeństwa będzie zapewnienie, by produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa, certyfikowane zgodnie z takimi schematami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa na poziomie ustawy.

Produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami ICT, usługami ICT, procesami ICT lub usługami zarządzanymi w zakresie bezpieczeństwa są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane, w szczególności mając na uwadze, że dotyczy to tak różnych produktów jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa należy doprecyzować na poziomie poszczególnych schematów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych w przypadku, gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować krajowe schematy certyfikacji cyberbezpieczeństwa do konkretnych produktów, zapewni ich skuteczność.

Należy wskazać, że ta różnorodność wpływa na wszelkie aspekty krajowych schematów certyfikacji cyberbezpieczeństwa, np. w wypadku wykrycia w certyfikowanym programie komputerowym podatności producent może mieć możliwość usunięcia tej wady przez jego aktualizację, podczas gdy wykrycie określonej podatności w przenośnej pamięci USB może wymusić konieczność wycofania określonej partii towaru z rynku. Tak samo dalsze monitorowanie spełnienia wymogów określonych w danym schemacie może wymagać zupełnie różnych metod. Ponadto każdy ze schematów będzie musiał być opracowywany przez innych ekspertów, tak by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.

Krajowe schematy będą mogły wprowadzić również wymogi dla systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych, dzięki czemu również w tych obszarach będzie możliwa promocja najlepszych rozwiązań z zakresu cyberbezpieczeństwa.

Rola PCA

Projektowana ustawa wprowadza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne PCA. Aby prowadzić ocenę zgodności produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych, zainteresowane podmioty będą musiały uzyskać akredytację PCA. Wymagania dla zainteresowanych zostały określone w załączniku do rozporządzenia 2019/881. Podstawą działania PCA w tym zakresie będzie rozdział 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Są

to przepisy, na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania ze strony PCA.

Sprawna wymiana informacji między PCA sprawującym nadzór nad akredytacją a ministrem jest niezbędna do sprawnego działania nowego systemu. W związku z tym PCA będzie informować ministra o dokonanych akredytacjach oraz o odmowie ich dokonania. Proponowane rozwiązanie gwarantuje, że minister będzie należycie poinformowany o wszystkich podmiotach wydających certyfikaty oraz będzie posiadał informacje niezbędne do prowadzenia nadzoru nad tym rynkiem.

Projektowana ustawa wskazuje, że PCA będzie nadzorowało jednostki oceniające zgodność pod kątem spełnienia przez nie wymogów akredytacji. PCA będzie pełniło taką samą rolę, jaką pełni w ogólnym systemie oceny zgodności. Zapewni to szybkie wdrożenie nowych przepisów w praktyce oraz spójność rozwiązań w zakresie akredytacji.

Kwestię ewentualnej odpowiedzialności PCA za działania podejmowane w ramach krajowego systemu certyfikacji cyberbezpieczeństwa będą określone w umowach między PCA a akredytowanymi jednostkami.

Zadania ministra

Projektowana ustawa określa zadania ministra. Zadania te wynikają wprost z przepisów rozporządzenia 2019/881 i dotyczą nadzoru oraz kontroli nad podmiotami tego systemu, jak również współpracy międzynarodowej w tym zakresie.

Minister będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w uksc. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania projektowanej ustawy.

W ramach obowiązków krajowego organu administracji rządowej właściwego w sprawach certyfikacji cyberbezpieczeństwa minister będzie prowadzić szereg postępowań administracyjnych dotyczących m.in.:

1) wyrażania zgody na wydanie europejskich certyfikatów odwołujących się do poziomu zaufania „wysoki”;
2) wydawania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających;

3) cofania i ograniczania zezwoleń na prowadzenie oceny zgodności w przypadku, gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających zgodność;
4) cofania certyfikatu odwołującego się do poziomu uzasadnienia zaufania „wysoki" wydanego wbrew przepisom rozporządzenia 2019/88 lub ustawy lub wbrew postanowieniom programu certyfikacyjnego;
5) nakładania kar pieniężnych.

Wszystkie rozstrzygnięcia w tym zakresie będą wydawane zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572) z zastrzeżeniem, że wydawanie zezwoleń na prowadzenie oceny zgodności, w przypadku gdy program certyfikacyjny określa szczególne wymagania dla jednostek oceniających, odbędzie się w tzw. postępowaniu uproszczonym, a pozostałe – w ogólnym.

Do obowiązków ministra jako krajowego organu administracji rządowej właściwego w sprawach certyfikacji cyberbezpieczeństwa będą również należały kwestie współpracy z analogicznymi organami w innych państwach Unii Europejskiej, jak również przeprowadzanie wzajemnych przeglądów z tymi organami, o których mowa w art. 59 rozporządzenia 2019/881. W ramach przeglądów organy będą nawzajem oceniać swoje działania i funkcjonowanie krajowych systemów certyfikacji cyberbezpieczeństwa. Konieczność wdrożenia tej procedury wynika wprost z przepisów rozporządzenia 2019/881.

Minister będzie również odpowiedzialny za tworzenie krajowych schematów certyfikacji cyberbezpieczeństwa. Posiada on najlepszą wiedzę zarówno o rynku ICT, jak i o samej certyfikacji cyberbezpieczeństwa, oraz nadzoruje państwowe instytuty badawcze zajmujące się cyberbezpieczeństwem, dzięki czemu posiada kompetencje niezbędne do przygotowania tych schematów.

Przepisy projektowanej ustawy przesądzają również, że zadania krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz zadania z zakresu nadzoru nad państwowymi instytutami badawczymi nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym ministra właściwego do spraw informatyzacji. Gwarantuje to, że nie wystąpi konflikt interesów przy wykonywaniu nowych zadań.

Zlecanie wykonania określonych czynności na rzecz ministra

Rynek certyfikacji cyberbezpieczeństwa jest obszarem wymagającym wysokich kwalifikacji oraz specjalistycznej wiedzy. Minister będzie rozwijał swoje zdolności w tym zakresie, ale również ze względu na różnorodność programów certyfikacyjnych do realizacji swoich zadań

będzie musiał korzystać z wiedzy ekspertów zewnętrznych. Podstawowym źródłem takiej wiedzy będą państwowe instytuty badawcze, które są nadzorowane przez tego ministra, w szczególności NASK–PIB oraz Instytut Łączności – Państwowy Instytut Badawczy. Są to doświadczone jednostki badawcze, które już obecnie dysponują kompetencjami w zakresie certyfikacji, gdyż np. wykonują już czynności w zakresie certyfikacji w metodologii Common Criteria – jednej z najstarszych i najbardziej zaawansowanych metodologii certyfikacji cyberbezpieczeństwa. Z tego względu projektowana ustawa przewiduje, że będą one wykonywały w porozumieniu z ministrem te zadania, które wymagają odpowiednich kompetencji czy infrastruktury, np. laboratoriów. Aby zapewnić finansowanie tych zadań na odpowiednim poziomie minister będzie mógł udzielić dotacji celowej na realizację tych zadań, tak aby zapewnić ich skuteczną realizację. W szczególności środki te mają służyć budowaniu infrastruktury oraz zaplecza eksperckiego. W związku z kompetencjami tych podmiotów są one również najlepiej przygotowane do przygotowania krajowych schematów certyfikacji cyberbezpieczeństwa.

Należy podkreślić, że realizacja tych zadań nie może wiązać się z powtórzeniem całego procesu oceny zgodności. W związku z tym, w ramach wspierania ministra właściwego do spraw informatyzacji w nadzorze, będą one mogły powtórzyć określoną czynność dokonaną w ramach tego procesu, ale nie cały proces.

Będą one mogły również wspierać ministra właściwego do spraw informatyzacji w zakresie weryfikacji kompetencji osób realizujących zadania z zakresu oceny zgodności w obszarze cyberbezpieczeństwa. Wymogi dla personelu jednostek oceniających zgodność są określone w załączniku do rozporządzenia 2019/881, w związku z czym kompetencje w tym obszarze są niezbędne dla zapewnienia prawidłowej realizacji zadań wynikających z prawa europejskiego. Ujednolicono również możliwość wspierania ministra właściwego do spraw informatyzacji przez instytuty badawcze przez niego nadzorowane i inne instytuty badawcze. Zapewnia to równe traktowanie wszystkich tych podmiotów.

W związku z tym, że będą pojawiały się kolejne europejskie programy certyfikacji cyberbezpieczeństwa, nie jest możliwe ustalenie precyzyjnie zakresu wiedzy i kompetencji potrzebnych w przyszłości. Dlatego projektowana ustawa przewiduje, że również instytuty badawcze nadzorowane przez inne organy, za zgodą tych organów, będą mogły wspierać ministra właściwego do spraw informatyzacji w wykonywaniu zadań związanych z certyfikacją cyberbezpieczeństwa. Gwarantuje to, że w kluczowym obszarze cyberbezpieczeństwa będzie możliwe wykorzystanie pełnego potencjału wiedzy, jaki posiadają państwowe instytuty badawcze.

Regulacją tą będą objęte również jednostki organizacyjne podległe Ministerstwu Obrony Narodowej. Jednostki te również mają doświadczenie w obszarze certyfikacji cyberbezpieczeństwa, w związku z czym uwzględnienie ich w ramach krajowego systemu certyfikacji cyberbezpieczeństwa pozwoli na lepszą koordynację polityki państwa w tym obszarze.

Projektowane przepisy określają też, że państwowe instytuty badawcze powinny rozwijać swoje kompetencje oraz rozwijać swoje kadry tak, aby móc skutecznie realizować te zadania. Gromadzenie kompetencji jest czymś, co będzie przynosiło korzyść na przyszłość i jest szczególnie istotne w obszarze, który wymaga dużych kompetencji oraz możliwości technicznych.

Projektowane przepisy zapewniają ponadto podstawę prawną do zlecania określonych czynności podmiotom innym niż państwowe instytuty badawcze. Jak wskazano powyżej rozwój europejskich programów certyfikacji może spowodować, że konieczne będzie wykorzystanie kompetencji w obszarze, w którym instytuty badawcze nie dysponują odpowiednią wiedzą. Innym przykładem sytuacji, w której zastosowanie tego przepisu będzie konieczne, to sytuacja konfliktu interesów, np. jeśli minister będzie musiał ocenić czynności dokonane przez któryś z instytutów badawczych. W takiej sytuacji musi istnieć możliwość skorzystania z wiedzy innych podmiotów. Jest to jednak szczególna sytuacja i podstawowymi podmiotami wspierającymi ministra mają być państwowe instytuty badawcze. Jest to niezbędne dla zapewnienia skutecznej realizacji zadań krajowego organu administracji rządowej właściwego w sprawach certyfikacji cyberbezpieczeństwa w niezwykle szybko zmieniającym się obszarze cyberbezpieczeństwa. W związku z wprowadzonymi zmianami, dla zapewnienia spójności przepisów, w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych zostanie wskazane , że wsparcie ministra właściwego do spraw informatyzacji w tym obszarze należy do kompetencji instytutów badawczych.

Przepisy gwarantują również, że dany instytut badawczy nie będzie mógł uczestniczyć w czynnościach związanych z wydanymi przez siebie certyfikatami.

Zezwolenie na prowadzenie oceny zgodności

Projektowana ustawa reguluje sytuację, w której określony europejski program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku oprócz akredytacji jednostki te będą musiały uzyskać zezwolenia ministra. Zezwolenia wynikają wprost z obowiązku wdrożenia rozporządzenia 2019/881. Jeśli bowiem europejskie programy certyfikacyjne będą zawierały postanowienia o szczególnych

wymaganiach w zakresie jednostek oceniających zgodność, musi istnieć organ sprawdzający te wymagania oraz zezwalający na działanie jednostek w ramach określonego programu certyfikacji. Należy podkreślić, że w związku z tym, że postępowanie to dotyczy spełnienia formalnych kryteriów, zdecydowano o zastosowaniu w tym przypadku przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego dotyczących postępowania uproszczonego. Pozwoli to maksymalnie przyśpieszyć postępowanie oraz ograniczy formalności. Minister w ramach sprawowanego nadzoru będzie mógł również zmieniać zakres udzielonego zezwolenia, jak również je cofnąć w przypadku, gdy dana jednostka przestanie spełniać określone wymagania. Gwarantuje to zachowanie odpowiedniej jakości usług świadczonych przez jednostki oceniające zgodność.

Ze względu na to, że zezwolenie to nie zastępuje akredytacji, ale jest dodatkową formą gwarancji spełnienia wymogów przez jednostkę oceniającą zgodność, projektowane przepisy wskazują, że zakres zezwolenia nie może być inny niż zakres akredytacji. W szczególności w przypadku, gdy akredytacja o takim zakresie zostanie cofnięta, wygaśnie również zezwolenie.

Projektowana ustawa reguluje również postępowanie w przypadku stwierdzenia, że podmiot, który otrzymał zezwolenie ministra na prowadzenie oceny zgodności przestał spełniać wymagania zawarte w określonym europejskim programie certyfikacji cyberbezpieczeństwa. W przypadku stwierdzenia naruszenia przepisów rozporządzenia 2019/881, ustawy lub postanowień określonego europejskiego programu certyfikacji cyberbezpieczeństwa minister będzie mógł z urzędu zawiesić wydane zezwolenie na czas określony nie dłuższy niż 2 lata, dając jednostce czas na usunięcie naruszeń. Zawieszenie zezwolenia będzie stosowane w przypadku, gdy dane naruszenie wymagań określonych w przepisach ma charakter odwracalny, nie wystąpiło w danej jednostce w ciągu ostatnich 3 lat, nie było związane z popełnieniem przestępstwa oraz nie podważa zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa. Przyjęte przesłanki mają zapewnić prawidłowe funkcjonowanie krajowego systemu certyfikacji cyberbezpieczeństwa. W przypadku gdy przywrócenie sytuacji zgodności z przepisami nie jest możliwe, zezwolenie będzie od razu cofane. Również jeśli to samo naruszenie występuje w danej jednostce kolejny raz w ciągu ostatnich 3 lat lub jest związane z popełnieniem przestępstwa, zasadne jest natychmiastowe cofnięcie zezwolenia. Przesłanka podważania zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa służy sankcjonowaniu sytuacji związanych z poważnym naruszeniem przyjętych zasad, które jednak niekoniecznie będzie związane z popełnieniem przestępstwa. W szczególności obejmie ona sytuacje związane z dokonaniem określonych czynności w zamian za korzyści materialne lub

osobiste. Ze względu na to, że jednostkami oceniającymi zgodność będą również podmioty prywatne, takie działania nie zawsze będą równoznaczne z naruszeniem przepisów karnych. Równocześnie ich szczególnie naganne okoliczności sprawiają, że konieczne jest podjęcie zdecydowanych działań, aby uniknąć utraty zaufania do wydanych certyfikatów.

Trzyletni termin dotyczący przesłanki powtarzania się niezgodności został przyjęty tak, aby nie mogła wystąpić sytuacja, w której w danym podmiocie ciągle występuje to samo naruszenie. Równocześnie uwzględniona została długość procesu oceny zgodności, który w przypadku bardziej skomplikowanych metodologii, jak np. w programie EUCC, może trwać nawet powyżej roku.

Również w sytuacji, gdy w wyznaczonym terminie naruszenia nie zostaną usunięte, minister cofa wydane zezwolenie. Taki sposób postępowania gwarantuje ochronę interesu publicznego, równocześnie dając przedsiębiorcy czas na usunięcie naruszeń, nie wymuszając na nim jednocześnie ponownego przechodzenia postępowania o wydanie zezwolenia.

W ramach postępowań związanych z zezwoleniami minister będzie mógł zasięgać opinii innych podmiotów w ramach postępowań związanych z zezwoleniem na prowadzenie oceny zgodności. Ze względu na znaczącą rolę specjalistycznej wiedzy w tym obszarze konieczne jest wyraźne podkreślenie możliwości skorzystania z wiedzy innych podmiotów.

Rezygnacja z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy

W ramach przygotowywanych przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) programów certyfikacji pojawiła się procedura wyrażania zgody na rezygnację w uzasadnionym przypadku z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy. Tego typu wyjątek od standardowej procedury certyfikacji wymaga zgody organu właściwego do spraw cyberbezpieczeństwa. W związku z tym konieczne było ustanowienie odpowiedniej procedury w przepisach krajowych.

Wprowadzanie zmian w metodyce oceny, która ma być stosowana przez jednostkę oceniającą zgodność

W ramach przygotowywanych przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) programów certyfikacji pojawiła się procedura wprowadzenia zmian w metodyce oceny stosowanej przez jednostkę oceniającą zgodność. Tego typu wyjątek od standardowej procedury certyfikacji wymaga zgody organu właściwego do spraw cyberbezpieczeństwa. W związku z tym konieczne było ustanowienie odpowiedniej procedury w przepisach krajowych.

Wyrażenie zgody na wydanie certyfikatów odwołujących się do poziomu uzasadnienia zaufania „wysoki”

Projektowane przepisy ustawy wprowadzają dodatkową gwarancję dla certyfikatów najwyższego poziomu. Wydanie takiego certyfikatu będzie możliwe tylko po otrzymaniu zgody ministra na jego wydanie. Zezwolenie będzie wydane po wydaniu decyzji certyfikacyjnej przez jednostkę oceniającą zgodność, ale przed wydaniem certyfikatu. Na tym etapie sam proces certyfikacji został już zakończony i można ocenić prawidłowość jego przeprowadzenia. Odmowa wydania zezwolenia jest możliwa w przypadku, gdy certyfikat został wydany wbrew przepisom rozporządzenia 2019/881, ustawy lub postanowieniom określonego europejskiego programu certyfikacji cyberbezpieczeństwa, w ramach którego prowadzona była procedura. Do postępowania będą stosowane przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe dla jego stron. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające przebieg procesu oceny zgodności. Projektowane przepisy przewidują ponadto, że w przypadku, gdy będzie to konieczne, minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów naukowych o wypowiedzenie się w kwestii danego programu certyfikacji. Wymóg ten służy przyśpieszeniu postępowania przez przekazanie do ministra potrzebnych mu dokumentów wraz z wnioskiem wszczynającym postępowanie. Bez tego przepisu minister musiałby wystąpić do jednostki, która wydała certyfikat, o te dokumenty, co przedłużyłoby cały proces.

Przepis ten reguluje również kwestie cofania certyfikatów wydanych niezgodnie z rozporządzeniem 2019/881, ustawą lub przepisami europejskiego programu certyfikacyjnego. Obowiązek wprowadzenia takiej procedury wynika z rozporządzenia 2019/881. Cofanie certyfikatów będzie dotyczyło tych certyfikatów, które już zostały wydane i odwołują się do poziomu uzasadnienia zaufania „wysoki”. Minister nie ponosi odpowiedzialności za ewentualne szkody wywołane cofnięciem certyfikatu. Cofnięcie certyfikatu może bowiem spowodować określone szkody dla podmiotu, którego dotyczy. Jest to jednak uprawnienie wynikające bezpośrednio z prawa europejskiego i w związku z tym prawidłowe korzystanie z niego nie może powodować obowiązków odszkodowawczych po stronie organu.

W celu zapewnienia możliwości usunięcia nieprawidłowości minister cofa certyfikat jedynie w przypadku, 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.

Każdy z tych trzech przypadków jest związany z zagrożeniem dla użytkowników danych produktów i usług czy kontrahentów podmiotów, które poddały certyfikacji swoje systemy zarządzania cyberbezpieczeństwem. W związku z powyższym w takich przypadkach konieczne jest podjęcie zdecydowanych działań i cofnięcie certyfikatu. W innych przypadkach certyfikat zostanie zawieszony, a jego posiadacz będzie miał możliwość usunięcia nieprawidłowości. W przypadku gdy w wyznaczonym terminie nie będzie w stanie tego uczynić, certyfikat zostanie cofnięty. Takie rozwiązanie pozwoli na zapewnienie trwałości wydanych certyfikatów. Możliwość usunięcia niewielkich niezgodności będzie dodatkową zachętą do inwestowania w europejskie i krajowe certyfikaty cyberbezpieczeństwa.

Zgodnie z art. 147 ust. 2 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841) doręczenie korespondencji nadanej przez osobę fizyczną lub podmiot niebędący podmiotem publicznym, będące użytkownikami konta w ePUAP, do podmiotu publicznego posiadającego elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne w skutkach prawnych z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego, do czasu zaistnienia obowiązku stosowania ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, przez ten podmiot publiczny. Innymi słowy do czasu rozpoczęcia stosowania przez ministra przepisów ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych sprzeciw będzie mógł być złożony na jego elektroniczną skrzynkę podawczą ePUAP.

W związku ze zmianą rozporządzenia 2019/881 przepisy te objęły również certyfikaty wydane dla usług zarządzanych w zakresie bezpieczeństwa. Zmiana ta jest niezbędna dla zapewnienia prawidłowego wykonania prawa europejskiego. Zapewni to również jednolite traktowanie wszystkich europejskich certyfikatów odwołujących się do poziomu uzasadnienia zaufania „wysoki".

Przekazanie informacji o wydaniu lub cofnięciu certyfikatu

Projektowana ustawa nakłada na jednostkę oceniającą zgodność obowiązek przekazania ministrowi danych podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia. Obowiązek ten umożliwia ministrowi sprawowanie skutecznego nadzoru nad całym krajowym systemem certyfikacji cyberbezpieczeństwa. W przypadku przekazania niepełnych danych minister może wystąpić o ich uzupełnienie, a jednostka oceniająca zgodność musi je uzupełnić w ciągu 14 dni.

Rozpatrywanie skarg

Każdy będzie mógł złożyć skargę na działania jednostki certyfikującej. Dokładną procedurę postępowania z taką skargą będą określały same jednostki oceniające zgodność i publikowały ją na swoich stronach internetowych. Będą jednak musiały zagwarantować, że skargę rozpatrują inne osoby niż te, które podejmowały dane działanie podjęte podczas certyfikacji. Rozstrzygnięcie skargi nie może trwać dłużej niż 2 miesiące, co gwarantuje, że decyzja zostanie podjęta w odpowiednim terminie. Możliwość zgłaszania skarg do jednostek wydających certyfikaty gwarantuje art. 63 rozporządzenia 2019/881. Równocześnie jest to rozwiązanie elastyczne, które pozwoli jednostkom oceniającym zgodność ustalić procedury dostosowane do ich wewnętrznej struktury. Projektowana ustawa wskazuje, że minister jest organem właściwym do rozpatrywania skarg na podmioty, które wydały deklaracje zgodności zgodnie z określonym europejskim programem certyfikacji cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa, dla których wystawiono deklarację zgodności, nie spełnia wymagań zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa. To uprawnienie dla ministra wynika wprost z przepisów rozporządzenia 2019/881. Należy zauważyć, że przepisy dotyczące skarg tworzą tylko ogólne ramy dla rozpatrywania skarg. Szczegółowo kwestie te będą regulowane w rozporządzeniach wykonawczych wydawanych przez Komisję Europejską dla poszczególnych programów certyfikacyjnych. Należy podkreślić, że będą one odrębnie określane dla każdego kolejnego programu, co sprawia, że konieczne jest pozostawienie wielu kwestii nieuregulowanych w przepisach krajowych. Skargi składane do ministra rozpatrywane będą zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra, wskazano, że przepisy te będą stosowane odpowiednio.

Równocześnie wprowadzono dwie odrębności w stosunku do rozwiązań zawartych w ustawie z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego dotyczące skarg i wniosków. Aby zwiększyć ochronę prawną osób składających skargi wskazano wyraźnie termin, w jakim organ ma odnieść się do ich skargi. W przypadku gdy osoba zgłaszająca skargę ma w tym interes prawny, będzie mogła skorzystać ze skargi na przewlekłość postępowania. Gwarantuje to odpowiedni poziom ochrony praw skarżących.
Obie opisane procedury skargowe są od siebie niezależne i mogą być stosowane równolegle.

Przekazywanie informacji do ministra

Podmioty krajowego systemu certyfikacji cyberbezpieczeństwa będą musiały przekazywać ministrowi wyjaśnienia w kwestiach związanych z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa. Daje to ministrowi możliwość sprawdzania otrzymywanych informacji bez konieczności stosowania długotrwałej i uciążliwej dla przedsiębiorcy procedury kontrolnej. Umożliwi to również ministrowi zbieranie informacji o zjawiskach zachodzących na rynku certyfikacji.

Kontrola

Przepisy projektowanej ustawy ustanawiają podstawę prawną dla prowadzenia przez ministra kontroli podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Do kontroli przeprowadzanej wobec podmiotów administracyjnych będą stosowane przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224), a w przypadku przedsiębiorców – przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. z 2024 r. poz. 236, 1222 i 1871 oraz z 2025 r. poz. 222) oraz art. 55-59 uksc. W związku z tym prawa strony postępowania będą odpowiednio chronione. Pozwoli to na skuteczną realizację obowiązków nadzorczych. Przepisy o kontroli nie będą dotyczyły osób fizycznych, które poddały swoją wiedzę i umiejętności ocenie w ramach krajowych schematów certyfikacji cyberbezpieczeństwa. Wskazane przepisy dotyczące kontroli odnoszą się do organizacji i w związku z tym nie byłoby możliwe zastosowanie ich do osób. Ponadto nie służą one sprawdzaniu wiedzy i kompetencji osób.

Zasady prowadzenia kontroli

Projektowana ustawa wskazuje, że do kontroli będą stosowane odpowiednio przepisy art. 55–59 uksc. Dzięki temu minister będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli, co pozwoli na najszybsze wdrożenie się do nowych obowiązków. W art. 55 pkt 1–6 uksc wskazany jest zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zaznaczyć, że uprawnienia wynikające z art. 55 uksc

dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że uprawnienia te nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli. Przepis art. 57 uksc wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58 uksc). W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, że protokół podpisuje osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole. W art. 59 uksc wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli organ właściwy lub minister uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie poinformować organ właściwy lub ministra o sposobie wykonania zaleceń. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej.

Uprawnienie do badania produktów ICT

Dla zapewnienia realnej kontroli nad jakością produktów, które otrzymały certyfikaty, minister został wyposażony w uprawnienia do przeprowadzania badań produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa oraz systemów zarządzania cyberbezpieczeństwem. W zakresie analizy technicznej produktów ICT minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów badawczych o wykonanie określonych czynności. Tego typu uprawnienie jest niezbędne dla zapewnienia realnego nadzoru nad jakością produktów na rynku. Należy podkreślić, że obecnie przygotowywane rozporządzenia

wykonawcze Komisji Europejskiej, w których wprowadzane są programy certyfikacyjne, mają nakładać na krajowe organy do spraw certyfikacji obowiązek przeprowadzenia określonej liczby badań produktów. W związku z tym konieczne jest zapewnienie ministrowi odpowiedniego uprawnienia.

Procedura pobierania próbek i badania produktów ICT

Przepisy projektowanej ustawy określają procedurę przeprowadzania badań produktów ICT oraz konsekwencje wykrycia, że produkt ICT nie spełnia wymagań określonych w odpowiednim programie certyfikacji. Projektowany przepis precyzuje kwestie dotyczące protokołu z pobrania próbki oraz określa kto ponosi koszt przeprowadzanych badań. Przepis został zaprojektowany tak, aby zapewnić skuteczne pobieranie próbek i przeprowadzanie badań, przy jednoczesnym zapewnieniu ochrony praw dostawcy produktu ICT.

Konsekwencje niespełniania wymagań po certyfikacji

Przepisy projektowanej ustawy określają uprawnienia ministra w przypadku, gdy poważnie uzasadnione podejrzenie, że określony produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa lub system zarządzania cyberbezpieczeństwem nie spełnia wymagań zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa albo krajowym schemacie certyfikacji cyberbezpieczeństwa. W takiej sytuacji minister przekazuje właściwą informację podmiotowi, który wydał certyfikat. W efekcie jednostka, która wydała certyfikat, będzie mogła zastosować odpowiednie postanowienia określonego europejskiego programu certyfikacji cyberbezpieczeństwa, regulujące takie sytuacje.

Kary administracyjne

Projektowana ustawa przewiduje nałożenie kary administracyjnej na jednostkę oceniającą zgodność za działanie bez wymaganej akredytacji. Przypadki niewypełnienia innych obowiązków, np. informacyjnych, utrudnianie przeprowadzenia kontroli, również są penalizowane w podobny sposób. Odpowiedzialności podlegać będą ponadto m.in. osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, które utrudniają lub uniemożliwiają właściwym organom prowadzenie czynności kontrolnych. Wysokość kar administracyjnych została odpowiednio zróżnicowana, tak by były one skuteczne, proporcjonalne do czynu oraz odstraszające. Kary będzie nakładał minister w ramach swojej roli jako krajowego organu do spraw certyfikacji cyberbezpieczeństwa. Kary będą stanowiły przychód Funduszu Cyberbezpieczeństwa. Pozwoli to zapewnić dodatkowe środki dla tego Funduszu i przyczyni się do wzrostu cyberbezpieczeństwa w podmiotach administracji publicznej. W związku z powyższym 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) uzupełniono katalog przychodów Funduszu Cyberbezpieczeństwa o kary wydawane na podstawie projektowanej ustawy.

Postępowanie dotyczące kar będzie prowadzone na podstawie przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Aby zapewnić prawidłową ochronę strony postępowania, wskazano, że w przypadku nałożenia kary będzie ona mogła wnieść skargę do wojewódzkiego sądu administracyjnego. Kary pieniężne będą podlegały egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym. Zapewni to spójność rozwiązań w zakresie egzekucji z innymi przepisami w tym zakresie.

Przepisy przejściowe i dostosowujące

Projektowana ustawa wskazuje, że akredytacje udzielone przez PCA jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie niniejszej ustawy są akredytacjami oraz certyfikaty wydane w ramach tych akredytacji pozostają ważne i stosuje się do nich przepisy dotychczasowe. Zagwarantuje to utrzymanie w mocy dotychczasowych certyfikatów oraz zapewni ciągłość działania wszystkich podmiotów, które do tej pory operowały w tym obszarze.

Reguła wydatkowa

Projektowana ustawa określa również limit wydatków na nowe zadania realizowane przez ministra oraz PCA. Wydatkowanie środków na cele rozwoju krajowego organu do spraw cyberbezpieczeństwa oraz publicznych jednostek oceniających zgodność rozpocznie się w 2025 r. Oznacza to konieczność zatrudnienia dodatkowych osób oraz zapewnienia im narzędzi pracy. W przypadku PCA dodatkowe środki mają pozwolić na zatrudnienie dodatkowych ekspertów z zakresu cyberbezpieczeństwa oraz na skuteczną realizację zadań nadzorczych nad rosnącą listą podmiotów. W kolejnych latach wzrost wydatków wynika z zapewnienia możliwości certyfikacji w jednostkach publicznych oraz opłacenia zewnętrznych opinii.

Zmiany w innych ustawach

Konieczne jest również dostosowanie innych ustaw do rozwiązań zawartych w projektowanej ustawie. Pierwszą taką ustawą jest ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych, w której do katalogu działań, jakie mogą podejmować instytuty badawcze, zostanie dodane wspieranie ministra właściwego do spraw informatyzacji w sprawach nadzoru nad krajowym systemem certyfikacji cyberbezpieczeństwa. Konkretne zadania w tym zakresie znajdują się w projektowanej ustawie. Ze względu na to, że są to zadania wymagające specjalistycznej

wiedzy i kompetencji to instytuty badawcze są najlepiej przygotowanymi do tego zadania podmiotami. Zmiana ta jest również niezbędna dla zapewnienia spójności systemu prawnego. Drugą niezbędną zmianą jest zmiana ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w której do katalogu przychodów Funduszu Cyberbezpieczeństwa zostaną dodane wpływy z kar pieniężnych, zawartych w projektowanej ustawie. Tę kwestię merytorycznie przesądza już ww. projekt, a zmiana w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa służy zapewnieniu spójności obu tych regulacji.

Wejście w życie

Projektowana ustawa wejdzie w życie po upływie miesiąca od dnia jej ogłoszenia. Taki termin gwarantuje, że wszystkie podmioty, których dotyczą projektowane przepisy, będą miały czas na zapoznanie się z nimi i przygotowanie się do ich stosowania.

Projekt ustawy nie zawiera przepisów technicznych w rozumieniu przepisów rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i w związku z tym nie podlega procedurze notyfikacji.

Projekt ustawy jest zgodny z przepisami prawa Unii Europejskiej i służy ich stosowaniu.

Projekt ustawy nie podlega przedstawieniu właściwym organom i instytucjom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535), projekt został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

Nazwa projektu Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Paweł Olszewski, Sekretarz Stanu **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa e-mail: Sekretariat.DC@cyfra.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa e-mail: Sekretariat.DC@cyfra.gov.pl	**Data sporządzenia** 09.04.2025 r. **Źródło:** Rozporządzenie 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) **Nr w Wykazie prac legislacyjnych Rady Ministrów:** UC42

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowana ustawa ma na celu dostosowanie polskiego porządku prawnego do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) 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), zwanym dalej „rozporządzeniem 2019/881". Uwzględnia również zmiany wprowadzone w rozporządzeniu 2019/881 przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2025/37 z dnia 19 grudnia 2024 r. w sprawie zmiany rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa, które rozszerzyło zakres tego aktu prawnego o usługi zarządzane w zakresie bezpieczeństwa (Dz. Urz. UE L 2025/37 z 15.01.2025). Projekt stanowi również realizację celu szczegółowego 2. nieobowiązującej już Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 – podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Rola sieci i systemów teleinformatycznych wzrosła niepomiernie w ostatnich latach, sprawiając, że stały się one niezbędnym elementem współczesnej gospodarki. W związku z pandemią COVID-19 oraz atakiem Rosji na Ukrainę proces ten postępuje coraz szybciej. Jako że społeczeństwa coraz bardziej będą polegały na produktach i usługach funkcjonujących w cyberprzestrzeni, tym istotniejsze staje się zapewnienie bezpieczeństwa działań podejmowanych na tej płaszczyźnie. Wprowadzenie jednolitych zasad przyznawania certyfikatów cyberbezpieczeństwa i ich wzajemne uznawanie w państwach Unii Europejskiej zapewnią, że przedsiębiorstwa będą w stanie lepiej zabezpieczyć swoje interesy w cyberprzestrzeni. Wzajemne uznawanie certyfikatów zapewni im ponadto lepszą pozycję w konkurencji na rynku europejskim. Działania te przyczynią się do ogólnego wzrostu bezpieczeństwa w cyberprzestrzeni poprzez promocję najbezpieczniejszych rozwiązań oraz dostarczenie konsumentom informacji o bezpieczeństwie produktów i usług. Wyraźne wsparcie państwa w zakresie certyfikacji powinno również przyczynić się do zwiększenia świadomości społecznej w kwestii cyberbezpieczeństwa.

Przyjęcie proponowanych przepisów może dać polskim przedsiębiorcom dużą szansę na pozyskanie klientów z sąsiednich krajów zainteresowanych certyfikacją swoich produktów. Będzie to więc szansą na znaczne poszerzenie bazy potencjalnych klientów. Z kolei producenci i dostawcy produktów uzyskają możliwość otrzymania certyfikatów dla swoich produktów i usług, które będą ważne na obszarze całej Unii Europejskiej. Należy podkreślić, że jeśli przepisy te nie zostałyby przyjęte, to polscy producenci musieliby korzystać z usług jednostek certyfikujących z innych krajów UE, co nie byłoby korzystne dla polskiej gospodarki.

Przyjęte w projektowanej ustawie rozwiązania umożliwią również tworzenie krajowych schematów certyfikacji cyberbezpieczeństwa. Dzięki temu możliwe będzie zwiększenie cyberbezpieczeństwa w obszarach uznanych za kluczowe.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Celem projektowanej ustawy jest:

1) określenie organizacji systemu certyfikacji cyberbezpieczeństwa w Polsce, w szczególności ustanowienie procedur niezbędnych do zapewnienia prawidłowości procesów certyfikacyjnych;
2) określenie sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy;
3) stworzenie podstawy do tworzenia krajowych schematów certyfikacji cyberbezpieczeństwa.

Powyższe działania mają doprowadzić do rozwoju rynku certyfikacji cyberbezpieczeństwa w Polsce, a przez to do zwiększenia bezpieczeństwa w tej dziedzinie. Projektowana regulacja ma też ułatwić przedsiębiorstwom konkurowanie na rynku unijnym przez wzajemne uznawanie certyfikatów opartych o programy unijne.

Projektowana ustawa może też dać niezbędny impuls do rozwoju rynku certyfikacji cyberbezpieczeństwa w Polsce, który może być zdolny do przyciągnięcia klientów z całej Europy Środkowo-Wschodniej.
Należy zaznaczyć, że w Europie Środkowo-Wschodniej wiele krajów nie dysponuje zdolnościami w zakresie certyfikacji, co oznacza, że tamtejsi producenci muszą certyfikować swoje produkty za granicą. W związku z tym rozwój tego rynku w Polsce może przyczynić się do przyciągnięcia klientów z sąsiednich krajów, co będzie stanowiło dodatkowy czynnik sprzyjający rozwojowi rynku certyfikacji, jak również zwiększy renomę kraju na arenie międzynarodowej. Ponadto, dzięki wprowadzeniu krajowych schematów certyfikacji cyberbezpieczeństwa, będzie możliwe wspieranie cyberbezpieczeństwa produktów w określonych obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Zapewni to zachętę dla producentów do zapewnienia cyberbezpieczeństwa produktów w danych obszarach.
Kontrolę w podmiotach należących do krajowego systemu certyfikacji cyberbezpieczeństwa będzie przeprowadzał organ nadzorczy, którym będzie minister właściwy do spraw informatyzacji, zwany dalej „ministrem". Minister będzie dysponował uprawnieniami do przeprowadzania kontroli u podmiotów krajowego systemu cyberbezpieczeństwa, do badania produktów ICT oraz uzyskiwania od tych podmiotów informacji związanych z certyfikowanymi produktami. Będzie również uczestniczył w pracach na forum Unii Europejskiej z tym związanych, zwłaszcza w ramach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa. W zakresie certyfikatów odwołujących się do poziomu zaufania „wysoki" minister będzie posiadał uprawnienia do wyrażania zgody na wydanie certyfikatu. Projektowane rozwiązanie jest gwarantem, że ocena zgodności na najwyższym poziomie bezpieczeństwa będzie przeprowadzana zgodnie z najlepszymi standardami w tej dziedzinie.
Istotną rolę będzie odgrywało również Polskie Centrum Akredytacji, zwane dalej „PCA", które będzie nadzorowało akredytowane podmioty. Podstawą działania PCA w tym zakresie będzie rozdział 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179). Są to przepisy, na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania ze strony PCA. Jednostki oceniające zgodność będą mogły prowadzić ocenę zgodności i wydawać certyfikaty w ramach europejskich programów certyfikacji cyberbezpieczeństwa. Przyjęty model zakłada, że będą one mogły wydawać certyfikaty odnoszące się do wszystkich poziomów zaufania. Minister będzie wyrażał zgodę na wydanie certyfikatów odwołujących się do poziomu zaufania „wysoki". Takie rozwiązanie pozwoli na szeroki udział podmiotów prywatnych w procesie oceny zgodności, a równocześnie zagwarantuje prawidłowość procesów oceny zgodności na najwyższym poziomie uzasadnienia zaufania. Krajowe jednostki akredytacyjne będą pełnić podobną rolę w każdym państwie Unii Europejskiej.
Zgodnie z rozporządzeniem 2019/881 minister będzie wydawał decyzje, zezwalając na dokonywanie określonych czynności w ramach procesu oceny zgodności, jeśli określony program certyfikacji to przewiduje.
W projekcie wprowadzone zostały kary administracyjne za nierealizowanie określonych obowiązków, np. za nieprzekazanie ministrowi informacji w odpowiednim terminie. Prowadzone kontrole oraz nakładane kary zapewnią wysoki poziom certyfikowanych produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.
Projektowana ustawa pozwoli również tworzyć krajowe schematy certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Dzięki temu administracja państwowa będzie mogła promować standardy w obszarach nieobjętych europejskimi programami certyfikacji.
Ponadto krajowe schematy certyfikacji cyberbezpieczeństwa będą mogły dotyczyć również systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych. Dzięki temu przedsiębiorcy dostaną możliwość uzyskania certyfikatu na cały stosowany u siebie system zarządzania cyberbezpieczeństwem. Z kolei certyfikaty dla poszczególnych osób fizycznych pozwolą w sposób bezstronny potwierdzić posiadane kompetencje z zakresu cyberbezpieczeństwa oraz wyróżnić się na rynku. Są to szczególnie istotne kwestie, gdyż takie potwierdzenie kompetencji w obszarze cyberbezpieczeństwa pozwoli ich kontrahentom i potencjalnym pracodawcom łatwo określić ich kompetencje i zdecydować czy chcą z nimi współpracować.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Francja
W ramach Francuskiej Agencji Cyberbezpieczeństwa (The National Cybersecurity Agency of France, zwana dalej ANSSI) kwestiami certyfikacji zajmuje się Narodowe Centrum Certyfikacji. Agencja ta zajmuje się również licencjonowaniem laboratoriów w tym zakresie. ANSSI zostało również wyznaczone jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z aktem o cyberbezpieczeństwie.
Sama certyfikacja czy licencjonowanie nie podlega opłatom. Osoby wnioskujące ponoszą koszty badań laboratoryjnych ich produktów. Wynoszą one zwykle 600–700 euro na dzień, a sama certyfikacja trwa ok. 25–35 dni. Podmioty obsługiwane są w kolejności złożenia wniosków, co często powoduje, że zainteresowani muszą czekać na otrzymanie usługi. Certyfikacji można dokonać również u autoryzowanych podmiotów działających na wolnym rynku.
System francuski zasadniczo różni się od przyjętego w projektowanej ustawie. Wynika to przede wszystkim z uwarunkowań instytucjonalnych.
Niemcy

Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) wykonuje zadania niezwykle zbliżone do zadań wynikających z rozporządzenia 2019/881, jak również posiada zadania wykonywane w Polsce przez Agencję Bezpieczeństwa Wewnętrznego. BSI został również wyznaczony jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z ww. aktem. BSI przygotowuje również krajowe schematy certyfikacyjne, takie jak niemiecki szybki program certyfikacji.

Szwecja

Kwestiami certyfikacji w Szwecji zajmuje się jedna z agencji rządowych – Swedish Defence Materiel Administration. Pobierane są liczne opłaty. Sam wniosek o certyfikację podlega bezzwrotnej opłacie w wysokości 20 000 koron. Agencja ta zajmuje się również zamówieniami dla szwedzkich sił zbrojnych oraz rozwojem technologii na potrzeby wojska.

To sprzężenie kwestii cyberbezpieczeństwa w wymiarze cywilnym i wojskowym stanowi zasadniczą różnicę między polskim a szwedzkim systemem w tym zakresie.

Włochy

Przyjęty we Włoszech model certyfikacji oparty jest na działaniach organów administracji publicznej. Certyfikaty wydawane są przez odpowiednią komórkę w Ministerstwie Rozwoju Gospodarczego. W związku z tym ten rodzaj działalności organów administracji publicznej jest finansowany w całości z budżetu państwa. Równocześnie podmioty ubiegające się o certyfikat nie muszą wnosić opłat w związku z jego wydaniem.

Cypr

W celu wdrożenia aktu o cyberbezpieczeństwie powołany został nowy organ, który ma pełnić rolę krajowego organu ds. certyfikacji cyberbezpieczeństwa.

Niderlandy

W przyjętym w Niderlandach modelu organy państwa mają jedynie rolę nadzorczą, natomiast sama certyfikacja jest dokonywana przez prywatne podmioty. Ten model funkcjonował jeszcze przed implementacją przepisów rozporządzenia 2019/881, a Niderlandy są jednym z państw wiodących w obszarze certyfikacji cyberbezpieczeństwa. Organem państwa nadzorującym działalność certyfikacyjną jest jeden z ministrów. Jest to model bardzo zbliżony do przyjętego w projektowanej ustawie.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Pozytywne. Minister uzyska uprawnienia kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie też prowadził postępowania administracyjne w sprawach związanych z certyfikacją, np. będzie zatwierdzał certyfikaty odnoszące się do poziomu zaufania „wysoki”.
Przedsiębiorcy z branży IT	131 000	Informacja ogólnodostępna	Pozytywne. Uzyskają dostęp do certyfikatów obowiązujących w całej Unii Europejskiej. Przepisy ułatwią też rozwój własnych kompetencji w obszarze certyfikacji.
Polskie Centrum Akredytacji	1	Informacja ogólnodostępna	Pozytywne. PCA uzyska uprawnienia do prowadzenia akredytacji w nowym obszarze tematycznym.
NASK–PIB	1	Informacja ogólnodostępna	Pozytywne. Proponowane rozwiązania wiążą się z rozwijaniem zdolności certyfikacyjnych w Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym, dalej „NASK–PIB”, oraz innych usług z tym związanych. Obecnie jest to jedyna

			jednostka certyfikująca działająca w ramach metodologii Common Criteria.
Państwowe instytuty badawcze	30	Informacje ogólnodostępne	Pozytywne. Będą one realizować zadania związane z certyfikacją cyberbezpieczeństwa. Zadania te będą w wielu wypadkach realizowane odpłatnie lub ze środków ministra.
Naczelny Sąd Administracyjny	1	Informacje ogólnodostępne	Przyjęcie ustawy będzie wiązało się ze zwiększeniem spraw podlegających Naczelnemu Sądowi Administracyjnemu, co przełoży się na zwiększenie ilości spraw rozpatrywanych przez ten sąd.
Wojewódzkie Sądy Administracyjne	1	Informacje ogólnodostępne	Przyjęcie ustawy będzie wiązało się ze zwiększeniem spraw podlegających wojewódzkim sądom administracyjnym, co przełoży się na zwiększenie ilości spraw rozpatrywanych przez te sądy.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt został poddany opiniowaniu i konsultacjom publicznym, które rozpoczęły się w maju 2024 r. i trwały ok. 30 dni. Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535), projekt został udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

W trybie przepisów ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2025 r. poz. 440) oraz ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2025 r. poz. 423) projekt został skierowany do zaopiniowania przez następujące podmioty:

1) Business Centre Club – Związek Pracodawców;
2) Federację Przedsiębiorców Polskich;
3) Forum Związków Zawodowych;
4) Konfederację „Lewiatan”;
5) Niezależny Samorządny Związek Zawodowy „Solidarność”;
6) Ogólnopolskie Porozumienie Związków Zawodowych;
7) Pracodawców Rzeczypospolitej Polskiej;
8) Związek Przedsiębiorców i Pracodawców;
9) Związek Rzemiosła Polskiego.

W ramach konsultacji publicznych projekt został skierowany do następujących podmiotów:

1) Polskiej Izby Informatyki i Telekomunikacji;
2) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
3) Polskiej Izby Komunikacji Elektronicznej;
4) Krajowej Izby Gospodarczej;
5) Krajowej Izby Komunikacji Ethernetowej;
6) Krajowej Izby Gospodarki Cyfrowej;
7) Fundacji Bezpieczna Cyberprzestrzeń;
8) Polskiego Towarzystwa Informatycznego;
9) Związku Pracodawców Branży Internetowej IAB Polska;
10) Polskiej Rady Biznesu;
11) Naczelnej Organizacji Technicznej;
12) Związku Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;

13) Izby Gospodarki Elektronicznej;
14) Internet Society Poland;
15) Związku Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska";
16) Polskiego Centrum Badań i Certyfikacji S.A.;
17) Polskiej Organizacji Handlu i Dystrybucji;
18) Naczelnej Rady Zrzeszeń Handlu i Usług;
19) Polskiego Stowarzyszenia Marketingu SMB;
20) Amerykańskiej Izby Handlowej w Polsce;
21) Krajowej Izby Rozliczeniowej;
22) Fundacji Pułaskiego;
23) Sektorowej Rady ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
24) Green Rev Institute.

W ramach opiniowania projekt został skierowany do następujących podmiotów:
1) Prezesa Urzędu Komunikacji Elektronicznej;
2) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
3) Prezesa Urzędu Zamówień Publicznych;
4) Prezesa Urzędu Ochrony Danych Osobowych;
5) Prezesa Głównego Urzędu Statystycznego;
6) Rzecznika Małych i Średnich Przedsiębiorców;
7) Rzecznika Praw Obywatelskich;
8) Krajowej Rady Radiofonii i Telewizji;
9) Polskiego Komitetu Normalizacyjnego;
10) Najwyższej Izby Kontroli;
11) Agencji Bezpieczeństwa Wewnętrznego;
12) Agencji Wywiadu;
13) Biura Bezpieczeństwa Narodowego;
14) Centralnego Biura Antykorupcyjnego;
15) Służby Kontrwywiadu Wojskowego;
16) Służby Wywiadu Wojskowego;
17) Rządowego Centrum Bezpieczeństwa;
18) Służby Ochrony Państwa;
19) Polskiego Centrum Akredytacji;
20) Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego;
21) Instytutu Łączności – Państwowego Instytutu Badawczego;
22) Rady Dialogu Społecznego;
23) Prezesa Prokuratorii Generalnej Rzeczypospolitej Polskiej.

Projekt nie wymagał zaopiniowania przez Radę ds. Cyfryzacji, gdyż nie dotyczy kwestii informatyzacji podmiotów realizujących zadania publiczne, ani też do wykorzystywanych przez nie systemów informacyjnych czy rejestrów publicznych.
Projekt nie wymagał zaopiniowania przez Radę Działalności Pożytku Publicznego, gdyż nie dotyczy funkcjonowania organizacji pozarządowych oraz działalności pożytku publicznego oraz wolontariatu.
Projekt nie wymagał zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego, gdyż nie dotyczy problematyki samorządu terytorialnego, w tym także kwestii określających relacje pomiędzy samorządem terytorialnym, a innymi organami administracji publicznej.

Szczegółowe omówienie konsultacji publicznych i opiniowania przedstawione zostało w raporcie z konsultacji oraz w jego załącznikach.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	0,14	0,15	0,15	0,16	0,17	0,18	0,19	0,2	0,21	0,22	0,23	2
budżet państwa												
JST												

Fundusz Cyberbezpieczeństwa	0,14	0,15	0,15	0,16	0,17	0,18	0,19	0,2	0,21	0,22	0,23	2
Wydatki ogółem	10,02	11,91	12,20	12,52	12,84	13,17	13,51	13,85	14,21	14,58	14,94	143,74
budżet państwa	9,72	11,60	11,88	12,19	12,50	12,82	13,15	13,49	13,84	14,20	14,56	139,94
JST												
pozostałe jednostki (oddzielnie)												
Polskie Centrum Akredytacji	0,3	0,31	0,32	0,33	0,34	0,35	0,36	0,36	0,37	0,38	0,38	3,8
Saldo ogółem	-9,88	-11,76	-12,05	-12,36	-12,67	-12,99	-13,32	-13,65	-14	-14,36	-14,71	-141,74
budżet państwa	-9,72	-11,60	-11,88	-12,19	-12,50	-12,82	-13,15	-13,49	-13,84	-14,20	-14,56	-139,94
JST												
Polskie Centrum Akredytacji	-0,3	-0,31	-0,32	-0,33	-0,34	-0,35	-0,36	-0,36	-0,37	-0,38	-0,38	-3,8
Fundusz Cyberbezpieczeństwa	0,14	0,15	0,15	0,16	0,17	0,18	0,19	0,2	0,21	0,22	0,23	2

Źródła finansowania	Wydatki będą dokonywane z budżetu państwa w części 27 – Informatyzacja. W związku z nowymi zadaniami konieczne będzie podwyższenie limitu wydatków z tej części. Wszystkie koszty w tabelach podano z dokładnością do dwóch miejsc po przecinku. Przyjęcie ustawy nie będzie podstawą do planowania i ubiegania się o dodatkowe środki z budżetu państwa w roku wejścia w życie ustawy oraz w latach kolejnych przez Naczelny Sąd Administracyjny.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Utworzenie wydziału krajowego systemu certyfikacji cyberbezpieczeństwa** W ramach przyjęcia nowych zadań w zakresie certyfikacji cyberbezpieczeństwa przez ministra konieczne jest wzmocnienie urzędu obsługującego ten organ. Pierwszy europejski program certyfikacji (EUCC) jest stosowany od 31 stycznia 2025 r., co oznacza, że pojawi się konieczność przeprowadzenia czynności administracyjnych przez krajowy organ ds. certyfikacji cyberbezpieczeństwa. Szacuje się, że będzie to jedno postępowanie w 2025 r. Z samego tego programu w 2026 r. i w kolejnych latach będzie prowadzonych około 5 czy 6 postępowań administracyjnych w ciągu roku. Obecnie trwają również prace nad kolejnymi europejskimi programami certyfikacji, z których pierwszym jest europejski program certyfikacji usług chmurowych. Przewiduje się, że wejdzie on w życie w 2026 r., co będzie wiązało się z dodatkowymi postępowaniami administracyjnymi – 1 w 2026 r. oraz 5–6 rocznie w latach kolejnych. Równocześnie od 2026 r. powstanie też konieczność przeprowadzania kontroli wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Zgodnie z art. 25 ust. 3 aktu implementującego EUCC[1)], krajowy organ ds. certyfikacji cyberbezpieczeństwa, we współpracy z innymi organami nadzoru rynku, corocznie poddaje kontroli wyrywkowej co najmniej 4% certyfikatów EUCC. W związku z tym wraz ze wzrostem liczby wydanych certyfikatów będzie szybko rosła liczba obowiązkowych kontroli, jakie będzie musiał przeprowadzać ten organ. Szacuje się, że będzie to: – w 2026 r. – 1 kontrola, – w 2027 r. – 4 kontrole, – od 2028 r. – 8 kontroli rocznie. Wraz z wejściem w życie każdego kolejnego programu certyfikacji cyberbezpieczeństwa będzie pojawiała się konieczność prowadzenia dodatkowych kontroli, co będzie stanowiło znaczne obciążenie dla pracy krajowego organu ds. certyfikacji cyberbezpieczeństwa. W związku z tym w celu sprawnego wykonywania nowych zadań konieczne będzie utworzenie nowego wydziału i zatrudnienie pracowników od 2026 r. Pracownicy tworzonego wydziału będą zajmować się przede wszystkim prowadzeniem postępowań administracyjnych, analizą rynku i przeprowadzaniem postępowań kontrolnych. Konieczne jest wyasygnowanie środków na stanowiska naczelnika wydziału oraz 2 głównych specjalistów. Do zadań tych osób będzie również należało uczestniczenie w posiedzeniach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa oraz w grupach roboczych związanych z certyfikacją, współpraca z podmiotami międzynarodowymi i krajowymi funkcjonującymi w tym obszarze oraz udział

[1)] Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz. Urz. UE L 2024/482 z 07.02.2024, późn. zm.).

w pracach nad kolejnymi europejskimi programami certyfikacji cyberbezpieczeństwa. Należy podkreślić, że zadania te będą wiązały się z koniecznością posiadania kompetencji nie tylko w obszarze postępowań administracyjnych i kontrolnych, ale również z zakresu cyberbezpieczeństwa. Ze względu na międzynarodowy charakter systemu certyfikacji niezbędna będzie też bardzo dobra znajomość języka angielskiego. Zadania te nie mogą być wykonane przy wykorzystaniu obecnych pracowników urzędu obsługującego ministra.

Z tego względu nałożenie na Ministra Cyfryzacji dodatkowych zadań powoduje konieczność zabezpieczenia dodatkowych środków na wynagrodzenia osobowe wraz z pochodnymi.

Od 2027 r. będzie również wypłacane dodatkowe wynagrodzenie roczne w kwocie 33,22 tys. zł. W związku z tym całkowita kwota na rok wzrośnie do 0,432 mln zł.

Przy wyliczeniach przyjęto mnożnik kwoty bazowej w wysokości:

- 3,2 dla głównych specjalistów,
- 4,0 dla naczelnika wydziału.

Wyliczenie uwzględnia wytyczne dotyczące wskaźników makroekonomicznych wydawane przez Ministra Finansów.

Koszty wynagrodzeń 3 stanowisk w mln zł										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,00	0,40	0,43	0,44	0,45	0,47	0,48	0,49	0,50	0,51	0,53

Koszty organizacji stanowisk pracy

Koszty organizacji stanowisk pracy dla wskazanych wyżej 3 osób wyniosą w 2026 r. łącznie 36 tys. zł. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja.

Koszty organizacji stanowisk pracy										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,00	0,04	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00

Koszt badań

Jednym z obowiązków ministra będzie przeprowadzanie badań produktów, które otrzymały certyfikaty cyberbezpieczeństwa. Będzie się to wiązało z koniecznością zakupu usług zewnętrznych, w szczególności usług wyspecjalizowanych laboratoriów. Zgodnie z art. 25 ust. 3 aktu implementującego EUCC krajowy organ ds. certyfikacji cyberbezpieczeństwa, we współpracy z innymi organami nadzoru rynku, corocznie poddaje kontroli wyrywkowej co najmniej 4% certyfikatów EUCC. Należy spodziewać się, że kolejne programy będą zawierały analogiczne postanowienia. Przewiduje się, że koszty takich badań wyniosą 315 tys. zł w 2025 r., a w kolejnych latach kwota będzie zwiększać się o 5% w każdym kolejnym roku. Przy określaniu założonych środków przyjęto, że koszt badań będzie wynosił ok. 1/4 kosztu przeprowadzenia oceny zgodności danego produktu. W przypadku Common Criteria taki średni koszt wynosi ok. 300 tys. zł. W związku z tym przyjęta kwota umożliwi przeprowadzenie badań czterech produktów. W przypadku poziomu zaufania „wysoki" taka kwota wystarczy na 1 albo 2 badania. Łącznie w latach 2025–2035 koszty wyniosą ok. 4,48 mln zł. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja. Badania te będą prowadzone w ramach kontroli prowadzonych przez ministra u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Koszty badań produktów ICT										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,32	0,33	0,35	0,37	0,38	0,40	0,42	0,44	0,47	0,49	0,51

Przygotowanie opinii na potrzeby realizacji zadań krajowego organu ds. certyfikacji cyberbezpieczeństwa

W celu wsparcia ministra w zakresie nadzoru nad krajowym systemem certyfikacji cyberbezpieczeństwa planuje się zlecanie przygotowania opinii zewnętrznych. Koszty opinii wyniosą ok. 30 tys. zł rocznie. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja. W ramach wskazanych kwot uwzględnione zostały wytyczne dotyczące wskaźników makroekonomicznych wydawane przez Ministra Finansów. Kwota ta uwzględnia również zakup norm technicznych niezbędnych do realizacji tego zadania.

Przygotowanie opinii										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,00	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,04	0,04

Wpływy z kar

Przewiduje się wpływy do Funduszu Cyberbezpieczeństwa z tytułu kar płaconych przez członków krajowego systemu certyfikacji cyberbezpieczeństwa.

Zgodnie z powyższym szacuje się, że dochody z kar pojawią się w 2025 r. w wysokości 147 543 zł. W związku ze wzrostem liczby wydawanych certyfikatów przewiduje się, że kwota ta będzie wzrastać o około 5% w każdym kolejnym roku. Ponadto w następnych latach powinny zostać przyjęte kolejne europejskie programy certyfikacyjne, co przełoży się na znaczny wzrost certyfikatów. W związku z tym w 2028 r. przyjęto dwukrotny wzrost wpływów z kar. Należy w tym miejscu zaznaczyć, że dane dotyczące kar pieniężnych to szacunki, a nie cele. Podkreślenia wymaga, że kary będą nakładane w drodze decyzji administracyjnej w następstwie naruszenia prawa, zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).

Wpływy z kar										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,14	0,15	0,15	0,16	0,17	0,18	0,19	0,2	0,21	0,22	0,23

Utworzenie zdolności do certyfikacji w ramach kolejnych europejskich programów certyfikacji

Koszty rozwoju zdolności do certyfikacji										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
9,40	10,80	11,07	11,35	11,63	11,92	12,22	12,52	12,84	13,16	13,49

Aby w pełni wykorzystać szanse jakie daje europejski system certyfikacji cyberbezpieczeństwa oraz zapewnić polskim konsumentom dostęp do certyfikowanych usług w tym obszarze, konieczne będzie zapewnienie możliwości przeprowadzenia certyfikacji w podmiotach publicznych, takich jak NASK–PIB. Należy podkreślić, że NASK–PIB prowadzi już działalność certyfikacyjną w ramach metodologii Common Criteria (projekt KSO3C), jednej z najstarszych i najbardziej skomplikowanych metodologii oceny bezpieczeństwa produktów ICT. W związku z powyższym te zdolności powinny być dalej rozwijane, tak aby przedsiębiorcy chcący certyfikować swoje produkty zawsze mieli możliwość dokonania tego w Polsce. Koszty na ten cel przewidziane zostały na podstawie doświadczeń z projektu KSO3C i uwzględniają m.in. koszt roboczogodzin związanych z dostosowaniem NASK–PIB do wymagań, nowego programu, zatrudnienie niezbędnych ekspertów oraz utrzymanie sprzętu niezbędnego do prowadzenia badań. Cały projekt KSO3C kosztował w sumie ok. 24 mln zł. W związku z tym za podstawę do dostosowania się jednostki certyfikującej i laboratoriów do nowych programów przewidziana została ok. 1/3 tej kwoty. W związku z tym w 2025 r. przewidziano na ten cel dodatkowe środki w wysokości 9,4 mln zł związane z wejściem w życie pierwszego europejskiego programu certyfikacji EUCC. W następnych latach przewiduje się wejście w życie kolejnych programów certyfikacyjnych, co będzie wiązało się z koniecznością rozwijania zdolności certyfikacyjnej w

nowych obszarach, w związku z tym przewiduje się na ten cel wydatki w wysokości 10,8 mln zł. Wydatki te będą związane każdorazowo z przygotowaniem odpowiedniego programu certyfikacji, uzyskaniem akredytacji PCA, pozyskaniem ekspertów posiadających wiedzę niezbędną do realizacji tych zadań, a także pozyskanie sprzętu potrzebnego do przeprowadzenia badań. Na razie żaden kolejny europejski program certyfikacji cyberbezpieczeństwa nie został przyjęty, w związku z czym trudno jest precyzyjnie ocenić jak wiele przygotowań będzie koniecznych do jego wprowadzenia. Dlatego podstawą dla przyjętej kwoty są doświadczenia z programu KSO3C. Jeśli prace te nie zostaną wykonane spowoduje to, że certyfikacja w ramach europejskich programów nie będzie możliwa w Polsce. Oznacza to, że polscy przedsiębiorcy chcący certyfikować swoje produkty będą musieli zwracać się do jednostek certyfikujących z innych krajów. W ramach tych kosztów wzmocnione zostaną wszystkie państwowe instytuty badawcze, których kompetencje są niezbędne dla zapewnienia efektywnego działania krajowego systemu cyberbezpieczeństwa. W szczególności wzmocnione zostaną NASK–PIB oraz Instytut Łączności – Państwowy Instytut Badawczy, które obecnie już wykonują zadania w obszarze certyfikacji cyberbezpieczeństwa. Równocześnie nie wyklucza się rozwijania tych zdolności również w innych instytutach. Nie jest wiadome, jakich jeszcze obszarów będą dotykały kolejne europejskie programy certyfikacji, w związku z czym nie można wykluczyć, że pojawi się program dotykający obszaru, w którym specjalizuje się inny instytut. W takim wypadku zasadnym będzie rozwijanie tego instytutu, a nie budowanie zdolności od początku w jednym z już wymienionych podmiotów. W szczególności środki te posłużą do wzmocnienia kadr w instytutach badawczych, tak aby stale dysponowały one ekspertami potrzebnymi do prowadzenia certyfikacji w tym obszarze. Należy zauważyć, że dotyczy to jednego z najbardziej konkurencyjnych obszarów gospodarki pod kątem płac. Zarobki konsultanta ds. cyberbezpieczeństwa mieszczą się w przedziale od 18 do 26 tys. zł[2)], a w przypadku certyfikacji konieczne jest pozyskanie osób mających szczególnie duże kompetencje i wiedzę. Do przeprowadzenia procesu certyfikacji potrzebni są specjaliści, którzy dysponują znaczną wiedzą techniczną, ale również wiedzą w zakresie metodologii badań oraz procesów certyfikacyjnych. Ich kompetencje są unikalne, w związku z czym pozyskanie i utrzymanie takich osób musi wiązać się z zapewnieniem im zarobków podobnych do rynkowych. W przeciwnym wypadku nie zostaną zrealizowane cele ustawy.
Budowa tych zdolności jest niezbędna dla realizacji celu ustawy, jakim jest stworzenie w pełni działającego systemu certyfikacji cyberbezpieczeństwa w Polsce. Znacząco utrudni to dostęp do certyfikowanych produktów i jednostek certyfikujących dla polskich przedsiębiorców. Ponadto środki te posłużą również na przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa. W ramach wskazanych kwot uwzględnione zostały wytyczne dotyczące wskaźników makroekonomicznych wydawane przez Ministra Finansów.

Polskie Centrum Akredytacji

Koszty działalności PCA w obszarze certyfikacji cyberbezpieczeństwa										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,3	0,31	0,32	0,33	0,34	0,35	0,36	0,36	0,37	0,38	0,38

Wejście w życie projektowanej ustawy związane jest z rozszerzeniem działalności akredytacyjnej o obszar wskazany w ustawie, a tym samym z koniecznością zwiększenia zatrudnienia w PCA w wymiarze jednego etatu od 2025 r. Osoba zatrudniona odpowiedzialna będzie za organizację prowadzenia procesu akredytacji podmiotów ubiegających się o uprawnienie do certyfikacji w ramach programów certyfikacji cyberbezpieczeństwa. Zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku Polskie Centrum Akredytacji prowadzi samodzielną gospodarkę finansową, a koszty działalności, w tym wynagrodzenia pracowników, są pokrywane z przychodów PCA. PCA nie otrzymuje środków z budżetu państwa. Zatrudnienie dodatkowej osoby wymagało będzie uwzględnienia w planie finansowym i zwiększenia wydatków w funduszu osobowym o 0,3 mln zł rocznie od 2025 r. Środki te przeznaczone będą na sfinansowanie dodatkowego etatu oraz na wynagrodzenia dla osób, które otrzymają dodatkowe zadania w projektowanym zakresie. Zwiększenie to musi być utrzymane w kolejnych latach, zwiększane o wskaźnik wzrostu płac i będzie sfinansowane w ramach samodzielnej gospodarki finansowej PCA. Do oszacowania wydatków wzięto pod uwagę średnie

[2)] https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-pensje-w-branzy-cyberbezpieczenstwa-ile-zarabiaja-specjalisci

	wynagrodzenie, jakiego oczekują kandydaci do pracy, z ostatniego okresu z uwzględnieniem kosztów pracodawcy.	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców, oraz na rodzinę, obywateli i gospodarstwa domowe

Skutki								
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0–10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							

W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Certyfikaty będą ważne na obszarze całej Unii Europejskiej, w związku z czym ich posiadanie ułatwi wejście na rynki innych państw europejskich. Ponadto certyfikaty będą brane pod uwagę przy zamówieniach publicznych zarówno dla poszczególnych państw członkowskich, jak i realizowanych przez samą Komisję Europejską. Przedsiębiorstwa posiadające certyfikaty uzyskają dodatkowo przewagę nad konkurencją. Obecnie coraz większa waga przykładana jest do cyberbezpieczeństwa produktów i usług. Szacuje się, że cyberataki kosztowały świat 8 bilionów USD w 2023 r.[3)] W związku z tym coraz więcej firm będzie szukało dla siebie rozwiązań sprawdzonych, które zagwarantują bezpieczeństwo ich danych. Dzięki wprowadzeniu certyfikacji osób przedsiębiorcy łatwiej uzyskają informacje o kompetencjach osób z zakresu cyberbezpieczeństwa, co ułatwi im pozyskiwanie wysoko wykwalifikowanych specjalistów.
	sektor mikro-, małych i średnich przedsiębiorstw	Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Certyfikaty będą ważne na obszarze całej Unii Europejskiej, w związku z czym ich posiadanie ułatwi wejście na rynki innych państw europejskich. Ponadto certyfikaty będą brane pod uwagę przy zamówieniach publicznych zarówno dla poszczególnych państw członkowskich jak i realizowanych przez samą Komisję Europejską. Przedsiębiorstwa posiadające certyfikaty uzyskają dodatkowo przewagę nad konkurencją. Obecnie coraz większa waga przykładana jest do cyberbezpieczeństwa produktów i usług. Szacuje się, że cyberataki kosztowały świat 8 bilionów USD w 2023 r.[3)] W związku z tym coraz więcej firm będzie szukało dla siebie rozwiązań sprawdzonych, które zagwarantują bezpieczeństwo ich danych. Ponadto przepisy te umożliwią również certyfikację procesów ICT. Dzięki wprowadzeniu certyfikacji osób przedsiębiorcy łatwiej uzyskają informacje o kompetencjach osób z zakresu cyberbezpieczeństwa, co ułatwi im pozyskiwanie wysoko wykwalifikowanych specjalistów.
	rodzina, obywatele oraz gospodarstwa domowe	Wprowadzone przepisy zapewnią większą dostępność rozwiązań technicznych zapewniających bezpieczeństwo indywidualnym użytkownikom. Widoczne certyfikaty cyberbezpieczeństwa będą również stanowić istotną pomoc dla konsumentów przy wyborze bezpiecznych produktów i usług. Ponadto przepisy te umożliwią również certyfikację procesów ICT. Dzięki wprowadzeniu certyfikacji osób przedsiębiorcy łatwiej uzyskają informacje o kompetencjach osób z zakresu cyberbezpieczeństwa, co ułatwi im pozyskiwanie wysoko wykwalifikowanych specjalistów.
Niemierzalne		

[3)] https://www.expressvpn.com/pl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Ze względu na przyjęcie dobrowolnego modelu certyfikacji procedowane przepisy nie spowodują zakłóceń konkurencyjności. Czas i koszt przeprowadzenia procesu certyfikacji zależą od przyjętego poziomu ewaluacji i dla: – 2 poziomu ewaluacji trwa 4–6 miesięcy i kosztuje ok. 200 tys. zł, – 3 poziomu ewaluacji trwa 6–9 miesięcy i kosztuje ok. 600 tys. zł, – 4 poziomu ewaluacji trwa 7–12 miesięcy i kosztuje ok. 900 tys. zł.

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz: Dobrowolny charakter certyfikacji sprawia, że nie dojdzie do zmiany obciążeń regulacyjnych spoczywających na przedsiębiorcach. Uczestnicy krajowego systemu certyfikacji cyberbezpieczeństwa będą musieli stosować przepisy niniejszej ustawy związane z kontrolą zarówno ze strony PCA, jak i ministra. PCA będzie przygotowywać programy akredytacji dla podmiotów zainteresowanych prowadzeniem oceny zgodności w ramach europejskich programów certyfikacji cyberbezpieczeństwa, a następnie będzie prowadzić proces akredytacji i nadzór nad akredytowanymi podmiotami. Uzyskanie akredytacji będzie miało charakter odpłatny i będzie odbywać się na warunkach rynkowych.
Minister będzie prowadził szereg postępowań administracyjnych, m.in. zezwalał na prowadzenie oceny zgodności w określonych przypadkach, wyrażał zgodę na wydanie certyfikatów odwołujących się do poziomu uzasadnienia zaufania „wysoki" oraz nakładał kary administracyjne. Ponadto będzie również prowadził postępowania kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.
Ponadto minister będzie wykonywał ciążące na wierzycielu obowiązki związane z postępowaniem egzekucyjnym, m.in. będzie wystawiał upomnienia i tytuły wykonawcze czy rozpatrywał zarzuty w sprawie egzekucji administracyjnej. Będą to kolejne obciążenia regulacyjne, które będą dotyczyły ministra.

9. Wpływ na rynek pracy

Sektor cyberbezpieczeństwa jest jednym z najbardziej dynamicznych sektorów gospodarki. Cyberprzestępstwa wskazywane są jako jedne z pięciu najistotniejszych zagrożeń dla firm obok m.in. katastrof naturalnych. Na tak szybko zmieniającym się rynku rola certyfikatów stanowiących dowód na odpowiedni poziom cyberbezpieczeństwa produktów będzie rosła. W związku z tym powstaną nowe miejsca pracy, m.in. w jednostkach certyfikujących czy laboratoriach badających te produkty i usługi. Ponadto krajowe certyfikaty cyberbezpieczeństwa wydawane dla osób ułatwią znacząco pozyskiwanie wysoko wykwalifikowanych specjalistów z dziedziny cyberbezpieczeństwa. Ich posiadacze będą mogli również łatwiej uzyskać zatrudnienie.
Jeśli osiągnięte zostaną cele projektowanej ustawy w zakresie rozwoju rynku prawdopodobne jest również powstanie nowych etatów w tym sektorze gospodarki.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☒ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozwiązania przyjęte w projektowanej ustawie powinny zapewnić impuls do rozwoju technologii w zakresie cyberbezpieczeństwa. Przyjęcie schematów certyfikacyjnych powinno przyczynić się do dalszego ujednolicenia standardów cyberbezpieczeństwa zarówno w sektorze prywatnym, jak i publicznym. Wejście w życie ustawy i zwiększenie poziomu cyberbezpieczeństwa w sektorze przedsiębiorstw może przyczynić się do zmniejszenia strat wynikających z działań cyberprzestępców. Ponadto wprowadzenie systemu certyfikacji cyberbezpieczeństwa może przyczynić się do zwiększenia dostępności tego typu usług dla sektora małych i średnich przedsiębiorstw. Przyjęte przepisy

	mogą stanowić również ważny bodziec do rozwoju technologii związanych z bezpieczeństwem w cyberprzestrzeni. Uznawalność certyfikatów na obszarze całej Unii Europejskiej będzie stanowiło zachętę do rozwoju rynku usług certyfikacyjnych w kraju. Certyfikaty będą również przydatne dla administracji publicznej przy dokonywaniu zakupów. Będą one mogły zostać wykorzystane w ramach oceny ofert pod kątem bezpieczeństwa w ramach zamówień publicznych. W związku z nowymi postępowaniami administracyjnymi, jakie wprowadza przedmiotowa ustawa, na wydawane w ich ramach decyzje będzie przysługiwała skarga do sądu administracyjnego. W związku z tym przyjęcie przedmiotowej ustawy będzie prowadziło do wzrostu liczby spraw rozpatrywanych przez te sądy. Z kolei sądy administracyjne będą rozpatrywać sprawy z zakresu kar administracyjnych, wydawanych w związku z naruszeniem przepisów ustawy i rozporządzenia 2019/881.

11. Planowane wykonanie przepisów aktu prawnego

Pierwszym krokiem jest stworzenie jednolitych procedur akredytacji i certyfikacji na potrzeby cyberbezpieczeństwa. Równocześnie utworzony zostanie organ nadzoru, który będzie monitorował rozwój rynku certyfikacji. Odpowiednie działania zostaną podjęte w Ministerstwie Cyfryzacji. Zatrudnione zostaną dodatkowe osoby, które będą prowadziły postępowania administracyjne oraz przeprowadzały kontrole, zgodnie z przepisami projektowanej ustawy. Działania te zostaną rozpoczęte w 2025 r. Zostaną również przygotowane rozporządzenia o krajowych schematach certyfikacji cyberbezpieczeństwa.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane zostaną następujące mierniki:
1) liczba akredytowanych jednostek oceniających zgodność;
2) liczba wydanych certyfikatów i wystawionych deklaracji zgodności.

13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Nie dotyczy.

RAPORT Z KONSULTACJI

dotyczący projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

Niniejszy raport został sporządzony na podstawie § 51 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806). Zawiera on podsumowanie konsultacji publicznych i opiniowania ww. projektu ustawy.

1. Omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania oraz informacje o okresie ich przeprowadzenia i terminie wyznaczonym do zajęcia stanowiska

Projekt został udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny, oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji.

W ramach konsultacji publicznych projekt (z terminem 30 dni na przedstawienie uwag) otrzymały następujące podmioty:

1) Polska Izba Informatyki i Telekomunikacji;
2) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
3) Polska Izba Komunikacji Elektronicznej;
4) Krajowa Izba Gospodarcza;
5) Krajowa Izba Komunikacji Ethernetowej;
6) Krajowa Izba Gospodarki Cyfrowej;
7) Fundacja Bezpieczna Cyberprzestrzeń;
8) Polskie Towarzystwo Informatyczne;
9) Związek Pracodawców Branży Internetowej IAB Polska;
10) Polska Rada Biznesu;
11) Naczelna Organizacja Techniczna;
12) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
13) Izba Gospodarki Elektronicznej;
14) Internet Society Poland;
15) Związek Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;
16) Polskie Centrum Badań i Certyfikacji S.A.;
17) Polska Organizacja Handlu i Dystrybucji;
18) Naczelna Rada Zrzeszeń Handlu i Usług;
19) Polskie Stowarzyszenie Marketingu SMB;
20) Amerykańska Izba Handlowa w Polsce;
21) Krajowa Izba Rozliczeniowa;
22) Fundacja Pułaskiego;
23) Sektorowa Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
24) Green Rev Institute.

W ramach opiniowania projekt (z terminem 30 dni na wyrażenie opinii) otrzymały następujące podmioty:

1) Prezes Urzędu Komunikacji Elektronicznej;
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów;

3) Prezes Urzędu Zamówień Publicznych;
4) Prezes Urzędu Ochrony Danych Osobowych;
5) Prezes Głównego Urzędu Statystycznego;
6) Rzecznik Małych i Średnich Przedsiębiorców;
7) Rzecznik Praw Obywatelskich;
8) Krajowa Rady Radiofonii i Telewizji;
9) Polski Komitet Normalizacyjny;
10) Najwyższa Izba Kontroli;
11) Agencja Bezpieczeństwa Wewnętrznego;
12) Agencja Wywiadu;
13) Biuro Bezpieczeństwa Narodowego;
14) Centralne Biuro Antykorupcyjne;
15) Służba Kontrwywiadu Wojskowego;
16) Służba Wywiadu Wojskowego;
17) Rządowe Centrum Bezpieczeństwa;
18) Służba Ochrony Państwa;
19) Polskie Centrum Akredytacji;
20) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;
21) Instytut Łączności – Państwowy Instytut Badawczy;
22) Rada Dialogu Społecznego;
23) Prezes Prokuratorii Generalnej Rzeczypospolitej Polskiej.

W trybie przepisów ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2025 r. poz. 440) oraz ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2025 r. poz. 423) projekt został skierowany (z terminem 30 dni na wyrażenie opinii) do następujących podmiotów:

1) Business Centre Club – Związku Pracodawców;
2) Federacji Przedsiębiorców Polskich;
3) Forum Związków Zawodowych;
4) Konfederacji Lewiatan;
5) Niezależnego Samorządnego Związku Zawodowego „Solidarność”;
6) Ogólnopolskiego Porozumienia Związków Zawodowych;
7) Pracodawców Rzeczypospolitej Polskiej;
8) Związku Przedsiębiorców i Pracodawców;
9) Związku Rzemiosła Polskiego.

Projekt nie wymagał zaopiniowania przez:

1) Radę do Spraw Cyfryzacji, gdyż nie dotyczy kwestii informatyzacji podmiotów realizujących zadania publiczne, ani też wykorzystywanych przez nie systemów informacyjnych czy rejestrów publicznych;
2) Radę Działalności Pożytku Publicznego, gdyż nie dotyczy funkcjonowania organizacji pozarządowych oraz działalności pożytku publicznego oraz wolontariatu;
3) Komisję Wspólną Rządu i Samorządu Terytorialnego, gdyż nie dotyczy problematyki samorządu terytorialnego, w tym także kwestii określających relacje pomiędzy samorządem terytorialnym a innymi organami administracji publicznej.

Konsultacje publiczne i opiniowanie projektu zostały przeprowadzone w okresie od dnia 21 maja 2024 r. do dnia 21 czerwca 2024 r.

W ramach konsultacji publicznych uwagi do projektu zgłosiły następujące podmioty:

1) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji;
2) ISSA Polska - Stowarzyszenie do spraw bezpieczeństwa systemów informacyjnych;
3) Pern S.A.;
4) Polska Federacja Producentów Żywności Związek Pracodawców;
5) Polska Izba Informatyki i Telekomunikacji;
6) Polskie Towarzystwo Informatyczne;
7) Polska Wytwórnia Papierów Wartościowych S.A.

W ramach opiniowania uwagi do projektu przedstawiły następujące podmioty:

1) Instytut Łączności – Państwowy Instytut Badawczy;
2) Krajowa Rada Radiofonii i Telewizji;
3) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;
4) Polskie Centrum Akredytacji;
5) Polski Komitet Normalizacyjny;
6) Prezes Urzędu Komunikacji Elektronicznej;
7) Prezes Urzędu Ochrony Danych Osobowych.

Omówienie uwag do projektu zostało przedstawione w załącznikach do niniejszego raportu z konsultacji. Załączniki zawierające stanowisko Ministra Cyfryzacji do przedstawionych uwag zostały udostępnione w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

2. Przedstawienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Projekt nie wymagał przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia.

3. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa, wraz ze wskazaniem kolejności dokonania zgłoszeń albo informację o ich braku

Nie dokonano zgłoszeń lobbingowych odnośnie ww. projektu.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

lp.	podmiot zgłaszający uwagę	jednostka redakcyjna	treść zgłoszonej uwagi	stanowisko Ministra Cyfryzacji
uwagi ogólne do projektu				
1.	**Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji**		Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji nie zgłasza konkretnych uwag na tym etapie, ponieważ jednoznaczna ocena projektu jest niemożliwa, gdyż jej praktyczna wartość zależy od rozporządzeń wykonawczych, które przesądzą o skuteczności certyfikacji. Niemniej jednak korzystając z uprzejmości Polskiej Izby Informatyki i Telekomunikacji, która udostępniła swoje stanowisko, wyraża poparcie dla wyrażonej tam ogólnej oceny obszaru związanego z procedowanym projektem.	**Uwaga przyjęta do wiadomości** Ministerstwo Cyfryzacji będzie kontynuowało rozwój obszaru certyfikacji w Polsce zarówno poprzez tworzenie krajowych programów certyfikacji cyberbezpieczeństwa, jak i umożliwienie stosowania przepisów europejskich w tym zakresie.
2.	**Polska Izba Informatyki i Telekomunikacji**		Projektowana ustawa dotyczy przede wszystkim ustanowienia odpowiedniego systemu instytucjonalnego i proceduralnego, który jest niezbędny dla wykonywania rozporządzenia 2019/881 (CSA). Sama w sobie nie zawiera określenia, ani przyszłych obszarów, w jakich zostaną wprowadzone możliwe schematy cyberbezpieczeństwa, ani nie określa ich ram czy szczegółowych metod oceny. Na tym etapie ograniczamy się więc do przedstawienia naszej ogólnej oceny obszaru związanego z procedowanym projektem. W szczególności popieramy przyjęte założenie dobrowolności udziału w budowanym systemie certyfikacji. Z ogólnej perspektywy dostrzegamy bardzo istotną rolę rozwoju rynku certyfikacji w obszarze cyberbezpieczeństwa. Budowa krajowego potencjału w tym obszarze jest uzasadniona, szczególnie jeśli identyfikowany jest potencjał do tworzenia rozwiązań mających potencjał do szerokiego uznawania na poziomie europejskim i globalnym. Silna obecność w systemie certyfikacji powinna być w naszej opinii celem krajowej administracji i jako taka zasługuje na poparcie. Może być bowiem także akceleratorem do rozwoju przedsiębiorstw mogących korzystać z funkcjonowania w Polsce silnych, niezależnych i renomowanych laboratoriów. Uważamy to	**Uwaga uwzględniona** W ramach prac nad projektowaną ustawą uwzględnione są obecne i projektowane przepisy w obszarze cyberbezpieczeństwa, w szczególności dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022, str. 80). W zakresie utworzenia grup roboczych dotyczących poszczególnych krajowych programów certyfikacji minister właściwy do spraw informatyzacji może takie grupy utworzyć na podstawie ogólnych przepisów i nie jest konieczne dodatkowe uregulowanie tej kwestii w projektowanej ustawie.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			również za niezbędny element długoterminowego wzmacniania ogólnego poziomu odporności cyfrowej naszego kraju, na wypadek wszelkiego rodzaju kryzysów, w tym o charakterze geopolitycznym i militarnym. Zauważamy jednocześnie, że ustawa będzie wprowadzana w relatywnie trudnym okresie legislacyjnym, gdyż z jednej strony nie zostały jeszcze implementowane przepisy dyrektywy NIS2, a w niedługim horyzoncie spodziewamy się finalnego zatwierdzenia i publikacji rozporządzenia Cyber Resilience Act (CRA), które również będzie dotyczyło wprowadzania wymagań, w tym certyfikacyjnych. Tym samym postulujemy, aby w szczególności na poziomie prac koncepcyjnych związanych z rozwojem krajowego systemu certyfikacji uwzględniane były już teraz spodziewane w przyszłości zmiany przepisów. Za istotne uważamy również, aby ewentualne schematy certyfikacji były projektowane z uwzględnieniem przyszłego zakresu obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa i mogły wspierać jej implementację, a także prace dot. schematów certyfikacji prowadzone na poziomie europejskim. W każdym wypadku przyjmowane programy certyfikacji powinny uwzględniać potencjał komercyjnego wykorzystania uzyskiwanej certyfikacji. Skutecznego stosowania wymagać będą mechanizmy chroniące przed tworzeniem specyficznych schematów certyfikacji, które funkcjonowałyby specyficznie tylko w Polsce lub innych krajach, potencjalnie utrudniając wprowadzanie lub rozwój zasobów ICT dedykowanych na rynki międzynarodowe. Kluczowe dla stosowania ustawy będzie wydanie rozporządzeń na gruncie art. 6, który przewiduje fakultatywne upoważnienie do wydania krajowych programów certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT. W tym zakresie poddajemy pod rozwagę wprowadzenie także szczególnych procedur konsultacyjnych dotyczących stworzenia grup	

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			eksperckich z udziałem środowisk naukowych i reprezentacji przedsiębiorstw, których rolą będzie współpraca w zakresie określania kluczowych obszarów dla wprowadzenia schematów certyfikacji, jak i ich szczegółowego brzmienia. W tym zakresie CSA, w art. 49 ust. 3 i 4 wskazuje odpowiednio dla ENISA, obowiązek konsultacji i ustanowienia grupy roboczej dla każdej propozycji programu certyfikacji. Podobnie za zasadne uznajemy sporządzenie na poziomu krajowym kroczącego programu prac na rzecz certyfikacji na wzór art. 47 CSA. Nie widzimy powodów dla rezygnacji z przyjęcia podobnych rozwiązań na poziomie krajowym.	
3.	**Polska Federacja Producentów Żywności**		Nowelizacja ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa obejmuje nowe sektory gospodarki, w tym produkcję żywności, co może oznaczać, że więcej przedsiębiorstw będzie musiało spełniać wymogi dyrektywy, niezależnie od ich dotychczasowego doświadczenia w obszarze cyberbezpieczeństwa.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
4.	**Polska Federacja Producentów Żywności**		Sam fakt, że dyrektywa NIS2 uznaje producentów żywności za podmioty ważne, a nie kluczowe, sugeruje, że ich rola w kontekście cyberbezpieczeństwa jest istotna, ale nie na tyle krytyczna, aby wymagać najwyższego poziomu regulacji.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
5.	**Polska Federacja Producentów Żywności**		Polska, podobnie jak inne państwa członkowskie UE, może napotkać trudności z terminową transpozycją dyrektywy NIS2, co sugeruje potrzebę przyjęcia bardziej elastycznego podejścia do klasyfikacji podmiotów.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
6.	**Polska Federacja Producentów Żywności**		Nowe przepisy wprowadzają bardziej rygorystyczne wymogi dotyczące cyberbezpieczeństwa, co może oznaczać konieczność inwestycji w lepsze systemy zabezpieczeń i procedury zarządzania ryzykiem.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32).

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

				Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
7.	**Polska Federacja Producentów Żywności**		Nadmierne obciążenia regulacyjne mogą wpłynąć negatywnie na konkurencyjność polskich producentów żywności na rynku europejskim, gdzie inne kraje mogą przyjąć mniej restrykcyjne podejście do klasyfikacji podmiotów w swoich krajowych transpozycjach dyrektywy NIS2.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
8.	**Polska Federacja Producentów Żywności**		Sektor produkcji żywności jest bardzo zróżnicowany, a zastosowanie jednolitych, rygorystycznych wymogów dla wszystkich podmiotów może nie uwzględniać specyfiki poszczególnych przedsiębiorstw.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
9.	**Polska Federacja Producentów Żywności**		Przedsiębiorstwa będą musiały ponieść znaczne koszty związane z dostosowaniem się do nowych wymogów, co może być szczególnie obciążające dla nowych sektorów gospodarki objętych projektem ustawy, w tym producentów żywności.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
10.	**Polska Federacja Producentów Żywności**		Dyrektywa NIS2 dotyczy nie tylko producentów żywności, ale również firm należących do ich łańcuchów dostaw, co może komplikować współpracę i zwiększać koszty operacyjne.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
11.	**Polska Federacja Producentów Żywności**		Za niewywiązanie się z obowiązków wynikających z dyrektywy NIS2 mogą zostać nałożone wysokie kary finansowe, niekoniecznie realistyczne w odniesieniu do polskich przedsiębiorstw, co stanowi dodatkowe ryzyko finansowe.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

12.	**Polska Federacja Producentów Żywności**		Osoby fizyczne odpowiedzialne za przedsiębiorstwo mogą być pociągnięte do odpowiedzialności za niewywiązanie się z obowiązków, co zwiększa presję na zarządzających i może wpływać na decyzje biznesowe.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
13.	**Polska Federacja Producentów Żywności**		Głównym celem dyrektywy NIS2 jest zwiększenie bezpieczeństwa cyfrowego, co dla przedsiębiorstw produkujących żywność oznacza konieczność zmierzenia się z nowymi wyzwaniami i obciążeniami, które mogą i zapewne mocno wpłyną, na ich działalność gospodarczą. Istotne pozostaje, iż choć produkcja żywności jest ważna dla bezpieczeństwa społecznego i gospodarczego, powyższe argumenty wskazują, że nie musi być ona automatycznie uznawana za sektor kluczowy w kontekście wymogów NIS2, zwłaszcza jeśli dyrektywa unijna klasyfikuje te przedsiębiorstwa jako podmioty ważne, a nie kluczowe.	**Wyjaśnienie uwagi** Uwaga nie dotyczy projektowanej ustawy, tylko projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Wyjaśnienie uwagi zamieszczone zostanie w tabeli konsultacji publicznych do ww. ustawy.
14.	**PERN S.A.**		Pożądanym byłoby wskazanie podmiotu prowadzącego rejestr certyfikowanych usług, produktów oraz dostawców, najlepiej w sposób otwarty. Podmiot Kluczowy podczas wyboru produktu mógłby wskazywać oferentom miejsce, gdzie będą mogli sprawdzić czy dany produkt jest certyfikowany i możliwy do użycia u Operatora.	**Wyjaśnienie uwagi** W zakresie europejskich programów certyfikacji cyberbezpieczeństwa takie informacje będą publikowane na dedykowanej stronie internetowej Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa zgodnie z art. 50 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanym dalej „rozporządzeniem 2019/881”. W zakresie krajowych programów certyfikacji cyberbezpieczeństwa informacje o wydanych certyfikatach będą publicznie udostępniane za zgodą podmiotów będących właścicielami danych produktów ICT, usług ICT i procesów ICT.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

15.	**PERN S.A.**		Projekt systemu certyfikacji powinien zakładać możliwość elektronicznego zgłoszenia produktu, usługi lub dostawcy poprzez dedykowany system, np. S46. Składanie wniosków o certyfikowanie produktu usługi lub dostawcy powinno być realizowane bezpiecznym kanałem komunikacji, w przypadku gdy uzasadnienie nie będzie mogło być ogłoszone publicznie.	**Wyjaśnienie uwagi** Poddawanie produktów certyfikacji będzie dokonywane na podstawie umów między właścicielem produktu ICT, usługi ICT lub procesu ICT, a określoną jednostką oceniającą zgodność. W związku z tym ta kwestia nie będzie regulowana przepisami ustawy.
uwagi do poszczególnych przepisów projektu				
16.	**ISSA Polska**	**tytuł projektu**	UKSCC zlewa się nazwą z UKSC (ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa i ustawa o krajowym systemie cyberbezpieczeństwa).Tytuł ustawy wprowadza w błąd nazwą, sugerując, że dotyczy całego obszaru cyfrowego, a tak naprawdę dotyczy uszczegółowienia rozporządzenia UE 2019/881, mającego w nazwie obszar certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych – jest to zupełnie inna sfera. Dodatkowo nazwa projektu ustawy nie odzwierciedla treści projektu, która wypełniona jest ICT (i tylko tego dotyczy) – czyli nazwa wprowadza w błąd co do treści aktu, albo treść nie odnosi się do tytułu aktu. Należy dookreślić zakres ustawy w jej nazwie tak, aby odzwierciedlała akt prawa UE, do którego się odnosi. Proponujemy tytuł – ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.	**Uwaga nieuwzględniona** Krajowy system certyfikacji cyberbezpieczeństwa ma być uzupełnieniem krajowego systemu cyberbezpieczeństwa i nazwa celowo nawiązuje do tej ustawy. Te dwa akty prawne mają razem stanowić podstawę regulacji krajowych w zakresie cyberbezpieczeństwa. Nie można się też zgodzić, że tytuł nie odnosi się do treści aktu. Wskazuje on, że dotyczy certyfikacji w obszarze cyberbezpieczeństwa, a jest to obszar, w którym nie ma innych tego typu regulacji. Certyfikacja w zakresie technologii informacyjno-komunikacyjnych jest też częścią ogólnego zagadnienia certyfikacji w obszarze cyberbezpieczeństwa. Przyjęty tytuł pozwoli też na ewentualne rozszerzenie zakresu ustawy w przypadku podjęcia takiej decyzji.
17.	**Polskie Towarzystwo Informatyczne**	**art. 2 pkt 2 oraz uzasad-nienie**	Powołany zapis oznacza, iż dla potrzeb stosowania przepisów ustawy obowiązuje polskojęzyczna definicja „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami", zawarta w obowiązującej polskojęzycznej wersji rozporządzenia (UE) 2019/881 oraz definicja „cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie	**Uwaga uwzględniona** Uzasadnienie zostanie uzupełnione.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób" zawarta tamże. Propozycja zapisu Uzupełnić uzasadnienie do projektu ustawy o ocenę skutków obowiązywania różnych definicji stosowanych pojęć i terminów, w tym pojęcia – terminu „cyberbezpieczeństwo". Uzasadnienie W Polsce obowiązują dziś również inne definicje cyberbezpieczeństwa np.: (1) Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i niezaprzeczalność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy" – Art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie bezpieczeństwa. Oznacza to potrzebę ujednolicenia terminologii i definicji po wejściu w życie ustawy.	
18.	**Polskie Towarzystwo Informatyczne**	**art. 2 pkt 4, art. 9 ust. 2 pkt 9 i art. 12 ust. 2**	Definicja „dokumentu odzwierciedlającego stan wiedzy" nie pochodzi z rozporządzenia 2019/881, a rozporządzenia wdrożeniowego Komisji 2024/482 odnoszącego się WYŁĄCZNIE do schematu (programu) EUCC. W tym schemacie wskazano możliwość odstępstwa od zastosowania dokumentu 'state-of-the art' wraz z opisem szczegółowym okoliczności oraz trybu postępowania Jednakże wprowadzenie tego mechanizmu do ustawy w ogólności, bez kontekstu EUCC nie jest właściwe. Propozycja zapisu Prosimy o przywrócenie kontekstu pochodzenia tego pojęcia oraz uwzględnienie ograniczeń wskazanych w rozporządzeniu 2024/482. Uzasadnienie Tryb postępowania z wyjątkami stosowania konkretnych dokumentów 'state-of- the-art' w odniesieniu do EUCC jest	**Wyjaśnienie uwagi** Wskazany przepis ma służyć jedynie określeniu formy prawnej rozstrzygnięcia krajowego organu do spraw certyfikacji cyberbezpieczeństwa. Szczegółowe kwestie procedur związanych z takim odstąpieniem zawarte są w odpowiednich rozporządzeniach wykonawczych Komisji Europejskiej. Należy zauważyć, że przepisy rozporządzeń wykonawczych wprowadzających poszczególne europejskie programy certyfikacji cyberbezpieczeństwa są bezpośrednio stosowane, wobec czego nie można przepisywać ich postanowień do prawa krajowego. Ponadto nawet w przypadku, gdy nie są one bezpośrednio wskazane w ustawie, to nie zwalnia to państwa członkowskiego z ich stosowania. Dlatego też te przepisy będą miały zastosowanie.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			opisany w art. 15 ust. 2 rozporządzenia Komisji 2024/482 i tam m.in. wskazuje się konieczność uzyskania opinii ECCG i zastosowania jej w najwyższym możliwym stopniu. Zapis art. 9 ust.2 pkt 9 nie ma jakichkolwiek ograniczeń swobody krajowego organu w określeniu odstąpienia od wymagań określonych w dokumencie 'state-of- the-art.', stąd daje krajowemu organowi zbyt duże uprawnienia, które nie były przewidziane w Rozporządzeniu 2019/881.	
19.	**ISSA Polska**	**art. 2 pkt 4**	Definicja pojęcia „dokumentu odzwierciedlającego stan wiedzy" pochodzi z rozporządzenia wdrożeniowego Komisji 2024/482, które odnosi się wyłącznie do schematu EUCC. W tym schemacie przewidziano możliwość odstępstwa od stosowania dokumentu „state-of-the-art" wraz z opisem okoliczności oraz trybu postępowania. Niemniej jednak, wprowadzenie tego mechanizmu do ustawy bez kontekstu EUCC jest niewłaściwe. Tryb postępowania z wyjątkami stosowania konkretnych dokumentów „state-of-the-art" w odniesieniu do EUCC jest opisany w art. 15 ust. 2 rozporządzenia Komisji 2024/482. Zawiera on wymóg uzyskania opinii ECCG i uwzględnienia jej w jak największym stopniu. Przepis art. 9 ust. 2 pkt 9 nie ogranicza swobody krajowego organu w odstąpieniu od wymagań określonych w dokumencie „state-of-the-art", co daje krajowemu organowi zbyt duże uprawnienia, nieprzewidziane w rozporządzeniu 2019/881. Należy zmienić przepis w propozycji ustawy tak, aby odzwierciedlał zapisy obu wymienionych aktów prawa unijnego, tj. rozporządzenia Komisji 2024/482 oraz rozporządzenia 2019/881.	**Wyjaśnienie uwagi** Wskazany przepis ma służyć jedynie określeniu formy prawnej rozstrzygnięcia krajowego organu do spraw certyfikacji cyberbezpieczeństwa. Szczegółowe kwestie procedur związanych z takim odstąpieniem zawarte są w odpowiednich rozporządzeniach wykonawczych Komisji Europejskiej. Należy zauważyć, że przepisy rozporządzeń wykonawczych wprowadzających poszczególne europejskie programy certyfikacji cyberbezpieczeństwa są bezpośrednio stosowane, wobec czego nie można przepisywać ich postanowień do prawa krajowego. Ponadto nawet w przypadku, gdy nie są one bezpośrednio wskazane w ustawie, to nie zwalnia to państwa członkowskiego z ich stosowania. Dlatego też te przepisy będą miały zastosowanie.
20.	**ISSA Polska**	**art. 2 pkt 10**	Definicja krajowego programu certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 10 projektu ustawy, jest niekompletna. Nie odnosi się w całości do przepisów rozporządzenia 2019/881. Należy uwzględnić ograniczenia nałożone na krajowe programy w art. 57 rozporządzenia 2019/881.	**Wyjaśnienie uwagi** Definicja ta odwołuje się do bezpośrednio obowiązującej definicji z rozporządzenia 2019/881 i w związku z tym nie może być modyfikowana. Nie można też w przepisach prawa krajowego powtarzać bezpośrednio obowiązujących

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

				przepisów prawa Unii Europejskiej, jak np. art. 57 ww. rozporządzenia.
21.	**PERN S.A.**	**art. 2 pkt 12**	Art. 2 pkt 12 projektu definiuje proces ICT jako zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania oraz utrzymywania produktów lub usług ICT. Zgodnie z celem przedmiotowej ustawy, dany proces ICT powinien uzyskać certyfikat cyberbezpieczeństwa. Przepis nie precyzuje, że w odniesieniu do utrzymywania produktów, np. oprogramowania, chodzi o dostawcę zgodnie z definicją art. 2 pkt 5, a nie o użytkownika końcowego. Propozycja brzmienia przepisu: Art. 2 pkt 12: „12) Proces ICT – proces ICT nieobejmujący użytkowników końcowych produktów i usług ICT, o którym mowa w art. 2 pkt 14 rozporządzenia 2019/881”;	**Uwaga nieuwzględniona** Proces ICT został zdefiniowany w rozporządzeniu 2019/881 i w związku z tym jego definicja nie może być zmieniana w przepisach prawa krajowego.
22.	**Polskie Towarzystwo Informatyczne**	**art. 3 ust. 1**	„(..)ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT przez wprowadzenie procedur w zakresie certyfikacji (…)” Samo wprowadzenie procedur nie jest wystarczającym uzasadnieniem celu certyfikacji. Same procedury nie przyczynią się do poprawy jakości wytwarzania czegokolwiek. Propozycja zapisu: Sugeruje się wykorzystanie tekstu wskazanego w uzasadnieniu projektu ustawy oraz np. motywu (75) rozporządzenia 2019/881: „Celem europejskich programów certyfikacji cyberbezpieczeństwa powinno być zapewnienie, by produkty ICT, usługi ICT i procesy ICT certyfikowane zgodnie z takimi programami spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powigzanych funkcji bgdź usług oferowanych lub	**Uwaga uwzględniona** Zmodyfikowano art. 3 ust. 1.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia" Redakcję przepisu pozostawiamy Autorom projektu Uzasadnienie: Cel polskiego krajowego systemu certyfikacji cyberbezpieczeństwa nie musi być tożsamy z celem europejskich programów cyberbezpieczeństwa. Powinien jedynie sprzyjać temu celowi i zapewniać optymalne warunki do tworzenia/współtworzenia dobrych krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.	
23.	**ISSA Polska**	**art. 3 ust. 1**	„(..)ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT przez wprowadzenie procedur w zakresie certyfikacji (..)" Wprowadzenie procedur nie jest wystarczającym uzasadnieniem celu certyfikacji, gdyż same procedury nie poprawią jakości wytwarzania. Dla określenia celu proponuje się skorzystanie z zapisu motywu (75) rozporządzenia 2019/881: „Celem europejskich programów certyfikacji cyberbezpieczeństwa powinno być zapewnienie, by produkty ICT, usługi ICT i procesy ICT certyfikowane zgodnie z takimi programami spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności danych oraz funkcji lub usług oferowanych przez te produkty, usługi i procesy w trakcie ich całego cyklu życia."	**Uwaga uwzględniona** Zmodyfikowano art. 3 ust. 1.
24.	**Polskie Towarzystwo Informatyczne**	**art. 3 ust. 2 lit. c**	„(..)prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa" definicja niepełna. CAB-y mogą realizować wyłącznie usługi certyfikacyjne, które są inną działalnością niż „ocena" (ewaluacja) albo realizować, i ewaluację, i certyfikację. Propozycja zapisu: Uzupełnić: prowadzące ocenę lub certyfikację (..) Uzasadnienie:	**Uwaga uwzględniona** Przepis otrzymał zaproponowane brzmienie.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			Zgodność z praktyką jednostek oceniających zgodność funkcjonujących na rynku.	
25.	**ISSA Polska**	**art. 3 ust. 2 lit. c**	„(..)prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa” Definicja jest niepełna, ponieważ CAB-y mogą realizować wyłącznie usługi certyfikacyjne lub zarówno ewaluację, jak i certyfikację. Należy uzupełnić konkretnie o co chodzi ustawodawcy.	**Uwaga uwzględniona** Uzupełniono przepis, tak aby odrębnie odnosił się do oceny i certyfikacji.
26.	**ISSA Polska**	**art. 4 ust. 1**	Sformułowanie „może być” rodzi uznaniowość. Rodzi to poważne wątpliwości interpretacyjne i możliwość nadużyć. Zmuszanie podmiotów do zawarcia umowy. Jest to niezgodne z zasadami prawa i swobody gospodarczej (a co jeśli podmiot nie chce? co w sytuacji, kiedy nie wpływa to korzystnie na jego biznes?). W przypadku prawa zamówień publicznych wszystko opiera się na najkorzystniejszej ofercie (raport kościuszki Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny str. 39 tab. 5). Taki zapis bez jasnych i wyznaczonych zasad oraz reguł, powoduje uznaniowość. Rodzi to też możliwość nadużyć i jest korupcjogenne, co jak wiadomo tworzy dodatkowe, negatywne koszty społeczne. Należy zwrócić uwagę, że ocena powinna być obligatoryjna dla wszystkich podmiotów, albo należy określić sytuacje, kiedy ocena taka powinna być przeprowadzana. Co zaś się tyczy umowy, należy określić jednoznacznie, czy ma to być umowa, czy jednak decyzja administracyjna. Jeżeli umowa, to należy wskazać warunki na jakich zawieranie takiej umowy się odbywa i jakie elementy ma ona zawierać.	**Wyjaśnienie uwagi** Sformułowanie „może być” wskazuje, że poddanie produktu ICT, usługi ICT lub procesu ICT ocenie zgodności jest dobrowolne. Natomiast odniesienie do umowy oznacza, że proces oceny zgodności realizowany jest na podstawie umowy zawieranej między producentem, a daną jednostką określającą zgodność. Ustawa nie wprowadza przymusowej oceny zgodności.
27.	**Polskie Towarzystwo Informatyczne**	**art. 4 ust. 2**	„2. Produkt ICT, usługa ICT lub proces ICT w ramach oceny zgodności, o której mowa w ust. 1, podlega ocenie zgodności z wymogami bezpieczeństwa, które odpowiadają jednemu z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881.” jest mylący. Poziomy uzasadnienia zaufania obejmują i wymagania bezpieczeństwa, i rygor,	**Uwaga uwzględniona** Brzmienie przepisu zmieniono zgodnie z propozycją.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			zakres oraz wnikliwość oceny. Aktualny zapis wskazuje jedynie odpowiedniość poziomu uzasadnienia zaufania do wymogów bezpieczeństwa. Propozycja zapisu: Sugeruje się modyfikację zapisu: „2. Ocena zgodności z wymaganiami bezpieczeństwa produktu ICT, usługi ICT lub procesu ICT ~~w ramach oceny zgodności~~ o-której mowa w ust. 1, ~~podlega ocenie zgodności z wymogami bezpieczeństwa, które odpowiadają~~ odnosi się do jednego z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881 Uzasadnienie: Zgodność z definicją poziomów uzasadnienia zaufania zawartej w rozporządzeniu 2019/881	
28.	**ISSA Polska**	**art. 4 ust. 2**	„Produkt ICT, usługa ICT lub proces ICT w ramach oceny zgodności, o której mowa w ust. 1, podlega ocenie zgodności z wymogami bezpieczeństwa, które odpowiadają jednemu z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881.” Zapis jest mylący, ponieważ poziomy uzasadnienia zaufania obejmują wymagania bezpieczeństwa, rygor, zakres oraz wnikliwość oceny. Obecny zapis sugeruje jedynie odpowiedniość poziomu uzasadnienia zaufania do wymogów bezpieczeństwa. Należy przepis rozszerzyć o brakujące w projekcie elementy, ponieważ poziomy uzasadnienia zaufania obejmują: wymagania bezpieczeństwa, rygor, zakres oraz wnikliwość oceny.	**Uwaga uwzględniona** Zmieniono brzmienie art. 4 ust. 2.
29.	**ISSA Polska**	**art. 6**	Zamiast „może” winno być „powinien”. Z jednej strony w przypadku nie wydania rozporządzenia wymagania nie będą respektowane po wejściu w życie ustawy. Istnieje ryzyko, że bez rozporządzenia wykonawczego do ustawy będzie jak – przykład: art. 616a ustawy o obronie ojczyzny – ustawa	**Uwaga nieuwzględniona** Rozporządzenie ustanawiające krajowe programy certyfikacji nie jest niezbędne do stosowania przepisów ustawy. Należy przypomnieć, że niniejsza ustawa służy stosowaniu rozporządzenia UE 2019/881 i tworzy ramy dla certyfikacji produktów w ramach europejskich programów certyfikacji

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			zabrania fotografowania infrastruktury krytycznej, lecz bez prawidłowego oznakowania wg wzorów wydanych w rozporządzeniu (którego nie ma) dalej można utrwalać wizerunek IK. Wniosek – bez wydania rozporządzenia wykonawczego do ustawy będzie podobnie jak w podanym przykładzie. Z drugiej strony powinno być określone, kiedy minister właściwy do spraw informatyzacji ma się tematem zajmować, a kiedy nie. Minister właściwy do spraw informatyzacji nie powinien podejmować czynności bez konkretnej przyczyny, powodu (podstawą nie może być sformułowanie: bo mi się chce). Taka decyzja jest uznaniowa, bez jasnych i wyznaczonych zasad oraz reguł. Powoduje to możliwość zaistnienia dodatkowych, nieprzewidzianych kosztów. Rodzi to też możliwość nadużyć i jest korupcjogenne, co jak wiadomo tworzy dodatkowe, negatywne koszty społeczne. Proponujemy w związku z powyższym, że minister właściwy do spraw informatyzacji powinien być zobligowany do wydania rozporządzenia w określonym terminie.	cyberbezpieczeństwa. Do realizacji tego celu nie jest konieczne wydanie dodatkowych rozporządzeń. Nie można też mówić o rodzeniu dodatkowych kosztów czy korupcjogenności takiej decyzji, ponieważ certyfikacja jest dobrowolna.
30.	**ISSA Polska**	**art. 6 pkt 1**	Nie ma potrzeby określania wymogów w tym punkcie, ponieważ wymogi są określone w art. 52 Rozporządzenia UE 2019/881 do którego odnosi się projekt ustawy. Przepis nie odnosi się do odpowiednich norm referencyjnych – zob. art. 54(1) lit. C rozporządzenia 2019/881. Dodatkowo według zapisu w projekcie ustawy brak jest uzasadnienia decyzji, brak określenia reguł objęcia urządzeń. Również nie jest jasne, czy mowa o klasie rozwiązań, czy też o konkretnym produkcie konkretnej firmy. Nie wiadomo, czy chodzi o produkt czy usługę ogólnie (rodzaj), czy o konkretny produkt, czy konkretną usługę. Powinno być to jasno określone, bo wtedy jest konkurencyjne dla wszystkich (takich samych podmiotów na rynku). Ścieżki odwoławczej brak – badanie w procesie administracyjnym jest tylko formalne, a nie	**Wyjaśnienie uwagi** Przepis ten nie służy stosowaniu rozporządzenia 2019/881 lecz wprowadza nową instytucję prawa krajowego, jaką będą krajowe programy certyfikacji cyberbezpieczeństwa. Z kolei art. 52 i 54 rozporządzenia 2019/881 odnoszą się tylko do europejskich programów cyberbezpieczeństwa i nie ma tu obowiązku stosowania tych przepisów.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			merytoryczne. Należy wykreślić ten punkt lub odnieść go do art. 52 rozp. UE.	
31.	**Polskie Towarzystwo Informatyczne**	**art. 6 pkt 1**	W przepisie nie ma związania z odpowiednimi normami referencyjnymi – zob. np. art. 54(1) lit c) rozporządzenia 2019/881, Propozycja zapisu: wymogi dla produktów ICT, usług ICT lub procesów ICT podlegających ocenie zgodności z odniesieniem do norm, zgodnie z art. 54(1) lit c rozporządzenia 2019/881; Uzasadnienie: Odniesienie do norm referencyjnych jest podstawą wiarygodności ocen zgodności – ich porównywalności i powtarzalności.	**Uwaga nieuwzględniona** Wymogi muszą być określone bezpośrednio w przepisach prawa, w związku z czym nie mogą zostać zastąpione odwołaniem do norm. Równocześnie możliwe będzie odwołanie do norm, w zgodzie z zasadami określonymi w ustawie z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483).
32.	**Polskie Towarzystwo Informatyczne**	**art. 6 pkt 2**	„szczegółowe metody stosowane w celu wykazania, że produkt ICT, usługa ICT lub proces ICT są zgodne z wymogami, o których mowa w pkt 1" – szczegółowość metody nie jest jej cechą charakterystyczną – kluczowe jest wskazanie metod znormalizowanych Propozycja zapisu: Szczegółowe, znormalizowane metody Uzasadnienie: Odniesienie do norm referencyjnych jest podstawą wiarygodności ocen zgodności ich porównywalności i powtarzalności.	**Uwaga nieuwzględniona** Wymogi muszą być określone bezpośrednio w przepisach prawa, w związku z czym nie mogą zostać zastąpione odwołaniem do norm. Równocześnie możliwe będzie odwołanie do norm, w zgodzie z zasadami określonymi w ustawie z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483).
33.	**ISSA Polska**	**art. 6 pkt 2**	„Szczegółowe metody stosowane w celu wykazania, że produkt ICT, usługa ICT lub proces ICT są zgodne z wymogami, o których mowa w pkt 1” Kluczowe jest wskazanie metod znormalizowanych, a nie szczegółowość metody.	**Uwaga nieuwzględniona** Wymogi muszą być określone bezpośrednio w przepisach prawa, w związku z czym nie mogą zostać zastąpione odwołaniem do norm. Równocześnie możliwe będzie odwołanie do norm, w zgodzie z zasadami określonymi w ustawie z dnia 12 września 2002 r. o normalizacji (Dz. U. z 2015 r. poz. 1483).

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

34.	**Polskie Towarzystwo Informatyczne**	**art. 6 pkt 5**	„5) dokumentację techniczną i sposób jej przechowywania," Zapis jest zbyt ogólny. Propozycja zapisu: Połączyć zapis pkt 7 z pkt 5: 5) dokumentację techniczną oraz inne istotne informacje związane z oceną zgodności z ~~i sposób ich przechowywa~~ uwzględnieniem warunków przetwarzania informacji z uwagi na zdefiniowaną wrażliwość informacji oraz okresu jej przechowywania i archiwizowania, a na końcu niszczenia. Uzasadnienie: Doprecyzowanie zapisu, co zostało uwzględnione chociażby w art. 43 rozporządzenia wdrożeniowego 2024/482 dot. EUCC	**Uwaga nieuwzględniona** W rozporządzeniu nie można nakładać obowiązku odnoszącego się do informacji nieokreślonych, nawet na poziomie ogólnym, w ustawie.
35.	**Polskie Towarzystwo Informatyczne**	**art. 7**	„Art. 7. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację w obszarze objętym jednym z europejskich albo krajowych programów certyfikacji cyberbezpieczeństwa". Zapis zbyt szeroki – mógłby prowadzić do błędnej interpretacji, że jak – przykładowo – CAB ma akredytacje na badania i testy zgodnie z Common Criteria, to mógłby również świadczyć usługi w programie dot. certyfikacji cyberbezpieczeństwa rozwiązań w chmurze. Propozycja zapisu: Art. 7. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację o zakresie odnoszącym się do danego ~~w obszarze objętym jednym z~~ europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa. Uzasadnienie: Powiązanie zakresu działalności CAB z zakresem akredytacji, jaki jednostka oceniająca zgodność faktycznie posiada.	**Uwaga uwzględniona** Brzmienie przepisu zmieniono zgodnie z propozycją.
36.	**Polskie Towarzystwo Informatyczne**	**art. 8 ust. 2**	„2. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854). Dokumenty odzwierciedlające stan wiedzy mogą mieć zastosowanie do akredytacji – tak jest w przypadku EUCC (zob. rozporządzenie	**Uwaga nieuwzględniona** Przedmiotowy przepis odnosi się jedynie do samego procesu akredytacji, a w zakresie wymagań mają zastosowanie też inne przepisy prawa powszechnie obowiązującego, np. załącznik do rozporządzenia 2019/881.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			wdrożeniowe 2024/482 Propozycja zapisu: 2. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854), z uwzględnieniem wskazanych dokumentów odzwierciedlających stan techniki, jeśli mają zastosowanie". Uzasadnienie: Specyfika cyberbezpieczeństwa wymaga uszczegółowienia lub rozszerzenia wymagań ogólnych dot. akredytacji CAB, zawartych w normach zharmonizowanych, jak to uczyniono już w wypadku EUCC.	
37.	**ISSA Polska**	**art. 8 ust. 2**	„Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854)." Dokumenty odzwierciedlające stan wiedzy mogą mieć zastosowanie do akredytacji, co przewiduje rozporządzenie wdrożeniowe 2024/482. Przepis art 8 ust 2 jest uregulowany gdzie indziej, a poprzez taki zapis wprowadza się chaos i niejasności interpretacyjne. Ustęp powinien zostać usunięty.	**Uwaga nieuwzględniona** Wskazany przepis jest niezbędny dla stosowania przepisów rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854 oraz z 2024 r. poz. 1089) do procesu akredytacji jednostek oceniających zgodność w obszarze certyfikacji. Nie ma merytorycznych przesłanek do odmiennego uregulowania tego procesu w związku z czym odwołanie do tamtych przepisów jest właściwą techniką legislacyjną służącą realizacji celu ustawy.
38.	**Polska Wytwórnia Papierów Wartościowych**	**art. 9 i art. 10**	Stosownie do treści art. 10 ust. 1, 3 i 5 państwowe instytuty badawcze nadzorowane przez ministra właściwego do spraw informatyzacji (dalej: minister), państwowe instytuty nie nadzorowane przez ministra, a także inne podmioty, wspierają ministra, w zakresie swoich kompetencji, w realizacji zadań, o których mowa w art. 9 ust. 2. Spółka zwraca uwagę, że zgodnie z treścią art. 9 ust. 2 pkt 1 i 2, do zadań ministra należy sprawowanie nadzoru nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa i przeprowadzanie kontroli, w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3 i 4. Państwowe instytuty badawcze oraz inne podmioty	**Uwaga nieuwzględniona** Przygotowane przepisy pozwolą uniknąć konfliktu interesów gwarantując ministrowi właściwemu do spraw informatyzacji swobodę w wyborze podmiotu dysponującego ekspercką wiedzą w danym obszarze. Należy tu zwrócić uwagę, w szczególności na ust. 5 pozwalający skorzystać z eksperckiej wiedzy każdego podmiotu dysponującego kompetencjami w danym obszarze. W związku z tym będzie możliwe zasięgnięcie opinii ekspertów, w przypadku których nie wystąpi konflikt interesów. Należy też podkreślić, że rola tych podmiotów w działaniach krajowego organu do spraw certyfikacji cyberbezpieczeństwa będzie jedynie pomocnicza,

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			wskazane w treści tego przepisu, mogą być, lub już obecnie są, jednocześnie, jednostkami oceniającymi zgodność, w rozumieniu art. 2 pkt 13 Rozporządzenia Parlamentu Europejskiego i Rady nr 765/2008 z dnia 9 lipca 2008 r. ustanawiającego wymagania w zakresie akredytacji i uchylającego rozporządzenie (EWG) nr 339/93. Wobec powyższego, na gruncie projektowanych przepisów, będzie dochodzić do sytuacji, w których jednostki oceniające zgodność będą, jednocześnie, tymi jednostkami (tj. w nomenklaturze przepisu, państwowymi instytutami badawczymi lub innymi podmiotami), przy pomocy których, minister będzie nadzorował rynek i przeprowadzał kontrolę uczestników rynku, w tym, jednostek oceniających zgodność. Istnieje więc ryzyko, że jednostki uczestniczące w rynku będą faktycznie (bo formalnie będą wspierać ministra) kontrolowały i nadzorowały siebie lub swoich konkurentów. Innymi słowy, w świetle tak sformułowanych przepisów, istnieje wysokie prawdopodobieństwo, że jednostki konkurujące na rynku, będą jednocześnie, faktycznie, wspierającymi ministra w wykonywaniu nadzoru nad rynkiem i będą miały wpływ na wynik kontroli, względem innych konkurujących na rynku jednostek. Projekt ustawy nie zawiera mechanizmu, który zapobiegałby tego typu zdarzeniom. W związku z tym, w projekcie ustawy, należy wyraźnie określić rozdział pomiędzy jednostkami oceniającymi zgodność, a państwowymi instytutami badawczymi i innymi podmiotami. Z przywołanych przepisów, powinno jednoznacznie wynikać, że w przypadku, gdy państwowy instytut badawczy lub inny podmiot wspiera ministra w realizacji zadań, o których mowa w art. 9 ust. 2, nie może on jednocześnie świadczyć usług związanych z oceną zgodności. Ponadto, projekt ustawy powinien zawierać regulacje dotyczące zasad wyboru państwowego instytutu badawczego i innego podmiotu, któremu minister chce zlecić wsparcie w realizacji zadań.	nie będą one podejmowały rozstrzygnięć. Nie można określić na tym poziomie zasad wyboru, gdyż będą one różne w przypadku różnych programów certyfikacji i zawartych w nich wymogach.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

39.	**ISSA Polska**	**art. 10**	Proponuje się rozszerzenie kompetencji instytutów badawczych o możliwość przedstawiania programów walki z zagrożeniami dla cyberbezpieczeństwa oraz rozpowszechniania wiedzy na temat obrony przed zagrożeniami w oparciu o europejskie i światowe badania. Należy również uwzględnić klasyfikację zagrożeń i nowe techniki wykrywania i obrony przed zagrożeniami oraz przygotowanie krajowych programów certyfikacji zgodnie z nowymi procedurami. Proponujemy zobligowanie ministra właściwego do spraw informatyzacji do reagowania na powyższe i wydawania odpowiedniego aktu wykonawczego do ustawy w formie rozporządzenia.	**Uwaga nieuwzględniona** Przedmiotem projektowanej ustawy jest certyfikacja cyberbezpieczeństwa oraz nadzór nad tym procesem. Wskazane w uwadze zagadnienia wychodzą poza jej zakres i w związku z tym nie powinny być przedmiotem niniejszej regulacji.
40.	**Instytut Technik Innowacyjnych E-mag**	**art. 10**	Propozycja zmiany: Proponujemy, aby art. 10 ustawy, wśród instytutów wspierających ministra, w zakresie swoich kompetencji, w realizacji zadań, o których mowa w art. 9 ust. 2 został uwzględniony Instytut Sieci Badawczej Łukasiewicz – Instytut Technik Innowacyjnych EMAG włącznie z możliwością uzyskania dotacji celowej z części budżetu państwa. Uzasadnienie: Sieć Badawcza Łukasiewicz – Instytut Technik Innowacyjnych EMAG (dalej jak Łukasiewicz – EMAG) ustanowiła w swoich strukturach laboratorium oceny bezpieczeństwa produktów teleinformatycznych ITSEF, posiadające akredytację Polskiego Centrum Akredytacji (PCA) nr AB 1781, które działa w ramach Centrum Badań i Certyfikacji Łukasiewicz – EMAG. Laboratorium ITSEF powstało w wyniku realizacji projektu badawczego, pt.: „Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C)” razem w konsorcjum z Instytutem Łączności-PIB oraz NASK-PIB. Projekt został sfinansowany przez Narodowe Centrum Badań i Rozwoju w ramach II programu „CyberSecIdent – Cyberbezpieczeństwo i	**Wyjaśnienie uwagi** Obecne art. 17 ust. 3 projektu przewiduje możliwość zlecania zadań i przekazywania dotacji celowych instytutom badawczym nienadzorowanym przez ministra właściwego do spraw informatyzacji za zgodą ministra nadzorującego dany instytut. W związku z tym nie ma konieczności wprowadzenia osobnego przepisu dotyczącego Instytutu Sieci Badawczej Łukasiewicz – Instytutu Technik Innowacyjnych EMAG.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			eTożsamość". Laboratorium oferuje usługi oceny bezpieczeństwa zgodnie z uznanym międzynarodowym standardem Common Criteria (ISO/IEC 15408) „Wspólne kryteria do oceny bezpieczeństwa technologii informatycznych" (ang. Common Criteria for Information Technology Security Evaluation), stosując metodykę oceny zabezpieczeń CEM (ang. Common Evaluation Methodology) opisaną w standardzie ISO/IEC 18045. Laboratorium ITSEF, w ramach akredytacji AB 1781, oferuje także usługi oceny bezpieczeństwa komponentów IACS oraz urządzeń przemysłowych zgodnie z międzynarodową normą IEC 62443-4-2. Norma ta określa wymagania techniczne bezpieczeństwa, które muszą być spełnione przez komponenty systemów przemysłowych. Łukasiewicz – EMAG posiada zatem niezbędne zaplecze, umiejętności i doświadczenie, aby pełnić funkcje wspierające ministra, ponieważ: 1. Brał udział w tworzeniu krajowego schemat oceny bezpieczeństwa KSO3C razem z instytutami IŁ-PIB i NASK-PIB i posiada odpowiednie kompetencje i doświadczenie. 2. Laboratorium ITSEF Łukasiewicz – EMAG dostarczył dowody z ocen pilotażowych produktów dla jednostki certyfikującej NASK w procesie autoryzowania polskiego programu oceny przez międzynarodowe porozumienia SOG-IS i CCRA. 3. Laboratorium ITSEF Łukasiewicz – EMAG jest umieszczone na liście laboratoriów autoryzowanych w porozumieniu SOG-IS i licencjonowanych w porozumieniu CCRA. 4. Laboratorium ITSEF Łukasiewicz – EMAG posiada licencję NASK na badania zgodnie z ISO/IEC 15408 na poziomach od EAL 1 do EAL 4.	

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			Laboratorium ITSEF Łukasiewicz – EMAG przygotowuje się we współpracy z NASK-PIB do uzyskania zgodności z europejskim programem certyfikacji EUCC.	
41.	**ISSA Polska**	**art. 10 ust. 1 pkt 3**	„3. Przeprowadzania badań produktów ICT;" Zakres przepisu jest zbyt wąski. Powinien obejmować także inne obszary, nie tylko produkty ICT. Należy dodać usługi ICT oraz procesy ICT.	**Uwaga uwzględniona** Dodano do przepisu usługi ICT i procesy ICT.
42.	**Polskie Towarzystwo Informatyczne**	**art. 10 ust. 1 pkt 3**	„3. przeprowadzania badań produktów ICT;" zakres tego przepisu jest zbyt wąski. Dlaczego tylko produktów ICT? dlaczego tylko badań? Propozycja zapisu: przeprowadzania badań lub testów produktów ICT, usług ICT lub procesów ICT" Uzasadnienie: Pokrycie możliwych potrzeb ministra właściwego do spraw informatyzacji w pełnym zakresie przedmiotu ustawy.	**Uwaga uwzględniona** Dodano do przepisu usługi ICT i procesy ICT.
43.	**Polskie Towarzystwo Informatyczne**	**art. 10 ust. 1 pkt 4**	„4. publikację specyfikacji technicznych, norm i standardów" Instytutu badawcze nie są uprawnione do publikowania norm – to wyłączne prawo krajowej jednostki normalizacyjnej w tym zakresie wynika z ustawy o normalizacji; dodatkowo, nie wiadomo, co w kontekście Ustawy oznacza termin „standard" Propozycja zapisu: Sugeruje się wykreślić przepis z projektu ustawy Uzasadnienie: Zakres stosowalności norm lub specyfikacji technicznych oraz sposobu ich używania określa rozporządzenie UE o normalizacji 2012/1025 i ono jest wystarczające; Ew. odniesienie do norm lub innych specyfikacji technicznych jest w zakresie uprawnienia ministra właściwego do spraw informatyzacji i już jest zawarte w przepisach art. 6 projektu ustawy	**Uwaga uwzględniona** Przedmiotowy przepis otrzymał brzmienie – „4) publikację wykazów specyfikacji technicznych, norm i standardów;", zgodnie z uwagą Polskiego Komitetu Normalizacyjnego.
44.	**ISSA Polska**	**art. 10 ust. 1 pkt 4**	„4. Publikację specyfikacji technicznych, norm i standardów" Instytuty badawcze nie mają prawa do publikowania norm, co jest wyłącznym prawem krajowej jednostki normalizacyjnej	**Uwaga uwzględniona** Przedmiotowy przepis otrzymał brzmienie – „4) publikację wykazów specyfikacji technicznych, norm

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			zgodnie z ustawą o normalizacji (w RP jest to Polski Komitet Normalizacyjny). Ponadto, termin „standard" nie jest precyzyjnie określony w kontekście ustawy. Należy usunąć punkt z projektu ustawy.	i standardów;", zgodnie z uwagą Polskiego Komitetu Normalizacyjnego.
45.	**Polskie Towarzystwo Informatyczne**	**art. 10 ust. 1 pkt 6**	„6. opracowanie i walidację procedur badawczych" – nie wiadomo, co Autor miał na myśli. Do „walidacji procedur" można odnieść działania wskazane w normie ISO 9001 (np. walidacja procesu) i definicję tam stosowaną. Z kolei, norma PN-EN 17025, która jest normą służącą do akredytacji laboratoriów badawczych i wzorcujących stosuje pojęcie „walidacji" w odniesieniu do metod badawczych (mówi się też o procedurze walidacji); jeśli Autor miał na myśli to drugie znaczenie, to mieści się ona w zapisie punktu 7. Propozycja zapisu: Sugeruje się skreślenie pkt 6 Uzasadnienie: Unikanie pojęć niezdefiniowanych „walidacja procedury badawczej", co może wprowadzić w błąd osoby wdrażające lub stosujące przepisy Ustawy	**Uwaga uwzględniona** Chodzi o walidację procesów badawczych. Brzmienie przepisu zostanie zmienione tak, aby nie powstawały wątpliwości w tym zakresie. Równocześnie, aby wyeliminować ewentualne wątpliwości co do zakresu działań jednostki, pkt 6 nie zostanie wykreślony. Przepis otrzymał brzmienie: „6) opracowanie i walidację procesów badawczych;".
46.	**ISSA Polska**	**art. 10 ust. 1 pkt 6**	„6. Opracowanie i walidację procedur badawczych" Niejasne jest, co autor miał na myśli przez „walidację procedur". Może to odnosić się do działań wskazanych w normie ISO 9001 lub do procedur walidacji metod badawczych zgodnie z normą PN-EN 17025. Należy dookreślić co ustawodawca ma na myśli, do czego ma odnosić się przepis.	**Uwaga uwzględniona** jw.
47.	**Polskie Towarzystwo Informatyczne**	**art. 10 ust. 4 pkt 1**	„1) utrzymanie stałej sprawności operacyjnej w zakresie opracowywania i walidacji procedur badawczych, metod i technik oceny oraz wytwarzania materiałów odniesienia;" – zapis kompletnie niezrozumiały oraz zbyt wąski. Niezrozumiałe jest, w jaki sposób państwowy instytut badawczy miałby tworzyć „materiał odniesienia"? Może Autor miał na myśli ew. organizację porównań	**Uwaga uwzględniona** Przepis otrzymał brzmienie „1) utrzymanie stałej sprawności operacyjnej w zakresie realizacji zadań, o których mowa w art. 16 ust. 2;".

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			międzylaboratoryjnych lub badaniach biegłości oraz – w wypadku jednostek certyfikujących – wzajemne oceny (peer assessment) (zob. PN-EN ISO/IEC 17025 oraz art. 54(1) lit u) rozporządzenia 2019/881, odpowiednio. Propozycja zapisu: Z uwagi na niepewność co do intencji Autora projektu, sugeruje się uogólnienie zapisu w następujący sposób: „utrzymanie stałej sprawności operacyjnej w zakresie realizacji zadań wskazanych w ust. 3". Można rozważyć dodanie w ust. 3 nowego punktu: „x) organizację porównań międzylaboratoryjnych lub badań biegłości lub wzajemnej oceny, w europejskim albo krajowym programie certyfikacji cyberbezpieczeństwa" Uzasadnienie: Zapewnienie zgodności między ust. 3 a 4, co do „operacyjnej gotowości".	
48.	**ISSA Polska**	**art. 10 ust. 2**	Koszty wrzucone w taryfę, odbiją się na wszystkich. Przenoszenie kosztów (bez podnoszenia podatków) – przełożenie kosztów na producenta, dostawcę, a ten przeniesie koszt na biorcę końcowego, podnosząc koszt swojego produktu, usługi. Wszyscy za to zapłacimy. Spowoduje to również brak konkurencyjności na rynku. Część rynku jest regulowana, a część komercyjna. Część komercyjna będzie miała problem. Ta część rynku poniesie niewspółmierne, nieadekwatne koszty, przez co jej produkty i usługi nie będą konkurencyjne. Spowoduje to nierówne traktowanie podmiotów na rynku.	**Wyjaśnienie uwagi** Art. 10 ust. 2 nie powoduje mechanizmu przenoszenia kosztów na podmioty prywatne. Finansowanie kwestii związanych z certyfikacją ze środków publicznych ma zapewnić ministrowi dostęp do specjalistycznej wiedzy potrzebnej do realizacji zadań nakładanych na niego niniejszą ustawą. Jest też powszechnie stosowane w krajach UE, np. Niemczech czy Francji.
49.	**ISSA Polska**	**art. 10 ust. 4 pkt 1**	Co to jest wytwarzanie materiałów odniesienia? – wymyślanie koła na nowo, ponieważ są już istniejące normy i standardy. Dodatkowo jakie kryteria oceny sprawności operacyjnej? Kto je stworzy? Kto będzie oceniał? Bez określenia tych fundamentalnych parametrów oraz reguł i zasad ich	**Uwaga uwzględniona** Zmieniono brzmienie art. 10 ust. 4 pkt 1. Przepis otrzymał brzmienie: „1) utrzymanie stałej sprawności operacyjnej w zakresie realizacji zadań, o których mowa w art. 16 ust. 2;".

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			stosowania pozwalamy na uznaniowość. Powoduje to możliwość zaistnienia dodatkowych, nieprzewidzianych kosztów oraz może powodować ich defraudację. Rodzi to też możliwość nadużyć i jest korupcjogenne, co jak wiadomo tworzy dodatkowe, negatywne koszty społeczne. Proponujemy w odniesieniu do powyższego zagadnienia stosowanie uznanych norm, standardów i metodyk.	
50.	**Polskie Towarzystwo Informatyczne**	**art. 10 ust. 5**	Błąd gramatyczny. W ust. 1 i 3 jest mowa o „państwowe instytuty badawcze” (liczba mnoga), a w ust. 5 jest mowa o „podmiocie” (liczba pojedyncza) Propozycja zapisu: Poprawić na liczbę mnogą („inne niż podmioty wskazane”) Uzasadnienie: Poprawka gramatyczna	**Uwaga uwzględniona** Wprowadzono stosowne zmiany.
51.	**ISSA Polska**	**art. 11**	Art. 11.1. Brakuje przepisu określającego relację „zezwolenia” do „akredytacji”. Akredytacja powinna być warunkiem koniecznym posiadania zezwolenia. 2. Brakuje określenia okresu ważności zezwolenia oraz warunków, w których status zezwolenia może się zmienić w zależności od akredytacji. Należy podkreślić (ująć), że zezwolenie ma być wydane w formie decyzji ministra właściwego do spraw informatyzacji.	**Uwaga uwzględniona** Uzupełniono art. 11 o powiązanie zezwolenia z akredytacją.
52.	**Polskie Towarzystwo Informatyczne**	**art. 11**	Brakuje przepisu określającego relację „zezwolenia" do „akredytacji". Akredytacja jest warunkiem koniecznym posiadania zezwolenia. Brakuje okresu ważności zezwolenia lub warunków, w których status zezwolenia zmienia się (zależność od akredytacji) Propozycja zapisu: Dodać nowe ustępy: „x) warunkiem koniecznym wydania lub wznowienia zezwolenia jest przedstawienie przez jednostkę oceniającą zgodność ważnego certyfikatu akredytacji o zakresie pokrywającym zakres europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa" y) zezwolenie jest ograniczane, zawieszane lub cofane	**Uwaga uwzględniona** jw.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			w wypadku analogicznych zmian w certyfikacie akredytacji lub na wniosek danej jednostki oceniającej zgodność" Uzasadnienie: Uzyskanie zgodności z przepisami określonymi w rozporządzeniu 2019/881.	
53.	**ISSA Polska**	**art. 11 ust. 7**	Art. 11 ust. 7 Zamiast „może" winno być „powinien". Powinno być określone, że minister właściwy do spraw informatyzacji ma zasięgać opinii. Minister właściwy do spraw informatyzacji nie powinien podejmować czynności bez konkretnej przyczyny, powodu (podstawą nie może być sformułowanie: bo mi się chce). Takie podejście jest uznaniowe, bez jasnych i wyznaczonych zasad oraz reguł. Brak opinii powoduje uznaniowość. Rodzi to też możliwość nadużyć i jest korupcjogenne, co jak wiadomo tworzy dodatkowe, negatywne koszty społeczne. Proponujemy zatem mając na względzie powyższe, że minister właściwy do spraw informatyzacji powinien być zobligowany do zasięgania opinii.	**Uwaga nieuwzględniona** Zasięgnięcie opinii zależy od okoliczności konkretnej sprawy i nie powinno odbywać się automatycznie. Należy zauważyć, że każde zasięgnięcie opinii przedłuża postępowanie i powoduje koszty po stronie podmiotu, do którego wystąpiono o opinię. Dlatego należy dokonywać tego tylko tam, gdzie okoliczności konkretnej sprawy tego wymagają.
54.	**Polskie Towarzystwo Informatyczne**	**art. 12 ust. 2**	Jak wskazano w rozporządzeniu wdrożeniowym Komisji 2024/482 (art. 15 ust. 2), uchylenie wymagań jest poparte uzyskaniem opinii ECCG oraz jej uwzględnieniem w jak największym stopniu. Propozycja zapisu: 2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na zrezygnowanie z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy w przypadku, gdy takie odstępstwo jest uzasadnione charakterem danego produktu ICT, usługi ICT lub procesu ICT oraz było poprzedzone zasięgnięciem opinii Europejskiej Grupy do spraw Certyfikacji Cyberbezpieczeństwa i jej uwzględnieniem w jak największym stopniu". Uzasadnienie: Zachowanie zasady oceny w odniesieniu do takich samych lub co najmniej równoważnych wymagań, co pozwala korzystać z	**Wyjaśnienie uwagi** Wskazany przepis ma służyć jedynie określeniu formy prawnej rozstrzygnięcia krajowego organu do spraw certyfikacji cyberbezpieczeństwa. Szczegółowe kwestie procedur związanych z takim odstąpieniem zawarte są w odpowiednich rozporządzeniach wykonawczych Komisji Europejskiej. Należy zauważyć, że przepisy rozporządzeń wykonawczych wprowadzających poszczególne europejskie programy certyfikacji cyberbezpieczeństwa są bezpośrednio stosowane, wobec czego nie można przepisywać ich postanowień do prawa krajowego. Ponadto nawet w przypadku, gdy nie są one bezpośrednio wskazane w ustawie, nie zwalnia państwa członkowskiego z ich stosowania. Dlatego też te przepisy będą miały zastosowanie.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			przywileju automatycznego uznawania certyfikatu wydanego w danym Kraju Członkowskim we wszystkich pozostałych Krajach UE oraz EOG. Odstępstwo może skutkować brakiem możliwości uznania certyfikatu jako zgodnego z danym europejskim programem certyfikacji cyberbezpieczeństwa.	
55.	**ISSA Polska**	**art. 12 ust. 2**	Art. 12 ust. 2. Zgodnie z rozporządzeniem wdrożeniowym Komisji 2024/482 (art. 15 ust. 2), uchylenie wymagań wymaga uzyskania opinii ECCG i uwzględnienia jej w jak największym stopniu. Należy uwzględnić powyższe w przepisie ustawy.	**Wyjaśnienie uwagi** jw.
56.	**Polskie Towarzystwo Informatyczne**	**art. 14**	Art. 14 określa model certyfikacji w wypadku zastosowania poziomu uzasadnienia zaufania „wysoki" w którym KAŻDY certyfikat jest zatwierdzany przez krajowy organ do spraw certyfikacji cyberbezpieczeństwa. Rozporządzenie 2019/881 w art. 56 ust. 6 przewiduje drugi model w postaci stałej delegacji „na podstawie ogólnego powierzenia przez krajowy organ do spraw certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność." Propozycja zapisu: Szczegółowe zapisy są w tej chwili niemożliwe do zaproponowania, ponieważ sugerujemy najpierw zastanowić się nad modelem, w którym krajowy organ przekazuje stałe powierzenie zarządzania certyfikatami wskazanej –akredytowanej i posiadającej zezwolenie do wydawania certyfikatów ocenianych na poziomie uzasadnienia zaufania „wysoki – jednostce certyfikującej. Uzasadnienie: Model stałego powierzenia jest wariantem bardziej korzystnym w wypadku krajowych organów, które się dopiero tworzą – przypadek Polski. Należy wskazać, że zarządzanie certyfikatami to nie tylko wydawanie i cofanie certyfikatu, ale też zawieszanie, odnawianie, zmiana zakresu certyfikatu. Jeśli jeszcze założyć,	**Uwaga nieuwzględniona** Model zatwierdzania certyfikatów przez krajowy organ jest modelem bardziej elastycznym i otwierającym dostęp do rynku. W przypadku zastosowania mechanizmu powierzenia możliwości wydawania certyfikatów odwołujących się do poziomu zaufania wysoki miałaby tylko jedna jednostka oceniająca zgodność. Projektodawca nie chce zawężać tego rynku i blokować podmiotom prywatnym możliwości rozwoju. Podobny model funkcjonuje obecnie w Niderlandach oraz Szwecji.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			że programów europejskich będzie więcej niż jeden, jak dziś (EUCC), to obciążenie administracyjne krajowego organu związane jedynie z zarządzaniem certyfikatami będzie przekraczało założoną wielkość komórki organizacyjnej w MC dedykowanej do roli krajowego organu.	
57.	**ISSA Polska**	**art. 14**	Art. 14 określa model certyfikacji dla poziomu uzasadnienia zaufania „wysoki", w którym każdy certyfikat jest zatwierdzany przez krajowy organ do spraw certyfikacji cyberbezpieczeństwa. Jednocześnie Rozporządzenie 2019/881 w art. 56 ust. 6 przewiduje także model stałej delegacji, w którym zadanie wydawania europejskich certyfikatów cyberbezpieczeństwa jest powierzone jednostce oceniającej zgodność. Należy uzupełnić o brakujące odniesienia do art. 56 ust. 6 rozp. UE.	**Wyjaśnienie uwagi** Projektodawca przyjął w ramach swobody pozostawionej przez rozporządzanie 2019/881 model zatwierdzania certyfikatów odwołujących się do poziomu zaufania „wysoki" przez krajowy organ do spraw certyfikacji. Jest to model elastyczny i otwarty na podmioty prywatne. W związku z tym nie ma potrzeby uzupełniania przepisów.
58.	**PWPW**	**art. 14**	a) w art. 14 ust. 1 użyto zwrotu „poziom zaufania wysoki". Należy zwrócić uwagę, że normatywnie funkcjonuje wyrażenie „poziom uzasadnienia zaufania wysoki". Posługuje się nim rozporządzenie 2019/881 i pojawia się ono w treści art. 9 ust. 2, b) w art. 14 ust. 1 użyto odesłania do art. 57 ust. 2 rozporządzenia 2019/881, w kontekście odwołania się do poziomu zaufania wysoki. Ww. przepis nie zawiera zapisów dotyczących tego poziomu zaufania. Najprawdopodobniej doszło do omyłki pisarskiej i chodzi o art. 52 ust. 7 rozporządzenia 2019/881.	**Uwaga uwzględniona** Poprawki zostały wprowadzone.
59.	**ISSA Polska**	**art. 14 ust. 2**	Art. 14 ust. 2 brak możliwości wystąpienia o sprawdzenie w innym laboratorium. Należy uzupełnić o taką możliwość (np. gdy badanie było nierzetelne).	**Wyjaśnienie uwagi** Taka możliwość została zapewniona poprzez odwołanie do art. 11 ust. 7 przewidujący możliwość zasięgnięcia opinii innych podmiotów o przeprowadzonym procesie.
60.	**PWPW**	**art. 14 ust. 2**	Stosownie do treści art. 14 ust. 2, minister zatwierdza, odmawia zatwierdzenia oraz cofa europejski certyfikat. Powyższe, czyni w drodze decyzji (ust. 6). Jednocześnie projekt ustawy nie wskazuje terminu wydania takiej decyzji.	**Wyjaśnienie uwagi** Wszystkie postępowania będą prowadzone na podstawie działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			Należy rozumieć, że w tych sytuacjach zastosowanie będą miały ogólne terminy, o których mowa w Rozdziale 7 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (dalej: KPA). Zasadne jest wskazanie, że decyzja o zatwierdzeniu, odmowie lub cofnięciu ww. certyfikatu ma bardzo duże znaczenie dla podmiotu, który oczekuje jej wydania. Może ona mieć charakter rozstrzygnięcia o istotnym znaczeniu gospodarczym dla tego podmiotu, wpływającym na stabilność prowadzonej przez ten podmiot działalności gospodarczej. Należy też pamiętać, że taka decyzja dotyczy produktu, usługi albo procesu, który z uwagi na poziom uzasadnienia zaufania wysoki, spełnia odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa i który został oceniony na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach i dysponujących znaczącymi zasobami. Dotyczy więc produktu, usługi albo procesu, który ma szczególne znaczenie gospodarcze dla tego podmiotu. Dlatego tak istotne, z punktu widzenia podmiotu, jest niezwłoczne i sprawne podjęcie przez ministra decyzji, w tym zakresie. W związku z powyższym, Spółka proponuje, aby sprawy związane z zatwierdzeniem certyfikatu określone w art. 14 ust. 2 były prowadzone, w trybie określonym w przepisach art. 122a – 122h KPA (Rozdział 8a Milczące załatwienie sprawy), a sprawy związane z cofnięciem ww. certyfikatu na zasadach ogólnych tj. na podstawie decyzji, z określonym terminem maksymalnym załatwienia sprawy, w miejsce ogólnych terminów wynikający z KPA, które mogą być znacznie przedłużane. Ponadto prosimy o rozważenie wprowadzenie rozwiązania polegającego na tym, że cofnięcie certyfikatu byłoby poprzedzone zobowiązaniem dostawcy do ponownego przeprowadzenia badania	poz. 572). Takie rozwiązanie zagwarantuje, że w przypadku, gdy nie będzie trzeba uzyskiwać dodatkowych informacji dotyczących danego procesu, rozstrzygnięcie nastąpi odpowiednio szybko.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			zgodności, z zastrzeżeniem, że jeżeli takie badanie nie zostanie przeprowadzone, albo jego wynik będzie negatywny tj. produkt nadal nie będzie spełniał wymogów zawartych w stosownym programie certyfikacji, to nastąpi cofnięcie certyfikatu.	
61.	**ISSA Polska**	**art. 14 ust. 6**	Art. 14 ust. 6 brak możliwości wystąpienia o sprawdzenie w innym laboratorium. Należy uzupełnić o taką możliwość (art. gdy badanie było nierzetelne).	**Wyjaśnienie uwagi** W wyniku zmian wprowadzonych w projekcie art. 14 otrzymał oznaczenie art. 22, a przepis do którego odnosi się uwaga otrzymał brzmienie: „6. Minister właściwy do spraw informatyzacji przed wydaniem decyzji, o których mowa w ust. 2 pkt 1 i 2 oraz ust. 5, może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w zakresie zgodności certyfikacji z danym europejskim programem certyfikacji cyberbezpieczeństwa. Podmiot, do którego wystąpiono o opinię, przekazuje ją w terminie miesiąca od dnia 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.”.
62.	**Polska Wytwórnia Papierów Wartościowych**	**art. 16**	Art. 16 przyznaje prawo złożenia skargi na dostawcę, który wydał deklarację zgodności, jeżeli produkt, usługa lub proces, którego dana deklaracja dotyczy, nie spełnia wymogów zawartych w europejskimprogramie certyfikacji cyberbezpieczeństwa. Projekt ustawy nie przewiduje tej możliwości, gdy produkt, usługa lub proces, którego deklaracja dotyczy, nie spełnia wymogów zawartych w krajowym programie certyfikacji cyberbezpieczeństwa. Natomiast, w przypadku możliwości złożenia skargi na jednostkę oceniającą zgodność, projekt ustawy nie odnosi się do rodzaju programu certyfikacji cyberbezpieczeństwa, w ramach którego, możliwe będzie złożenie skargi.	**Uwaga uwzględniona** Uzupełniono przepis poprzez wskazanie, że dotyczy to jednostek oceniających zgodność działający w obszarze certyfikacji cyberbezpieczeństwa.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			Wątpliwości budzi to, czy przyjęte rozwiązanie jest zamierzone przez projektodawcę, czy też jest to omyłka. Jeżeli to jest działanie zamierzone, to projektodawca nie wyjaśnił przyczyn takiego ukształtowania treści przepisu w uzasadnieniu do projektu ustawy.	
63.	**Polskie Towarzystwo Informatyczne**	**art. 16 ust. 1 pkt 2**	Skarga – na jednostkę oceniającą zgodność; Uprawnienie to jest przypisane każdemu, bez jakiegokolwiek uwarunkowania. Może to doprowadzić do działań wrogich, skierowanych na zakłócenie działalności CAB-a, art. przez konkurencyjny podmiot. Propozycja zapisu: „2. na jednostkę oceniającą zgodność, w wypadku uzasadnienia interesu skarżącego” Uzasadnienie: Zapewnienie bezpieczeństwa prawnego jednostkom oceniającym zgodność	**Uwaga nieuwzględniona** Zgodnie z przepisami projektu ustawy minister ma pełnić ogólny nadzór nad działalnością certyfikacyjną. W związku z tym należy zapewnić mu możliwie szerokie możliwości otrzymywania informacji o nieprawidłowościach występujących w tym systemie. Również rozporządzenie 2019/881 nie ogranicza skarg do krajowego organu do podmiotów mających interes prawny.
64.	**Polska Wytwórnia Papierów Wartościowych**	**art. 18**	Stosownie do treści art. 18 ust. 1, minister, w ramach nadzoru, o którym mowa w art. 9 ust. 2 pkt 1, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów, usług lub procesów. W ramach kontroli, minister może przeprowadzić lub zlecić badania (art. 20), aby ustalić, czy są spełnione wymogi zawarte w określonym europejskim programie certyfikacji cyberbezpieczeństwa. Ten przepis jest przykładem obszaru możliwej materializacji ryzyka konfliktu interesów opisanego w uwadze nr 1: a) w związku z możliwością prowadzenia przez ministra kontroli wobec jednostek oceniających zgodność, w przypadku, gdy jednocześnie te jednostki byłyby jednostkami świadczącymi usługi wsparcia dla ministra, w realizacji jego zadań, o których mowa w art. 9 ust. 2 projektu ustawy, b) w przypadku, gdy badania prowadzone lub zlecone przez ministra byłyby wykonywane przez państwowy instytut badawczy lub inny podmiot będący jednocześnie jednostką	**Wyjaśnienie uwagi** Przygotowane przepisy pozwolą uniknąć konfliktu interesów gwarantując ministrowi swobodę w wyborze podmiotu dysponującego ekspercką wiedzą w danym obszarze. Należy tu zwrócić uwagę w szczególności na projektowany art. 22 ust. 6 pozwalający skorzystać z eksperckiej wiedzy każdego podmiotu dysponującego kompetencjami w danym obszarze. W związku z tym będzie możliwe zasięgnięcie opinii ekspertów, w przypadku których nie wystąpi konflikt interesów. Należy też podkreślić, że rola tych podmiotów w działaniach krajowego organu do spraw certyfikacji cyberbezpieczeństwa będzie jedynie pomocnicza, nie będą one podejmowały rozstrzygnięć. Nie można określić na tym poziomie zasad wyboru, gdyż będą one różne w przypadku różnych programów certyfikacji i zawartych w nich wymogach.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			oceniającą zgodność, konkurującą z kontrolowaną jednostką oceniającą, c) w przypadku, gdy badania prowadzone lub zlecone przez ministra byłyby wykonywane przez państwowy instytut badawczy lub inny podmiot będący, jednocześnie, jednostką oceniającą zgodność i dotyczyłyby produktu, który posiada certyfikat wydany przez jednostkę oceniającą zgodność – konkurenta jednostki oceniającej zgodność prowadzącej badanie produktu.	
65.	**Polska Wytwórnia Papierów Wartościowych**	**art. 20**	Stosownie do treści art. 20, minister, w ramach przeprowadzanej kontroli może poddać produkt, usługę lub proces, badaniom lub może zlecić innemu podmiotowi przeprowadzenie badania, na okoliczność, czy są spełnione wymagania zawarte w europejskim programie certyfikacji cyberbezpieczeństwa. Przepis nie precyzuje, jakiemu podmiotowi, i przy spełnieniu jakich warunków przez ten podmiot, minister może zlecić stosowne badanie. W wyniku badań, może dojść do uchylenia decyzji o zatwierdzeniu certyfikatu (art. 20 ust. 5) albo do podania przez ministra do publicznej wiadomości informacji o niespełnianiu przez produkt wymogów określonych w programie (art. 20 ust. 4). Są to więc konsekwencje daleko idące. Dlatego, należy określić w projekcie ustawy, zasady zlecania usług przeprowadzania badań i doprecyzować wymogi dla podmiotów, które mogą świadczyć takie usługi.	**Wyjaśnienie uwagi** Minister właściwy do spraw informatyzacji będzie zlecał to zadanie podmiotom dysponującym odpowiednimi kompetencjami w danym obszarze. Nie jest możliwe dokładniejsze doprecyzowanie tych kwestii ze względu na to, że różne programy certyfikacji będą miały różne zakresy przedmiotowe. Z powyższych względów nie można tych kwestii określić na poziomie ustawy.
66.	**Polska Wytwórnia Papierów Wartościowych**	**art. 21**	a) stosownie do art. 21 ust. 1, badanie, o którym mowa w art. 20, może zostać przeprowadzone na próbkach produktu. Spółka zwraca uwagę, że projekt ustawy nie zawiera definicji próbki produktu. Tymczasem, dostawca będzie obowiązany na wezwanie ministra do przekazania osobom prowadzącym czynności kontrolne próbki produktu. Należy podnieść, że taka próbka może dotyczyć produktu, który objęty będzie tajemnicą przedsiębiorstwa, a więc produktu, z którym związane będą	**Uwaga częściowo uwzględniona** Doprecyzowano czym jest próbka w art. 30 projektu. W zakresie kosztów badań należy zwrócić uwagę, że certyfikacja jest dobrowolna, w związku z tym kosztów tych nie poniosą żadne podmioty, które dobrowolnie nie dołączyły do krajowego systemu certyfikacji cyberbezpieczeństwa.

			informacje techniczne, technologiczne lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów, nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób. W związku z powyższym, Spółka wnosi o dodanie do projektu ustawy definicji próbki oraz zasady ochrony poufności informacji o rozwiązaniach stanowiących tajemnicę przedsiębiorstwa zawartych w próbce, stosownie do art. 21 ust. 7, koszty badań, o których mowa w art. 20 i 21, ponosi dostawca produktu, niezależnie, czy badanie wykaże uchybienia w produkcie, czy też nie. Takie rozwiązanie, w ocenie Spółki nie jest prawidłowe. W związku z tym, Spółka wnosi o wprowadzenie rozwiązania zgodnie z którym możliwe jest poniesienie kosztu badania przez dostawcę, ale tylko w przypadku, gdy w wyniku takiego badania zostanie ustalone, że produkt, usługa lub proces nie spełnia wymogów zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa.	
67.	**ISSA Polska**	**art. 21**	Nie jest określona w przepisie karencja dostosowania się podmiotu (właściciela certyfikatu oraz wszystkich podmiotów korzystających z jego produktów i usług) do decyzji ministra właściwego do spraw informatyzacji w sprawie cofnięcia certyfikatu. Jednocześnie przepisy takie mogą kolidować z przepisami Prawo Zamówień Publicznych i skutkować obowiązkiem rozwiązania lub odstąpienia od umowy w zakresie PZP w całości lub części. Minister właściwy do spraw informatyzacji nie ma możliwości ponownego przekazania do innego laboratorium, np. gdy badanie było nierzetelne (przy badaniu nierzetelnym ponowne badanie tylko na wniosek, wynikający ze skargi - art 16 ust 1 - skarga) Po uzyskaniu decyzji ministra właściwego do spraw informatyzacji nie istnieje proces naprawczy - nie ma	**Uwaga uwzględniona** Wprowadzono przepisy nowy art. 31 – umożliwiający wyeliminowanie nieprawidłowości bez utraty certyfikatu.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			możliwości recertyfikacji po usunięciu niezgodności. Proponujemy ustalenie terminu karencji w ustawie. Jednocześnie zwracamy uwagę, że terminy te powinny być różne w zależności od kwalifikacji podmiotu i proporcjonalne do parametrów technicznych oraz organizacyjnych. Powinny brać również pod uwagę kwalifikację poziomu zaufania, którego dotyczy decyzja, wskazanego w art. 52 Rozporządzenia 2019/881. Dodatkowo termin powinien uwzględniać możliwości uzyskania danego rodzaju produktu, czy usługi na rynku lub możliwości zdobycia alternatywnych produktów lub usług oraz możliwość uzyskania certyfikacji.	
68.	**ISSA Polska**	**art. 21 ust. 4**	Pytanie czy umieszczenie informacji w biuletynie nie jest za słabym rozwiązaniem (sposobem poinformowania)? Co z podmiotami, które np. na podstawie certyfikatu, który okazał się po jakimś czasie nieważny, rozstrzygały jakiś proces zakupowy/przetarg i certyfikat był jednym z wymogów? Co z podmiotami, które kupiły wadliwie certyfikowany produkt aby wypełnić jakieś zapisy certyfikowania ich samych, albo certyfikowania ich usług lub procesów? Może producent produktu/usługi/procesu powinien być zobligowany do poinformowania swoich klientów o utracie takiego certyfikatu dla swojego produktu? A co jak dostawcą jest monopolista? Należy wskazać konieczność prowadzenia rejestru przez ministra właściwego do spraw informatyzacji, gdzie każdy może sprawdzić, czy ktoś ma certyfikat i jaki. Dookreślić rejestr obowiązek po stronie ministra właściwego do spraw informatyzacji, a nie podmiotu. Cykl życia certyfikatu powinien być jasno określony w rejestrze. Zobligowanie producenta do poinformowania swoich klientów o utracie certyfikatu dla swojego produktu czy usługi.	**Wyjaśnienie uwagi** Planowane jest utworzenie na stronie podmiotowej BIP MC osobnej zakładki, w której będą znajdować się informacje o cofniętych lub zawieszonych certyfikatach. Równocześnie przepisy nie stoją na przeszkodzie, aby minister właściwy do spraw informatyzacji informował o tym również np. na swojej stronie internetowej. W związku z tym przedmiotowe informacje będą dostępne dla zainteresowanych.
69.	**ISSA Polska**	**art. 21 ust. 7**	Koszty badań zleconych podczas kontroli ponosi dostawca. Przenoszenie kosztów (bez podnoszenia podatków) przełożenie kosztów na producenta, dostawcę, a ten przeniesie koszt na biorcę końcowego, podnosząc koszt swojego	**Uwaga nieuwzględniona** Należy podkreślić, że certyfikacja cyberbezpieczeństwa jest dobrowolna w związku z tym koszty te będą ponosiły jedynie

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			produktu, usługi. Wszyscy za to zapłacimy. Spowoduje to również brak konkurencyjności na rynku. Część rynku jest regulowana, a część komercyjna. Część komercyjna będzie miała problem. Ta część rynku poniesie niewspółmierne, nieadekwatne koszty, przez co jej produkty i usługi nie będą konkurencyjne. Spowoduje to nierówne traktowanie podmiotów na rynku.	podmioty, które dobrowolnie dołączyły do krajowego systemu certyfikacji cyberbezpieczeństwa.
70.	**Polskie Towarzystwo Informatyczne**	**dodatkowy przepis**	Wydaje się celowe uzupełnienie opiniowanego projektu o przepis nakazujący przeprowadzanie okresowych przeglądów oraz dokonywanie okresowych kompleksowych ocen funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji (na wzór przepisów Art 67 rozporządzenia 2019/881) i przedkładania wyników Radzie Ministrów RP. Uzasadnienie: Krajowy System Certyfikacji Cyberbezpieczeństwa jest nowym rozwiązaniem systemowym w polskim systemie prawnym i powinien podlegać „tuning'owi”	**Uwaga nieuwzględniona** Minister właściwy do spraw informatyzacji, w ramach swoich ogólnych kompetencji będzie oceniał skuteczność przyjętych regulacji i nie ma potrzeby tworzyć dodatkowych przepisów dotyczących tej kwestii.
71.	**Polskie Towarzystwo Informatyczne**	**Nowa propozycja**	W projekcie ustanowiono mechanizm planowania generowania przychodów z kar – kto, dlaczego i na jakich zasadach może być ukarany – czy karane mają być nieupoważnione/nieakredytowane jednostki oceniające zgodność, jednostki oceniające zgodność wydające certyfikaty klientom niespełniającym wymagań lub jeśli same nie spełniają wymagań, klienci łamiący wymagania stawiane przez krajowy/europejski program certyfikacji cyberbezpieczeństwa po otrzymaniu certyfikatu i w czasie obowiązywania. Krajowy system certyfikacji cyberbezpieczeństwa jest w Polsce konstrukcją nową i rozbudowany system kar będzie po prostu odstraszający. Wydaje się, że lepiej jest pomagać i dawać dobry przykład niż karać. Propozycja zapisu: Sugeruje się znaczące zmniejszenie wysokości kar.	**Uwaga nieuwzględniona** Rozporządzenie 2019/881 nakłada na wszystkie państwa członkowskie Unii Europejskiej obowiązek wprowadzenia kar za naruszenie przepisów związanych z certyfikacją. Zgodnie z art. 65 tego aktu prawnego kary te muszą być skuteczne, proporcjonalne i odstraszające. Obniżenie kar skutkowałoby nieosiągnięciem efektu odstraszającego, który chce wywołać ustawodawca europejski.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			Uzasadnienie: Uniknięcie efektu odstraszania i promocja certyfikacji (pozytywne bodźce), która jest jednym z oczywistych celów Ustawy.	
uwagi do Oceny Skutków Regulacji				
72.	**Polskie Towarzystwo Informatyczne**	**pkt 1**	„Sama certyfikacja w zakresie cyberbezpieczeństwa jest procesem czasochłonnym i kosztownym, co ogranicza dostępność do certyfikatów. Wprowadzenie krajowego systemu certyfikacji powinno przyczynić się do zmiany tego stanu rzeczy." Teza ta jest nietrafna. Samo wprowadzenie krajowych programów certyfikacji cyberbezpieczeństwa nie może być aktem woli krajowego organu, ponieważ rozporządzenie 2019/881 zakazuje tworzenia krajowych programów, jeśli zakres przedmiotowy pokrywa europejski program certyfikacji cyberbezpieczeństwa. Stąd Minister ma tu bardzo ograniczone pole do działania. Propozycja zapisu: Sugeruje się skreślenie wskazanego akapitu z OSR. Uzasadnienie: Przepisy Art. 57 ust. 2 rozporządzenia 2019/881 stanowią cyt. „Państwa członkowskie nie mogą wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT i procesów ICT, które są już objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa.". Co więcej, tamże (ust. 4) stanowi: „Z myślą o unikaniu rozdrobnienia rynku wewnętrznego, państwa członkowskie informują Komisję i ECCG o wszelkich zamiarach dotyczących opracowania nowych krajowych programów certyfikacji cyberbezpieczeństwa.". Wskazany akapit (przedostatni) p. 1-go OSR co najmniej niejednoznaczny może wprowadzać w błąd Ustawodawcę w trakcie procedowania opiniowanego projektu	**Uwaga uwzględniona** Przedmiotowy fragment został skreślony.

Zestawienie uwag zgłoszonych w ramach konsultacji publicznych projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			ustawy w Parlamencie.	
73.	**PERN S.A.**		Projekt nie zawiera informacji o potencjalnych kosztach przedsiębiorców – użytkowników końcowych produktów i usług ICT, wynikających z negatywnej oceny zgodności z warunkami certyfikacji cyberbezpieczeństwo, przeprowadzanej u Dostawców produktów usług ICT ani związanych z tym regulacji.	**Wyjaśnienie uwagi** W związku z tym, że projekt nie przewiduje obowiązkowej certyfikacji, jego wejście w życie nie powoduje żadnych obowiązkowych kosztów po stronie przedsiębiorców.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

lp.	podmiot zgłaszający uwagę	jednostka redakcyjna	treść uwagi	stanowisko Ministra Cyfryzacji
uwagi ogólne do projektu				
1.	**Instytut Łączności – Państwowy Instytut Badawczy**		Przedstawiciele Instytutu Łączności – Państwowego Instytutu Badawczego (IŁ-PIB) brali udział w pracach zespołu eksperckiego Polskiego Towarzystwa Informatycznego (PTI) i przedstawili uwagi do projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42). Uwagi przekazane przez PTI do Ministerstwa Cyfryzacji w przedmiotowej sprawie w całości pokrywają uwagi i obserwacje IŁ-PIB.	Odniesienia do uwag PTI znajdują się w załączniku nr 1 do raportu z konsultacji.
2.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**		Projekt ustawy swoim zakresem obejmuje trzy kategorie pojęciowe, tj. produkty ICT, usługi ICT oraz procesy ICT. W naszej opinii projekt powinien objąć swoim zakresem, poza ww. kategoriami, również zagadnienia związane z certyfikacją osób oraz systemów zarządzania, które w bliskiej przyszłości będą musiały znaleźć odzwierciedlenie w krajowym porządku prawnym. Objęcie projektem regulacji również certyfikacji osób może stanowić istotne narzędzie nadzoru dla zapisanych w art. 20 ust. 2 Dyrektywy NIS2 wymagań w zakresie zapewnienia przez państwa członkowskie tego, *aby członkowie organu zarządzającego podmiotów kluczowych i ważnych mieli obowiązek odbywać regularne szkolenia, a także zachęcania podmiotów kluczowych i ważnych do oferowania podobnych szkoleń ich pracownikom."* Wspomniany przepis dyrektywy ma zostać zaimplementowany do polskiego prawodawstwa w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa (UC32), w planowanym art. 8e, w brzmieniu: *„Kierownik podmiotu kluczowego lub podmiotu ważnego raz w roku kalendarzowym przechodzi szkolenie z zakresu wykonywania obowiązków, o których mowa w art. 7, art. 8, art. 8d, art. 8e, art. 8f ust. 2, art. 8h, art. 9–11 i art. 15. Udział w szkoleniu jest udokumentowany.".* Dodatkowo w innych unijnych aktach prawnych z zakresu prawa nowych technologii pojawiają się zagadnienia z obszaru oceny zgodności systemów zarządzania cyberbezpieczeństwem czy kompetencji osób. W związku z powyższym, celowe wydaje się rozszerzenie ww. projektu ustawy o certyfikację osób, jak i systemów zarządzania.	**Uwaga uwzględniona** W projekcie zostały zamieszczone przepisy dotyczące certyfikacji osób oraz systemów zarządzania.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			W przypadku nieuwzględnienia powyższej uwagi, proponujemy zmianę brzmienia art. 5 i 6 projektu ustawy poprzez dodanie możliwości poddania ocenie zgodności na podstawie określonego krajowego programu certyfikacji cyberbezpieczeństwa również osób i systemów zarządzania, a także proponujemy uwzględnienie możliwości publikacji krajowych programów certyfikacji cyberbezpieczeństwa w zakresie certyfikacji osób i systemów zarządzania. Wprowadzenie tej zmiany niewątpliwie ułatwi przygotowanie krajowego programu certyfikacji cyberbezpieczeństwa kierowników podmiotów kluczowych i ważnych, o których mowa w art. 8e nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który uprawniałby jego beneficjenta do otrzymania certyfikatu na europejskim poziomie.	
3.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**		Dodatkowo, w nawiązaniu do wykonywania ww. zadań zleconych, rekomendujemy powołanie Krajowej Jednostki Certyfikującej Cyberbezpieczeństwa, która byłaby częścią Krajowego Systemu Certyfikacji Cyberbezpieczeństwa, a do której podstawowych zadań należałoby wsparcie ministra właściwego do spraw informatyzacji w pełnieniu funkcji krajowego organu do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881 (dalej: CSA), i realizacji zadań w zakresie m.in.: • przeprowadzania wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881 (CSA), • przeprowadzania wzajemnej oceny, o których mowa w art. 54 ust. 1 lit. u CSA, • zatwierdzania europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania wysoki, o którym mowa w art. 52 ust. 7 CSA, • innych zadań wymagających specjalistycznych kompetencji technicznych. Organizacja Krajowej Jednostki Certyfikującej Cyberbezpieczeństwa jest wykonalna dla NASK Państwowego Instytutu Badawczego, jako naturalna konsekwencja dotychczasowej działalności, tj. działającej obecnie akredytowanej Jednostki Certyfikującej oraz pełnoprawnego uczestnika porozumień międzynarodowych dotyczących certyfikacji cyberbezpieczeństwa (SOG-IS MRA i CCRA).	**Uwaga nieuwzględniona** Projektodawca przewidział inny model wydawania certyfikatów odwołujących się do poziomu uzasadnienia zaufania „wysoki”. Celem projektodawcy jest zapewnienie pełnej konkurencyjności w tym względzie, tak aby zachęcić podmioty prywatne do tworzenia jednostek oceniających zgodność. W związku z tym nie można wyróżniać jednej konkretnej jednostki certyfikującej poprzez wpisanie jej w przepisy projektowanej ustawy. Takie rozwiązanie budziłoby również wątpliwości ze względu na jego wpływ na konkurencyjność w tym obszarze.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			NASK-PIB posiada odpowiednie (unikalne w skali kraju) kompetencje wykonawcze, zdolności organizacyjne, doświadczenie praktyczne oraz wykwalifikowany personel. Należy w tym miejscu przypomnieć, że analogiczne rozwiązanie zostało zaimplementowane w ustawie o Krajowym Systemie Cyberbezpieczeństwa w odniesieniu do utworzenia CSIRT NASK na bazie już istniejącego zespołu reagowania na incydenty komputerowe, tj. CERT Polska. Jednocześnie, należy tutaj wskazać istotny dla właściwego funkcjonowania systemu certyfikacji element nadzoru nad certyfikowanymi produktami, związany z reagowaniem na podatności ujawnione wobec certyfikowanych wyrobów/produktów. Jest to proces zależny m.in. od sprawnego przepływu informacji w zakresie skoordynowanego ujawniania podatności. Należy w tym miejscu wspomnieć, że procedowana równolegle zmiana ustawy o Krajowym Systemie Cyberbezpieczeństwa (UC 32) w art.26a ust. 1 wskazuje NASK – PIB jako koordynatora na potrzeby skoordynowanego ujawniania podatności. Tożsamość podmiotowa dla wykonywania obu funkcji, tj. zadań w zakresie certyfikacji cyberbezpieczeństwa i ujawniania podatności umożliwia synergiczne wykorzystanie potencjału instytucji.	
4.	**Prezes Urzędu Ochrony Danych Osobowych**		Przyjęcie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa wynika z konieczności implementacji rozporządzenia 2019/8813 oraz ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT przez wprowadzenie procedur w zakresie certyfikacji produktów ICT, usług ICT lub procesów ICT w ramach europejskich albo krajowych programów certyfikacji cyberbezpieczeństwa. W projekcie wprowadzono dwie możliwości otrzymania certyfikatu z zakresu cyberbezpieczeństwa. Jak podniesiono w uzasadnieniu projektu ustawy, „[w] zakresie akredytacji oraz certyfikacji w znacznej mierze stosowane będą przepisy ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854). Stosowane przepisy proceduralne są już wykorzystywane przez podmioty, których dotyczą, a nowym elementem będą jedynie wymagania określane dla każdego z poziomów zaufania”. Certyfikowanie ma się odbywać na podstawie określonego europejskiego programu certyfikacji cyberbezpieczeństwa lub na podstawie określonego krajowego programu certyfikacji cyberbezpieczeństwa. Krajowe programy certyfikacji	**Przyjęto do wiadomości**

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			cyberbezpieczeństwa będą tworzone w drodze rozporządzeń ministra, które mogą, choć nie muszą, być przez niego wydane. Zgodnie z treścią projektu podmiotem upoważnionym do udzielania akredytacji będzie Polskie Centrum Akredytacji. Warto podkreślić, że proponowane regulacje nie zawierają odniesień do rozporządzenia 2016/679 ani nie modyfikują zasad z niego wynikających. Rozporządzenie 2016/679 znajdzie zastosowanie do oceny procesów związanych z przetwarzaniem danych osobowych i administratorzy będą zobowiązani do stosowania przepisów o ochronie danych osobowych (w tym: analizy ryzyka, projektowania ochrony danych i tzw. domyślnej ochrony czy też stosowania rozwiązań wynikających z art. 42 i 43 rozporządzenia 2016/679 i odpowiednich przepisów ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781). Należy wskazać także, że administratorzy ubiegający się o uzyskanie certyfikatu muszą pamiętać o zapewnieniu także zgodności procesów przetwarzania danych osobowych z przepisami rozporządzenia 2016/679, w tym dokonaniu – wskutek zaistnienia warunków z art. 35 rozporządzenia 2016/679 – oceny skutków dla ochrony danych.	
uwagi do poszczególnych przepisów projektu				
5.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**	**art. 2**	Kolejnym zagadnieniem, które wymaga rozważenia, w celu zachowania spójności terminologicznej, jest definicja zawarta w art. 2 pkt 13 projektu ustawy. Otóż zgodnie z nomenklaturą używaną przy zagadnieniach związanych z akredytacją i certyfikacją należy posługiwać się pojęciem „wyroby", a nie „produkty". W literaturze przedmiotu zdarza się, że pojęcia te są używane zamiennie, ale z formalnego punktu widzenia należy używać pojęcia „wyrób" w przypadku akredytowanej działalności certyfikacyjnej. W związku z tym proponujemy zmianę definicji poprzez jej rozszerzenie i dopisanie, że pojęcie produktu jest równoważne z pojęciem wyrobu.	**Uwaga częściowo uwzględniona** Ze względu na to, że rozporządzenie 2019/881 nie posługuje się pojęciem „wyrób", jego wprowadzenie mogłoby spowodować wątpliwości związane ze zgodnością przepisów ustawy z prawem europejskim. W związku z tym kwestia ta zostanie dodana do uzasadnienia.
6.	**Polski Komitet Normalizacyjny**	**art. 2**	Dodatkowo w ocenie PKN zasadne wydaje się wprowadzenie w art. 2 projektu definicji terminów: „specyfikacja techniczna", „norma" i „standard". Obecne zapisy art. 10 rodzą wątpliwości, co do interpretacji, gdyż nie wiadomo czy chodzi np. o normy jakości (niebędące Polskimi Normami) czy o „normy" zdefiniowane w art. 2 pkt 4 ustawy o normalizacji, w którym przez termin norma rozumie się *dokument przyjęty na zasadzie konsensu i zatwierdzony przez*	**Uwaga uwzględniona** Wprowadzono definicję „specyfikacji technicznej" oraz „normy". Standard nie jest definiowany przez rozporządzenie 2019/881 w związku z czym, aby nie wywoływać wątpliwości co do zgodności z

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			upoważnioną jednostkę organizacyjną, ustalający – do powszechnego i wielokrotnego stosowania – zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie. Jednocześnie uprzejmie informuję, że termin „standard" nie jest stosowany w normalizacji krajowej jako synonim „normy".	przepisami europejskimi nie zostanie wprowadzona jego definicja.
7.	**Urząd Komunikacji Elektronicznej**	**art. 2 pkt 3**	W celu wyeliminowania ewentualnych wątpliwości interpretacyjnych w zakresie definiowanego w art. 2 pkt 3 pojęcia „deklaracja zgodności" proponuje się zastąpienie go używanym na gruncie 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) pojęciem „unijna deklaracja zgodności". Należy bowiem zauważyć, że sformułowana w motywie 81 do rozporządzenia UE nr 2019/881 definicja „unijnej deklaracji zgodności" jest zbieżna z definicją „deklaracji zgodności" w rozumieniu projektowanej ustawy.	**Uwaga uwzględniona** Zdefiniowano pojęcie „deklaracja zgodności" określając wprost, że oznacza ono europejską deklaracje zgodności, zgodnie ze stanowiskiem Rządowego Centrum Legislacji przedstawionym w ramach uzgodnień.
8.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**	**art. 10**	W projektowanym brzmieniu art. 10 ust. 2 ustawy wskazuje się na udzielenie przez ministra właściwego do spraw informatyzacji dotacji celowej na realizację zadań, o których mowa w art. 9 ust. 2, z tej części budżetu państwa, której minister jest dysponentem. Specyfika dotacji celowych polega na tym, że są one udzielane na realizację zadań zleconych z zakresu administracji rządowej. W przypadku zadań, które mogą być zlecone państwowym instytutom badawczym, o których mowa we wspomnianym art. 9 ust. 2 projektu ustawy (czytanym łącznie z art. 10 ust. 4) powodują uzasadnione wątpliwości, czy środki finansowe na realizację tych zadań nie powinny być przyznane w drodze dotacji podmiotowej. Zgodnie bowiem z art. 131 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, dotacje podmiotowe obejmują środki dla podmiotu wskazanego w odrębnej ustawie lub w umowie międzynarodowej, wyłącznie na dofinansowanie działalności bieżącej w zakresie określonym w odrębnej ustawie lub umowie międzynarodowej. W kontekście przywołanego wyżej art. 10 ust. 4 i konieczności utrzymanie stałej sprawności operacyjnej i odpowiedniego poziomu kompetencji w zakresie opracowywania i walidacji	**Uwaga nieuwzględniona** Dotacja, o której mowa w przedmiotowym przepisie, będzie związana z konkretnymi działaniami jednostki certyfikującej. Z tego względu bardziej adekwatna w tej sytuacji jest dotacja celowa.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			procedur badawczych, metod i technik oceny oraz wytwarzania materiałów odniesienia, czy pozyskiwanie i utrzymanie ekspertów umożliwiających sprawną realizację zadań, wydaje się, że powinna być przyznawana dotacja podmiotowa, a nie celowa na realizację wskazanych w projekcie ustawy zadań.	
9.	**Prezes Urzędu Ochrony Danych Osobowych**	**art. 10**	Odnosząc się szczegółowo do regulacji zawartych w projekcie, należy wskazać na art. 10 ust. 1 pkt 2 projektu, na podstawie którego państwowe instytuty badawcze uprawnione są do weryfikacji dokumentów pochodzących od jednostek oceniających zgodność prowadzących ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa oraz od dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje produkty ICT, usługi ICT lub procesy ICT ocenie zgodności w ramach określonego europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa. Przepis ten sformułowany jest jednak w sposób zbyt ogólny. Nie określa bowiem zakresu weryfikowanych dokumentów, co powoduje brak przejrzystości w zakresie przetwarzania danych osobowych potencjalnie zawartych w treści tychże dokumentów (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Brak określenia sposobu weryfikacji i jej celu również wpływa na możliwość ustalenia celu i sposobu przetwarzania danych osobowych, o ile znajdą się w treści dokumentów.	**Uwaga nieuwzględniona** Wskazano pod jakim kątem będzie odbywała się weryfikacja dokumentów. Pełne określenie zakresu dokumentów nie jest możliwe, gdyż poszczególne europejskie programy certyfikacji mogą wprowadzać różne rodzaje dokumentów związanych z certyfikacją.
10.	**Polski Komitet Normalizacyjny**	**art. 10**	W ocenie PKN wątpliwości budzi użyty w art. 10 ust. 1 pkt 4 oraz ust. 3 pkt 4 zapis - *publikację specyfikacji technicznych, norm i standardów.* Zwracam uwagę, że proponowany zapis może sugerować obowiązek publikacji przez państwowe instytuty badawcze treści Polskich Norm. Zgodnie z art. 5 ust. 5 ustawy o normalizacji z dnia 12 września 2002 r. (Dz. U. z 2015 r. poz. 1483) *Polskie Normy korzystają z ochrony jak utwory literackie, a autorskie prawa majątkowe do nich przysługują krajowej jednostce normalizacyjnej*. Natomiast zgodnie z art. 5 ust. 6 ustawy o normalizacji te same zasady *stosuje się odpowiednio do norm europejskich i międzynarodowych, z zachowaniem porozumień międzynarodowych*. PKN jest członkiem europejskich (CEN, CENELEC) i międzynarodowych (ISO, IEC) organizacji normalizacyjnych. Organizacje te zobowiązują swoich członków do zapewnienia najwyższego poziomu ochrony praw autorskich do norm na poziomie krajowym. Zatem,	**Uwaga uwzględniona** Przepis otrzyma zaproponowane brzmienie.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			jeżeli intencją ustawodawcy jest wprowadzenie możliwości publikowania przez państwowe instytuty badawcze norm i specyfikacji technicznych, rozumianych jako m.in. Polskie Normy, zachodzi sprzeczność projektowanych przepisów z zapisami ustawy o normalizacji w zakresie praw autorskich, które z mocy ustawy należą do PKN. Ponadto zwracam uwagę, że zgodnie z w art. 11 pkt 2 ustawy o normalizacji do zadań statutowych PKN należy *organizowanie i nadzorowanie działań związanych z opracowywaniem i* ***rozpowszechnianiem Polskich Norm*** *i innych dokumentów normalizacyjnych.* Zatem kwestie związane z publikacją i rozpowszechnianiem Polskich Norm są wyłączną kompetencją PKN zgodnie z przepisami ustawy o normalizacji. Mając na uwadze powyższe proponuję zmianę projektowanych przepisów art. 10 ust. 1 pkt 4 oraz ust. 3 pkt 4 w następujący sposób: *publikację wykazów specyfikacji technicznych, norm i standardów.* Taki zapis pozwoli uniknąć niejednoznaczności oraz nie będzie sprzeczny z ustawą o normalizacji.	
11.	**Polski Komitet Normalizacyjny**	**art. 10**	Konieczne jest także doprecyzowanie użytego w art. 10 ust. 1 pkt 5 i ust. 3 pkt 5 sformułowania *reprezentację interesów krajowych w międzynarodowych grupach normalizacyjnych*. Art. 11 pkt 4 ustawy o normalizacji jako jedno z zadań PKN wskazuje „reprezentowanie Rzeczypospolitej Polskiej w międzynarodowych i regionalnych organizacjach normalizacyjnych". Do kompetencji PKN należy m.in. reprezentowanie krajowych interesariuszy w organach zarządzających i wykonawczych europejskich i międzynarodowych organizacji normalizacyjnych, uczestniczenie we wszystkich pracach na poziomie technicznym między innymi przekazywanie stanowiska krajowego do projektów norm (ankieta powszechna i głosowanie), zgłaszanie ekspertów do grup roboczych (WG), delegatów na posiedzenia ciałach technicznych (TC, SC) oraz prowadzenie sekretariatów komitetów/ podkomitetów technicznych. Należy zatem zdefiniować intencje ustawodawcy tak, aby nie były sprzeczne z ustawą o normalizacji. Proponuję zmianę zapisu art. 10 ust. 1 pkt 5 i ust. 3 pkt 5 w następujący sposób: *Udział w pracach międzynarodowych grup normalizacyjnych z zakresu cyberbezpieczeństwa zgodnie z zasadami normalizacji krajowej i międzynarodowej.*	**Uwaga uwzględniona** Przepisy otrzymają zaproponowane brzmienie.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

12.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**	**art. 14**	Rekomendujemy doprecyzowanie brzmienia art. 14 ust. 1 projektu ustawy. Nie został w sposób jasny dookreślony 14-dniowy termin na przesyłanie do ministra właściwego do spraw informatyzacji, wniosku o zatwierdzenie europejskiego certyfikatu w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania wysoki, o którym mowa w art. 57 ust. 2 CSA. Określenie użyte w przepisie „po przeprowadzeniu certyfikacji" może odnosić się do wielu różnych zdarzeń, które można zakwalifikować jako następujące: a. „po przeprowadzeniu certyfikacji" tj. np. wydania sprawozdania z certyfikacji, b. wydania decyzji certyfikacyjnej, c. wydania samego certyfikatu, d. dostarczenia certyfikatu do rąk jego posiadacza. W związku z tym rekomendujemy dokładne określenie momentu/ zdarzenia, od którego należy liczyć ww. termin. Naszym zdaniem 14-dniowy termin powinien być liczony od dnia wydania decyzji certyfikacyjnej. Wydanie decyzji certyfikacyjnej (pkt. 7.6 normy PN-EN ISO/IEC 17065) przez odpowiednio umocowany personel Jednostki Certyfikującej (np. Komitet Certyfikujący, jak ma to miejsce w JC NASKPIB) jest zdarzeniem o tyle właściwym, że następuje po dokonaniu oceny (pkt. 7.4) oraz przeglądu (pkt. 7.5), natomiast przed wydaniem dokumentów certyfikacyjnych (pkt. 7.7).	**Uwaga uwzględniona** Doprecyzowano terminy.
13.	**Prezes Urzędu Ochrony Danych Osobowych**	**art. 15**	W art. 15 ust. 1 projektu projektodawca określił obowiązek jednostki oceniającej zgodność do przekazania właściwemu ministrowi danych dostawcy wraz z m.in. kopią europejskiego lub krajowego certyfikatu. O ile sam zakres przekazywanych danych nie budzi wątpliwości, to prawodawca określić powinien sposób, w jaki dane mają być przekazywane. Uzasadnienia wymaga również obowiązek przekazania kopii certyfikatu, który również zawierać może dane osobowe. Prawodawca określić powinien sposób przechowywania ww. kopii (art. 5 ust. 1 lit. f rozporządzenia 2016/679) oraz okres retencji danych pochodzących z ich treści (art. 5 ust. 1 lit. e rozporządzenia 2016/679).	**Uwaga uwzględniona** Dodano przepisy dotyczące sposobu przechowywania danych oraz okres, przez jaki przechowywane są kopie certyfikatów. W pozostałym zakresie nie przewidujemy przechowywania danych osobowych w związku z czym nie ma konieczności dokładniejszego regulowania innych kwestii związanych z danymi, niebędącymi danymi osobowymi.
14.	**Urząd Komunikacji Elektronicznej**	**art. 20-22**	Zgodnie z art. 20 minister właściwy do spraw informatyzacji w ramach przeprowadzanej kontroli może poddać badaniom produkt ICT, usługę ICT lub	**Uwaga uwzględniona**

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			proces ICT, dla których został wydany certyfikat albo deklaracja zgodności. W związku z treścią tego przepisu należy zauważyć, że w art. 21 i art. 22, które dotyczą wspomnianej kontroli, mowa jest tylko o produktach ICT. Proponuje się zatem uspójnienie projektowanych przepisów w powyższym zakresie. Na marginesie zasygnalizować również warto rozważenie zasadności wprowadzenia analogicznego uspójnienia w art. 10 ust. 1 pkt 3 i ust. 3 pkt 3 - o ile wolą projektodawcy jest, aby minister właściwy do spraw informatyzacji mógł być wspierany przez państwowe instytuty badawcze w zakresie przeprowadzania badań nie tylko produktów ICT, lecz również usług ICT i procesów ICT.	Dodano usługę ICT i proces ICT do art. 22. Art. 21 dotyczy pobierania próbek produktów, w związku z czym nie może odnosić się do usług i procesów.
uwaga do Oceny Skutków Regulacji				
15.	**Polskie Centrum Akredytacji**	**pkt 6**	Nie zgłaszam uwag do rozwiązań zawartych w projekcie ww. ustawy natomiast proszę o uzupełnienie zapisów zawartych w ocenie skutków regulacji w części „wpływ na sektor finansów publicznych" o następujący (co do rozwiązań merytorycznych) zapis: „Wejście w życie projektowanej ustawy związane jest z rozszerzeniem działalności akredytacyjnej o obszar wskazany w ustawie, a tym samym, z koniecznością zwiększenia zatrudnienia w Polskim Centrum Akredytacji w wymiarze jednego etatu od 2025 r. Osoba zatrudniona odpowiedzialna będzie za organizację prowadzenia procesu akredytacji podmiotów ubiegających się o uprawnienie do certyfikacji w ramach programów certyfikacji cyberbezpieczeństwa. Zgodnie z ustawą o systemach oceny zgodności i nadzoru rynku (Dz. U. 2022 poz. 1854) Polskie Centrum Akredytacji prowadzi samodzielną gospodarkę finansową a koszty działalności, w tym wynagrodzenia pracowników, są pokrywane z przychodów PCA. PCA nie otrzymuje środków z budżetu państwa. Zatrudnienie dodatkowej osoby wymagało będzie uwzględnienia w planie finansowym i zwiększenia wydatków w funduszu osobowym o 0,3 mln. zł. rocznie od 2025 r. Środki te przeznaczone będą na sfinansowanie dodatkowego etatu oraz na wynagrodzenia dla osób, które otrzymają dodatkowe zadania w projektowanym zakresie. Zwiększenie to musi być utrzymane w kolejnych latach, zwiększane o wskaźnik wzrostu płac i będzie sfinansowane w ramach samodzielnej gospodarki finansowej PCA. Do oszacowania wydatków wzięto pod uwagę średnie wynagrodzenie jakiego	**Uwaga uwzględniona** Przekazany fragment został dodany do OSR.

Zestawienie uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

			oczekują kandydaci do pracy z ostatniego okresu z uwzględnieniem kosztów pracodawcy.”	

Zestawienie nieuwzględnionych uwag zgłoszonych w ramach opiniowania projektu ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

lp.	podmiot zgłaszający uwagę	jednostka redakcyjna	treść uwagi	stanowisko Ministra Cyfryzacji
uwaga ogólna do projektu				
1.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**		Dodatkowo, w nawiązaniu do wykonywania ww. zadań zleconych, rekomendujemy powołanie Krajowej Jednostki Certyfikującej Cyberbezpieczeństwa, która byłaby częścią Krajowego Systemu Certyfikacji Cyberbezpieczeństwa, a do której podstawowych zadań należałoby wsparcie ministra właściwego do spraw informatyzacji w pełnieniu funkcji krajowego organu do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881 (dalej: CSA), i realizacji zadań w zakresie m.in.: • przeprowadzania wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881 (CSA), • przeprowadzania wzajemnej oceny, o których mowa w art. 54 ust. 1 lit. u CSA, • zatwierdzania europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania wysoki, o którym mowa w art. 52 ust. 7 CSA, • innych zadań wymagających specjalistycznych kompetencji technicznych. Organizacja Krajowej Jednostki Certyfikującej Cyberbezpieczeństwa jest wykonalna dla NASK Państwowego Instytutu Badawczego, jako naturalna konsekwencja dotychczasowej działalności, tj. działającej obecnie akredytowanej Jednostki Certyfikującej oraz pełnoprawnego uczestnika porozumień międzynarodowych dotyczących certyfikacji cyberbezpieczeństwa (SOG-IS MRA i CCRA). NASK-PIB posiada odpowiednie (unikalne w skali kraju) kompetencje wykonawcze, zdolności organizacyjne, doświadczenie praktyczne oraz wykwalifikowany personel. Należy w tym miejscu przypomnieć, że analogiczne rozwiązanie zostało zaimplementowane w ustawie o Krajowym Systemie Cyberbezpieczeństwa w odniesieniu do utworzenia CSIRT NASK na bazie już istniejącego zespołu reagowania na incydenty komputerowe, tj. CERT Polska. Jednocześnie, należy tutaj wskazać istotny dla właściwego funkcjonowania systemu certyfikacji element nadzoru nad certyfikowanymi produktami, związany z reagowaniem na podatności ujawnione wobec certyfikowanych wyrobów/ produktów. Jest to proces zależny m.in. od sprawnego przepływu	**Uwaga nieuwzględniona** Projektodawca przewidział inny model wydawania certyfikatów odwołujących się do poziomu uzasadnienia zaufania wysoki. Chcemy zapewnić pełną konkurencyjność w tym względzie, tak aby zachęcić podmioty prywatne do tworzenia jednostek oceniających zgodność. W związku z tym nie chcemy wyróżniać jednej konkretnej jednostki certyfikującej poprzez wpisanie jej w przepisy ustawy. Takie rozwiązanie budziłoby również wątpliwości ze względu na jego wpływ na konkurencyjność w tym obszarze.

			informacji w zakresie skoordynowanego ujawniania podatności. Należy w tym miejscu wspomnieć, że procedowana równolegle zmiana ustawy o Krajowym Systemie Cyberbezpieczeństwa (UC 32) w art.26a ust. 1 wskazuje NASK – PIB jako koordynatora na potrzeby skoordynowanego ujawniania podatności. Tożsamość podmiotowa dla wykonywania obu funkcji, tj. zadań w zakresie certyfikacji cyberbezpieczeństwa i ujawniania podatności umożliwia synergiczne wykorzystanie potencjału instytucji.	
uwagi do poszczególnych przepisów projektu				
2.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**	**art. 2**	Kolejnym zagadnieniem, które wymaga rozważenia, w celu zachowania spójności terminologicznej, jest definicja zawarta w art. 2 pkt 13 projektu ustawy. Otóż zgodnie z nomenklaturą używaną przy zagadnieniach związanych z akredytacją i certyfikacją należy posługiwać się pojęciem „wyroby", a nie „produkty". W literaturze przedmiotu zdarza się, że pojęcia te są używane zamiennie, ale z formalnego punktu widzenia należy używać pojęcia „wyrób" w przypadku akredytowanej działalności certyfikacyjnej. W związku z tym proponujemy zmianę definicji poprzez jej rozszerzenie i dopisanie, że pojęcie produktu jest równoważne z pojęciem wyrobu.	**Uwaga częściowo uwzględniona** Ze względu na to, że 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) nie posługuje się pojęciem „wyrób", jego wprowadzenie mogłoby spowodować wątpliwości związane ze zgodnością przepisów ustawy z prawem europejskim. W związku z tym kwestia ta zostanie dodana do uzasadnienia.
3.	**Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy**	**art. 10**	W projektowanym brzmieniu art. 10 ust. 2 ustawy wskazuje się na udzielenie przez ministra właściwego do spraw informatyzacji dotacji celowej na realizację zadań, o których mowa w art. 9 ust. 2, z tej części budżetu państwa, której minister jest dysponentem. Specyfika dotacji celowych polega na tym, że są one udzielane na realizację zadań zleconych z zakresu administracji rządowej. W przypadku zadań, które mogą być zlecone państwowym instytutom badawczym, o których mowa we wspomnianym art. 9 ust. 2 projektu ustawy (czytanym łącznie z art. 10 ust. 4) powodują uzasadnione wątpliwości, czy środki finansowe na realizację tych zadań nie powinny być przyznane w	**Uwaga nieuwzględniona** Dotacja, o której mowa w przedmiotowym przepisie będzie związana z konkretnymi działaniami jednostki certyfikującej. Z tego względu bardziej adekwatna w tej sytuacji jest dotacja celowa.

			drodze dotacji podmiotowej. Zgodnie bowiem z art. 131 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, dotacje podmiotowe obejmują środki dla podmiotu wskazanego w odrębnej ustawie lub w umowie międzynarodowej, wyłącznie na dofinansowanie działalności bieżącej w zakresie określonym w odrębnej ustawie lub umowie międzynarodowej. W kontekście przywołanego wyżej art. 10 ust. 4 i konieczności utrzymanie stałej sprawności operacyjnej i odpowiedniego poziomu kompetencji w zakresie opracowywania i walidacji procedur badawczych, metod i technik oceny oraz wytwarzania materiałów odniesienia, czy pozyskiwanie i utrzymanie ekspertów umożliwiających sprawną realizację zadań, wydaje się, że powinna być przyznawana dotacja podmiotowa, a nie celowa na realizację wskazanych w projekcie ustawy zadań.	
4.	**Prezes Urzędu Ochrony Danych Osobowych**	**art. 10**	Odnosząc się szczegółowo do regulacji zawartych w projekcie, należy wskazać na art. 10 ust. 1 pkt 2 projektu, na podstawie którego państwowe instytuty badawcze uprawnione są do weryfikacji dokumentów pochodzących od jednostek oceniających zgodność prowadzących ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa oraz od dostawców produktów ICT, usług ICT lub procesów ICT, którzy poddają swoje produkty ICT, usługi ICT lub procesy ICT ocenie zgodności w ramach określonego europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa. Przepis ten sformułowany jest jednak w sposób zbyt ogólny. Nie określa bowiem zakresu weryfikowanych dokumentów, co powoduje brak przejrzystości w zakresie przetwarzania danych osobowych potencjalnie zawartych w treści tychże dokumentów (art. 5 ust. 1 lit. a rozporządzenia 2016/679). Brak określenia sposobu weryfikacji i jej celu również wpływa na możliwość ustalenia celu i sposobu przetwarzania danych osobowych, o ile znajdą się w treści dokumentów.	**Uwaga nieuwzględniona** Wskazano pod jakim kątem będzie odbywała się weryfikacja dokumentów. Pełne określenie zakresu dokumentów nie jest możliwe, gdyż poszczególne europejskie programy certyfikacji mogą wprowadzać różne rodzaje dokumentów związanych z certyfikacją.

TABELA ZGODNOŚCI				
TYTUŁ PROJEKTU	ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)			
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO	rozporządzenie 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)			
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU	Termin wejścia w życie uwzględnia konieczność podjęcia niezbędnych działań przez krajowy organ certyfikacji cyberbezpieczeństwa oraz zapewnienia odpowiedniego czasu dla podmiotów, których te przepisy dotyczą, na dostosowanie się do nich. Pierwszy europejski program certyfikacji cyberbezpieczeństwa stosuje się od 27 lutego 2025 r.			
lp.	**jed. red. aktu o cyberbezpieczeństwie**	**treść przepisu UE**	**jednostka redakcyjna ustawy**	**treść przepisu/przepisów projektu ustawy**
1.	art. 2 pkt 12–15	12) „produkt ICT” oznacza element lub grupę elementów sieci lub systemów informatycznych; 13) „usługa ICT” oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych; 14) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT; 14a) „usługa zarządzana w zakresie bezpieczeństwa” oznacza usługę świadczoną osobie trzeciej, polegającą na prowadzeniu lub zapewnianiu pomocy dla działań związanych z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa, takich jak postępowanie w przypadku incydentu, testy penetracyjne, audyty bezpieczeństwa i doradztwo w ramach wsparcia technicznego, w tym doradztwo fachowe;	art. 2 pkt 1, 17, 18, 22 i 23	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 nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylającym rozporządzenie (EWG) nr 339/93 (Dz. Urz. UE L 218 z 13.08.2008, str. 30 z późn. zm.), zwanego dalej „rozporządzeniem 765/2008”; (…) 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; (…) 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.

		15) „akredytacja” oznacza akredytację zgodnie z definicją w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008;		
2.	art. 2 pkt 8	8) „cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób;	art. 2 pkt 4	Art. 2. Użyte w ustawie określenia oznaczają: (…) 4) cyberzagrożenie – cyberzagrożenie, o którym mowa w art. 2 pkt 8 rozporządzenia 2019/881;
3.	art. 2 pkt 17 i 18	17) „ocena zgodności” oznacza ocenę zgodności zgodnie z definicją w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008; 18) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność zgodnie z definicją w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008;	art. 2 pkt 11 i 15	Art. 2. Użyte w ustawie określenia oznaczają: (…) 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; (…) 15) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;
4.	art. 46	1. Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienia zharmonizowanego podej-ścia na poziomie unijnym do europejskich programów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego rynku cyfrowego w zakresie produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa. 2. Europejskie ramy certyfikacji cyberbezpieczeństwa przewidują mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności lub poufności	art. 1, art. 3, art. 5 i art. 16	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 tego systemu, kontroli działalności tych podmiotów oraz koordynacji ich działalności. 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; 3) zapewnienie:

		przechowywanych, przekazywanych lub przetwarzanych danych, lub funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Potwierdza on ponadto, że usługi zarządzane w zakresie bezpieczeństwa, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności i poufności danych, do których uzyskuje się dostęp, lub które są przetwarzane, przechowywane lub przekazywane w związku ze świadczeniem tych usług, oraz że usługi te są świadczone w sposób ciągły z zachowaniem wymaganych kompetencji, wiedzy fachowej i doświadczenia przez personel o wystarczającym i odpowiednim poziomie odpowiedniej wiedzy technicznej i uczciwości zawodowej.		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. 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 mające 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 w procesie certyfikacji 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. 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.
5.	art. 56 ust. 6	6. W przypadku gdy europejski program certyfikacji cyberbezpieczeństwa przyjęty na podstawie art. 49 wymaga poziomu uzasadnienia zaufania „wysoki”, europejski certyfikat cyberbezpieczeństwa wydawany w ramach tego programu może być wydany wyłącznie przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – w następujących przypadkach – przez jednostkę oceniającą zgodność: a) po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa każdego europejskiego certyfikatu cyberbezpieczeństwa wydanego przez daną jednostkę oceniającą zgodność; lub b) na podstawie ogólnego powierzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność.	art. 22	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 zawartych 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. 9. Minister właściwy do spraw informatyzacji nie ponosi odpowiedzialności za szkody wywołane wydaniem decyzji, o której mowa w ust. 5.
6.	art. 58 ust. 1–6	1. Każde państwo członkowskie wyznacza na swoim terytorium przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – za zgodą innego państwa członkowskiego – wyznacza przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa ustanowiony na terytorium tego innego państwa członkowskiego jako organ odpowiedzialny za zadania związane z nadzorem w wyznaczającym państwie członkowskim. 2. Każde państwo członkowskie informuje Komisję o wyznaczonych krajowych organach ds. certyfikacji cyberbezpieczeństwa, a w przypadku gdy państwo członkowskie wyznacza więcej niż jeden organ, informuje	art. 4, art. 18, art. 35 i art. 39	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;

		ono również Komisję o zadaniach powierzonych każdemu z tych organów. 3. Bez uszczerbku dla art. 56 ust. 5 lit. a) i art. 56 ust. 6 każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa pozostaje niezależny od jednostek, nad którymi sprawuje nadzór, w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji. 4. Państwa członkowskie zapewniają, by działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, była ściśle oddzielona od ich działalności związanej z nadzorem określonej w niniejszym artykule i by oba rodzaje tej działalności były wykonywane niezależnie od siebie. 5. Państwa członkowskie zapewniają, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa posiadały odpowiednie zasoby na potrzeby wykonywania swoich uprawnień i wywiązywania się ze swoich zadań w skuteczny i wydajny sposób. 6. W celu skutecznego wdrożenia niniejszego rozporządzenia zasadnym jest, aby organy te uczestniczyły w pracach ECCG w aktywny, skuteczny, wydajny i bezpieczny sposób.		5) wyrażanie zgody na wydanie europejskich certyfikatów cyberbezpieczeństwa 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; 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) przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa; 13) nadzorowanie stosowania zawartych 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 został wydany europejski 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. 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) przygotowanie 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 zawartymi 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 dokonywania 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) opracowanie i walidację procesów badawczych; 7) przygotowanie 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 do 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: 1) przygotowanie 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 dokonywania 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) opracowanie i walidację procesów badawczych; 7) przygotowanie 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 do 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. 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 utrzymanie 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. 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 … o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. …).”. Art. 39. 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 przekroczenia 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 których mowa w ust. 2, oraz odpowiedzialnym za wdrożenie mechanizmów korygujących, o których mowa w ust. 3, jest minister właściwy do spraw gospodarki.
7.	art. 58 ust. 7 lit. a–d	7. Krajowe organy ds. certyfikacji cyberbezpieczeństwa: a) nadzorują i egzekwują stosowanie zawartych w europejskich programach certyfikacji bezpieczeństwa na podstawie art. 54 ust. 1 lit. j) zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z wymogami europejskich certyfikatów cyberbezpieczeństwa wydanych na ich terytoriach, we współpracy z innymi odpowiednimi organami nadzoru rynku; b)monitorują wykonywanie obowiązków wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, którzy mają siedzibę na ich terytorium i którzy przeprowadzają ocenę zgodności przez stronę pierwszą, oraz egzekwują	art. 4, art. 17, art. 23 i art. 27	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;

		takie obowiązki, w szczególności monitorują wykonywanie obowiązków takich wytwórców lub dostawców, które określono w art. 53 ust. 2 i 3 i w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa, oraz egzekwują takie obwiązki; c) bez uszczerbku dla art. 60 ust. 3 aktywnie wspomagają i wspierają krajowe jednostki akredytujące w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia; d) monitorują i nadzorują działalność podmiotów publicznych, o których mowa w art. 56 ust. 5;		5) wyrażanie zgody na wydanie europejskich certyfikatów cyberbezpieczeństwa 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; 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) przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa; 13) nadzorowanie stosowania zawartych 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 został wydany europejski 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. 17. 1. Akredytacji jednostki 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 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179). 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, przy uwzględnieniu 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. 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. 27. 1. Minister właściwy do spraw informatyzacji w ramach nadzoru, o którym mowa w art. 4 ust. 2 pkt 1, może wystąpić do podmiotów, o których mowa w art. 3 ust. 2 pkt 3–6, z wnioskiem o przedstawienie 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.
8.	art. 58 ust. 7 lit. e	e) w stosownych przypadkach zezwalają na działalność jednostek oceniających zgodność, zgodnie z art. 60 ust. 3, oraz ograniczają, zawieszają lub cofają istniejące zezwolenia, jeżeli jednostki oceniające zgodność naruszają wymogi niniejszego rozporządzenia;	art. 4 ust. 2 pkt 7 oraz art. 19	Art. 4. 2. Do zadań ministra właściwego do spraw informatyzacji należy: (…) 7) prowadzenie postępowań w sprawie zezwoleń, o których mowa w art. 19; 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. 5. Minister właściwy do spraw informatyzacji z urzędu, w drodze decyzji, cofa albo zawiesza 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: 1) naruszenie, o którym mowa w ust. 5, nie występowało w ciągu ostatnich 3 lat, nie było związane z popełnieniem przestępstwa ani nie podważa zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa; 2) naruszenie, o którym mowa w ust. 5, jest odwracalne. 7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na czas określony, 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 zgodności certyfikacji z danym europejskim programem 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 otrzymania opinii 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) 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.
9.	art. 58 ust. 7 lit. f	f) rozpatrują skargi osób fizycznych lub prawnych dotyczące europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa, europejskich certyfikatów cyberbezpieczeństwa wydanych przez jednostki	art. 25 i art. 26	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

		oceniające zgodność zgodnie z art. 56 ust. 6 lub unijnych deklaracji zgodności wydanych na podstawie art. 53 oraz badają w odpowiednim zakresie przedmiot takich skarg i informują skarżącego w rozsądnym terminie o postępach i wynikach badania;		zawartych w danym europejskim programie certyfikacji cyberbezpieczeństwa; 2) jednostkę oceniającą zgodność prowadzącą ocenę produktów ICT, usług ICT, procesów ICT 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 i 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.
10.	art. 58 ust. 7 lit. g	g) przedkładają ENISA i ECCG roczne sprawozdanie z działań przeprowadzonych na podstawie lit. b), c) i d) niniejszego ustępu lub na podstawie ust. 8;	art. 4 ust. 1 i ust. 2 pkt 8	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: (…) 8) przekazywanie Agencji Unii Europejskiej do spraw 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;
11.	art. 58 ust. 7 lit. h	h) współpracują z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa z wymogami niniejszego rozporządzenia	art. 4 ust. 1 i ust. 2 pkt 4	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: (…) 4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji;

		lub z wymogami określonych europejskich programów certyfikacji cyberbezpieczeństwa;		
12.	art. 58 ust. 7 lit. i	i) monitorują odpowiednie zmiany w dziedzinie certyfikacji cyberbezpieczeństwa.	art. 4 ust. 1	Art. 4. 1. Minister właściwy do spraw informatyzacji jest krajowym organem do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881.
13.	art. 58 ust. 8 lit. a	8. Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa ma co najmniej następujące uprawnienia do: a) żądania od jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz podmiotów, które wydały unijne deklaracje zgodności przekazania wszelkich informacji, których organ ten potrzebuje do wykonywania swoich zadań;	art. 27	Art. 27. 1. Minister właściwy do spraw informatyzacji w ramach nadzoru, o którym mowa w art. 4 ust. 2 pkt 1, może wystąpić do podmiotów, o których mowa w art. 3 ust. 2 pkt 3–6, z wnioskiem o przedstawienie 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.
14.	art. 58 ust. 8 lit. b–d	b) prowadzenia postępowań, w formie audytów, w stosunku do jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i	art. 28–32	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

		podmiotów, które wydały unijne deklaracje zgodności, w celu weryfikacji przestrzegania przez nie niniejszego tytułu; c) stosowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia, by jednostki oceniające zgodność, posiadacze europejskich certyfikatów cyberbezpieczeństwa i podmioty, które wydały unijne deklaracje zgodności przestrzegali niniejszego rozporządzenia lub zachowywali zgodność z danym europejskim programem certyfikacji cyberbezpieczeństwa; d) uzyskania dostępu do pomieszczeń jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa do celów prowadzenia postępowań zgodnie z prawem procesowym Unii lub państwa członkowskiego;		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, 1222 i 1871 oraz z 2025 r. poz. 222) 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 zawarte 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) wielkość 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 zawartych 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 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.

				3. Decyzję o zawieszeniu europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, wydaje się na czas określony, nie dłuższy niż 6 miesięcy. 4. W przypadku przywrócenia zgodności z wymogami zawartymi 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, system zarządzania cyberbezpieczeństwem lub osoba fizyczna, dla których wydano europejski certyfikat albo krajowy certyfikat, nie spełniają wymogów zawartych w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa, a w przypadku systemu zarządzania cyberbezpieczeństwem lub osób fizycznych – nie spełniają wymogów zawartych w danym krajowym schemacie certyfikacji cyberbezpieczeństwa, informuje o tym podejrzeniu jednostkę oceniającą zgodność, która wydała europejski certyfikat albo krajowy certyfikat.
15.	art. 58 ust. 8 lit. e	e) cofnięcia, zgodnie z prawem krajowym, europejskich certyfikatów cyberbezpieczeństwa wydanych przez krajowe organy ds. certyfikacji cyberbezpieczeństwa lub europejskich certyfikatów cyberbezpieczeństwa wydanych przez jednostki oceniające zgodność zgodnie z art. 56 ust. 6, jeżeli certyfikaty te nie są zgodne z niniejszym rozporządzeniem lub z europejskim programem certyfikacji cyberbezpieczeństwa;	art. 4 ust. 1 i art. 22	Art. 4. 1. Minister właściwy do spraw informatyzacji jest krajowym organem do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881. 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 zawartych 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. 9. Minister właściwy do spraw informatyzacji nie ponosi odpowiedzialności za szkody wywołane wydaniem decyzji, o której mowa w ust. 5.

16.	art. 58 ust. 8 lit. f	f) nakładania kar zgodnie z prawem krajowym, jak przewidziano w art. 65, oraz żądania natychmiastowego zaprzestania naruszeń obowiązków określonych w niniejszym rozporządzeniu.	art. 4 ust. 1 i ust. 2 pkt 1, art. 33 i art. 34	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; (…) Art. 33. 1. Jednostka oceniająca zgodność, która będąc do tego obowiązana, nie przekazuje danych, o których mowa w art. 23 ust. 1, lub przekazuje nieprawdziwe lub niekompletne 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 przeprowadzanie 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 unijna 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.
17.	art. 58 ust. 9	9. Krajowe organy ds. certyfikacji cyberbezpieczeństwa współpracują ze sobą i z Komisją, w szczególności wymieniając informacje, doświadczenie i dobre praktyki odnoszące się do certyfikacji cyberbezpieczeństwa i kwestii technicznych dotyczących cyberbezpieczeństwa	art. 4 ust. 1 i ust. 2 pkt 4	Art. 4. 1. Minister właściwy do spraw informatyzacji pełni funkcję krajowego organu do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881. 2. Do zadań ministra właściwego do spraw informatyzacji należy: (…)

		produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.		4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji; (…)
18.	art. 59	1. W celu uzyskania równoważnych norm w całej Unii w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności krajowe organy ds. certyfikacji cyberbezpieczeństwa podlegają wzajemnemu przeglądowi. 2. Wzajemny przegląd przeprowadza się w oparciu o rzetelne i przejrzyste kryteria i procedury oceny, w szczególności w odniesieniu do wymagań dotyczących struktury, zasobów ludzkich i procedur, poufności i skarg. 3. W ramach wzajemnego przeglądu ocenia się: a) w stosownych przypadkach – czy działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, jest ściśle oddzielona od działalności związanej z nadzorem określonej w art. 58 i czy te działalności są wykonywane niezależnie od siebie; b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z europejskimi certyfikatami cyberbezpieczeństwa na podstawie art. 58 ust. 7 lit. a); c) procedury nadzorowania i egzekwowania obowiązków wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa na podstawie art. 58 ust. 7 lit. b); d) procedury monitorowania, wydawania zezwoleń na działalność i nadzorowania działalności jednostek oceniających zgodność; e) w stosownych przypadkach – czy członkowie personelu organów i jednostek wydających certyfikaty o poziomie uzasadnienia zaufania „wysoki” zgodnie z art. 56 ust. 6 mają odpowiednią wiedzę fachową.	art. 4 ust. 1 i ust. 2 pkt 3	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: (…) 3) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;

		4. Wzajemny przegląd musi być przeprowadzany przez co najmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisję i musi być przeprowadzany co najmniej raz na pięć lat. ENISA może uczestniczyć we wzajemnym przeglądzie. 5. Komisja może przyjmować akty wykonawcze ustanawiające plan wzajemnego przeglądu obejmujący okres co najmniej pięciu lat, ustanawiające kryteria dotyczące składu zespołu ds. wzajemnego przeglądu, metodykę wykorzystywaną do wzajemnego przeglądu, harmonogram, częstotliwość oraz inne zadania związane z wzajemnym przeglądem. Przyjmując te akty wykonawcze, Komisja należycie uwzględnia stanowisko ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2. 6. Wyniki wzajemnych przeglądów analizuje ECCG, która sporządza podsumowania, które można podawać do wiadomości publicznej, i która, w razie potrzeby, wydaje wytyczne lub zalecenia dotyczące działań lub środków, jakie mają podjąć zainteresowane podmioty.		
19.	art. 60 ust. 1 i 2	1. Jednostki oceniające zgodność są akredytowane przez krajowe jednostki akredytujące wyznaczone na podstawie rozporządzenia (WE) nr 765/2008. Akredytacji takiej udziela się jedynie wtedy, gdy jednostki oceniające zgodność spełniają wymagania określone w załączniku do niniejszego rozporządzenia. 2. W przypadku gdy europejski certyfikat cyberbezpieczeństwa wydawany jest przez krajowy organ ds. certyfikacji cyberbezpieczeństwa na podstawie art. 56 ust. 5 lit. a) i art. 56 ust. 6, jednostkę certyfikującą krajowego organu ds. certyfikacji cyberbezpieczeństwa akredytuje się jako jednostkę oceniającą zgodność na podstawie ust. 1 niniejszego artykułu.	art. 17	Art. 17. 1. Akredytacji jednostki 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 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179). 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, przy uwzględnieniu 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.
20.	art. 60 ust. 3	3. W przypadku gdy europejskie programy certyfikacji cyberbezpieczeństwa określają szczególne lub dodatkowe wymogi zgodnie z art. 54 ust. 1 lit. f), krajowy organ ds. certyfikacji cyberbezpieczeństwa może zezwolić na wykonywanie zadań w ramach takich programów wyłącznie takim jednostkom oceniającym zgodność, które spełniają te wymogi.	art. 19–21	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. 5. Minister właściwy do spraw informatyzacji z urzędu, w drodze decyzji, cofa albo zawiesza 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: 1) naruszenie, o którym mowa w ust. 5, nie występowało w ciągu ostatnich 3 lat, nie było związane z popełnieniem przestępstwa ani nie podważa zaufania do krajowego systemu certyfikacji cyberbezpieczeństwa; 2) naruszenie, o którym mowa w ust. 5, jest odwracalne. 7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na czas określony, 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 zgodności certyfikacji z danym europejskim programem 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 otrzymania opinii 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) 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.
21.	art. 60 ust. 4	4. Akredytacji, o której mowa w ust. 1, udziela się jednostkom oceniającym zgodność na maksymalnie pięć lat i można ją odnowić na tych samych warunkach, o ile	art. 5 i art. 17	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

		jednostka oceniająca zgodność nadal spełnia wymogi określone w niniejszym artykule. Krajowe jednostki akredytujące podejmują, w odpowiednich ramach czasowych, wszelkie stosowne środki w celu ograniczenia, zawieszenia lub cofnięcia akredytacji jednostki oceniającej zgodność udzielonej na podstawie ust. 1, w przypadku gdy warunki udzielenia akredytacji nie zostały spełnione, przestały być spełnione lub gdy jednostka oceniająca zgodność narusza niniejsze rozporządzenie.		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 mające 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 w procesie certyfikacji 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. 17. 1. Akredytacji jednostki 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 2022 r. poz. 1854, z 2024 r. poz. 1089 oraz z 2025 r. poz. 179). 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, przy uwzględnieniu 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.
22.	art. 62	1. Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („ECCG”). 2. W skład ECCG wchodzą przedstawiciele krajowych organów ds. certyfikacji cyberbezpieczeństwa lub przedstawiciele innych odpowiednich organów krajowych. Członek ECCG nie może reprezentować więcej niż dwóch państw członkowskich. 3. Interesariusze i odpowiednie strony trzecie mogą być zapraszani na posiedzenia ECCG i do udziału w jej pracach. 4. ECCG ma następujące zadania: a) doradzanie i pomaganie Komisji przy pracach nad zapewnieniem spójnego wprowadzania i stosowania niniejszego tytułu, w szczególności w odniesieniu do unijnego kroczącego programu prac, kwestii związanych z polityką certyfikacji cyberbezpieczeństwa, koordynacji koncepcji politycznych oraz przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa;	art. 4 ust. 2 pkt 9	Art. 4. 2. Do zadań ministra właściwego do spraw informatyzacji należy: 9) uczestniczenie w pracach Europejskiej Grupy do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) na podstawie art. 58 ust. 6 rozporządzenia 2019/881; (…)

		b) pomaganie, doradzanie i współpracowanie z ENISA w związku z przygotowywaniem propozycji programu na podstawie art. 49; c) wydawanie opinii na temat propozycji programu przygotowanej przez ENISA na podstawie art. 49 niniejszego rozporządzenia; d) zwracanie się do ENISA z wnioskiem o przygotowanie propozycji programu na podstawie art. 48 ust. 2; e) wydawanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa; f) monitorowanie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk odnoszących się do programów certyfikacji cyberbezpieczeństwa; g) ułatwianie współpracy pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa w ramach niniejszego tytułu poprzez budowanie zdolności, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa; h) wspieranie w zakresie wdrażania mechanizmów wzajemnej oceny zgodnie z zasadami ustanowionymi w danym europejskim programie certyfikacji cyberbezpieczeństwa na podstawie art. 54 ust. 1 lit. u); i) ułatwianie dostosowywania europejskich programów cyberbezpieczeństwa do międzynarodowo uznanych norm, w tym przez dokonywanie przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa i, w stosownych przypadkach, wydawanie skierowanych do ENISA zaleceń dotyczących podjęcia współpracy z odpowiednimi międzynarodowymi organizacjami normalizacyjnymi w celu wyeliminowania		

		braków lub luk w istniejących międzynarodowo uznanych normach. 5. Komisja, z pomocą ENISA, przewodniczy ECCG i zapewnia ECCG obsługę sekretariatu, zgodnie z art. 8 ust. 1 lit. e).		
23.	art. 63	1. Osoby fizyczne i prawne mają prawo do wniesienia skargi do podmiotu, który wydał europejski certyfikat cyberbezpieczeństwa lub, w przypadku gdy skarga dotyczy europejskiego certyfikatu cyberbezpieczeństwa wydanego przez jednostkę oceniającą zgodność, działającą zgodnie z art. 56 ust. 6 – do odpowiedniego krajowego organu ds. certyfikacji cyberbezpieczeństwa. 2. Organ lub jednostka, do których wniesiono skargę, informuje skarżącego o stanie postępowania i podjętej decyzji, a także informuje skarżącego o prawie do skutecznego środka prawnego przed sądem, o którym mowa w art. 64.	art. 24	Art. 24. 1. Każdy może złożyć skargę do jednostki oceniającej zgodność 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 załatwienia skargi.
24.	art. 65	Państwa członkowskie ustanawiają przepisy o karach nakładanych w przypadku naruszenia niniejszego tytułu i naruszenia europejskich programów certyfikacji cyberbezpieczeństwa oraz stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie niezwłocznie powiadamiają Komisję o tych przepisach i środkach, a następnie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy.	art. 33 i art. 34	Art. 33. 1. Jednostka oceniająca zgodność, która będąc do tego obowiązana, nie przekazuje danych, o których mowa w art. 23 ust. 1, lub przekazuje nieprawdziwe lub niekompletne 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 przeprowadzanie 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 unijna 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.

ODWRÓCONA TABELA ZGODNOŚCI			
projekt ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)			
lp.	**jed. red. projektu**	**treść przepisu**	**uzasadnienie wprowadzenia przepisu**
1.	art. 2 pkt 13	Art. 2. Użyte w ustawie określenia oznaczają: (…) 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 publiczny, mających zastosowanie do certyfikacji systemów zarządzania cyberbezpieczeństwem albo osób fizycznych w zakresie cyberbezpieczeństwa;	Przepis ten definiuje krajowe schematy certyfikacji cyberbezpieczeństwa. Pojęcie to będzie obejmowało krajowe programy cyberbezpieczeństwa zdefiniowane w rozporządzeniu 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), zwanym dalej „rozporządzeniem 2019/881", a także analogiczne dokumenty dotyczące osób oraz systemów zarządzania cyberbezpieczeństwem. Takie rozwiązanie jest zgodne z rozporządzeniem 2019/881 w zakresie, w jakim odnosi się ono do krajowych schematów certyfikacji cyberbezpieczeństwa. Rozporządzenie to odnosi się do nich tylko w kontekście programów dotyczących produktów ICT, usług ICT i procesów ICT, które są również objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa. W takim wypadku krajowe programy certyfikacji cyberbezpieczeństwa odnoszące się do tych produktów ICT, usług ICT oraz procesów ICT przestają działać, a państwo nie może przyjmować nowych programów. W związku z tym wprowadzenie krajowych schematów certyfikacyjnych odnoszących się do osób oraz systemów zarządzania cyberbezpieczeństwem nie będzie w żaden sposób kolidowało z przepisami rozporządzenia 2019/881 w tym zakresie, gdyż będą one dotyczyły innych obszarów merytorycznych.
2.	art. 6	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.	Przepis ten wprowadza podstawę do prowadzenia oceny zgodności na podstawie krajowych schematów certyfikacji cyberbezpieczeństwa. Będzie ona odbywała się na takich samych zasadach, jak ocena zgodności w ramach europejskich programów cyberbezpieczeństwa, tj. będzie całkowicie dobrowolna oraz będzie odbywała się na podstawie umowy cywilnoprawnej między zainteresowanym dostawcą, a jednostką oceniającą zgodność. Jednostka oceniająca zgodność będzie musiała być akredytowana przez Polskie

		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 warunkach wskazanych w umowie 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 mające 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	Centrum Akredytacji. Należy podkreślić, że rozporządzenie 2019/881 pozwala na funkcjonowanie krajowych schematów certyfikacji obok europejskich programów certyfikacji tak długo, jak ich zakresy pozostają rozbieżne. Dzięki temu będzie możliwa certyfikacja w ramach krajowych schematów certyfikacyjnych. Takie rozwiązanie jest zgodne z rozporządzeniem 2019/881 w zakresie, w jakim odnosi się ono do krajowych programów cyberbezpieczeństwa. Rozporządzenie to odnosi się do nich tylko w kontekście programów dotyczących produktów ICT, usług ICT i procesów ICT, które są również objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa. W takim wypadku krajowe programy odnoszące się do tych produktów ICT, usług ICT oraz procesów ICT przestają działać, a państwo nie może przyjmować nowych programów. W związku z tym wprowadzenie krajowych programów certyfikacyjnych odnoszących się do osób oraz systemów zarządzania cyberbezpieczeństwem nie będzie w żaden sposób kolidowało z przepisami rozporządzenia 2019/881 w tym zakresie gdyż będą one dotyczyły innych obszarów merytorycznych.

		handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także ochrony praw własności intelektualnej.	
3.	art. 7	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.	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym ogólnych wymagań do wydania certyfikatu. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.
4.	art. 8	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.	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym ogólnego katalogu czynności przeprowadzanych w ramach badania, czy przedmiot certyfikacji spełnia wymogi określone w programie certyfikacji. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.

5.	art. 9	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 podmiotu dokonującego certyfikacji oraz wskazanie adresu jego 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 zgodnie z art. 15 ust. 1.	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym treści certyfikatów wydawanych w ramach takich schematów. Nie ma potrzeby określania tej kwestii dla europejskich certyfikatów cyberbezpieczeństwa, gdyż będzie to określone w rozporządzeniach wykonawczych Komisji. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.
6.	art. 10	Art. 10. 1. Krajowy certyfikat jest wydawany na okres nie krótszy niż 2 lata i nie dłuższy niż 5 lat. 2. Krajowy certyfikat może zostać przedłużony na wniosek: 1) dostawcy, 2) osoby fizycznej, która poddała swoją wiedzę i swoje umiejętności praktyczne ocenie zgodności, 3) podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności – w przypadku gdy produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym treści certyfikatów wydawanych w ramach takich schematów. Nie ma potrzeby określania tej kwestii dla europejskich certyfikatów cyberbezpieczeństwa, gdyż będzie to określone w rozporządzeniach wykonawczych Komisji. Nie wpływa to na implementację przepisów rozporządzenia 2019/881. W związku z wprowadzeniem krajowych schematów certyfikacyjnych konieczne jest określenie na poziomie ustawowym maksymalnego okresu, na jaki może być wydany certyfikat, oraz zasad jego przedłużania. W przypadku europejskich programów certyfikacji te kwestie będą uregulowane w rozporządzeniach wykonawczych Komisji. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.

		cyberbezpieczeństwem lub osoba fizyczna nadal spełniają wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa. 3. Podmiot, o którym mowa w ust. 2, składa wniosek o przedłużenie ważności krajowego certyfikatu w terminie co najmniej 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 osoby fizyczne, o których 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.	
7.	art. 11	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.	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa wprowadzany jest obowiązek zagwarantowania, że produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna spełniają odpowiednie wymogi przez cały okres, na jaki został wydany certyfikat. Jest to konieczne dla zapewnienia, aby certyfikaty pełniły swoją funkcję. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.
8.	art. 12	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 związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym obowiązku przekazywania informacji przez posiadacza certyfikatu do jednostki oceniającej zgodność. Jest to niezbędne dla zapewnienia realnej kontroli, że wymogi spełnione są przez cały okres, na jaki certyfikat został wydany. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.

		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.	
9.	art. 13	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 z zapewnieniem bezpieczeństwa i ochrony tajemnic handlowych i innych informacji poufnych, w tym tajemnic przedsiębiorstwa, a także zapewnieniem ochrony 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 i dane osoby zatwierdzającej protokół. Protokoły	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym maksymalnego okresu przechowywania dokumentacji technicznej związanej z certyfikowanymi wyrobami. W przypadku europejskich programów certyfikacji te kwestie będą uregulowane w rozporządzeniach wykonawczych Komisji. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.

		brakowania dokumentacji są przechowywane przez jednostki oceniające zgodność.	
10.	art. 14	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.	W związku z wprowadzeniem krajowych schematów certyfikacji cyberbezpieczeństwa konieczne jest określenie na poziomie ustawowym procedury stosowanej w przypadku gdy przedmiot certyfikacji przestaje spełniać wymogi już po uzyskaniu krajowego certyfikatu. Nie wpływa to na implementację przepisów rozporządzenia 2019/881.

		5. Jednostka oceniająca zgodność powiadamia ministra właściwego do spraw informatyzacji o cofnięciu krajowego certyfikatu.	
11.	art. 15	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 lub osób fizycznych podlegających 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;	Przepis ten pozwoli ministrowi właściwemu do spraw informatyzacji przyjmować krajowe schematy certyfikacji cyberbezpieczeństwa w drodze rozporządzeń. Przy tworzeniu ww. schematów minister będzie mógł korzystać z pomocy nadzorowanych przez niego państwowych instytutów badawczych oraz innych podmiotów, posiadających specjalistyczną wiedzę. Ze względu na to, że krajowe schematy certyfikacji cyberbezpieczeństwa mogą dotyczyć różnych obszarów, nie da się na tym etapie określić, jaka dokładnie wiedza będzie niezbędna. Należy wyraźnie podkreślić, że ocena zgodności w ramach krajowych schematów certyfikacji cyberbezpieczeństwa będzie całkowicie dobrowolna, a więc nie nakładają one obowiązków na podmioty, które dobrowolnie nie poddadzą się ocenie zgodności.

		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.	
12.	art. 36	Art. 36. 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… o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. …);”.	Przedmiotowy przepis ma służyć zapewnieniu spójności systemu prawa. Projektowany art. 34 ust. 3 przesądził, że przychód z kar nałożonych na podstawie art. 33 stanowi przychód Funduszu Cyberbezpieczeństwa. W związku z tym konieczne jest zapewnienie spójności przepisu przez wskazanie tego źródła przychodu 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).
13.	art. 37 i art. 38	Art. 37. 1. Akredytacje udzielone przez Polskie Centrum Akredytacji jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie niniejszej ustawy stają się akredytacjami w rozumieniu niniejszej ustawy. 2. W terminie 14 dni od dnia wejścia w życie niniejszej ustawy Polskie Centrum Akredytacji informuje ministra właściwego do spraw	W związku z przyjęciem przepisów o krajowych schematach certyfikacji cyberbezpieczeństwa konieczne było ustalenie reguł intertemporalnych dla akredytacji i certyfikatów.

		informatyzacji o udzielonych akredytacjach, o których mowa w ust. 1. Art. 38. 1. Certyfikaty wydane w ramach akredytacji, o której mowa w art. 37, obowiązują do końca terminu ich ważności. Do tych certyfikatów stosuje się przepisy dotychczasowe. 2. W terminie 14 dni od dnia wejścia w życie niniejszej 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.	

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia

w sprawie krajowego schematu certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo

Na podstawie art. 15 ust. 1 i 3 ustawy z dnia ……. r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. 1. Określa się krajowy schemat certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo, stanowiący załącznik nr 1 do rozporządzenia.

2. Określa się wzór graficzny krajowego certyfikatu stanowiący załącznik nr 2 do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie po upływie 14 dni od dnia ogłoszenia.

MINISTER CYFRYZACJI

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 18 grudnia 2023 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 2720).

Załączniki
do rozporządzenia
Ministra Cyfryzacji
z dnia
(Dz. U. poz. …)

Załącznik nr 1

Firma Bezpieczna Cyfrowo – krajowy schemat certyfikacji cyberbezpieczeństwa

1. Cel schematu

Niniejszy krajowy schemat certyfikacji cyberbezpieczeństwa stosuje się do prowadzenia oceny, certyfikacji oraz nadzoru nad certyfikatem wydanym w ramach krajowego schematu certyfikacji – Firma Bezpieczna Cyfrowo, zwanym dalej „certyfikatem FBC".

Celem niniejszego schematu certyfikacji jest określenie zasad przebiegu certyfikacji systemu zarządzania cyberbezpieczeństwem w małych i średnich przedsiębiorstwach, zwanych dalej „MŚP", przez niezależną ocenę zgodności z wymogami określonymi w tym schemacie.

Certyfikat FBC wydany dla MŚP jest poświadczeniem, że system zarządzania cyberbezpieczeństwem w danym podmiocie spełnia wymogi określone w niniejszym schemacie certyfikacji.

Zakłada się, że przedsiębiorstwo, które uzyskało certyfikat FBC, wdrożyło dobre praktyki i spełnia podstawowe wymogi z obszaru zarządzania cyberbezpieczeństwem, w szczególności:

1) utworzyło i aktualizuje rejestr aktywów;
2) wdrożyło i prowadzi politykę dostępu i bezpiecznych haseł;
3) wdrożyło wymagane przez schemat certyfikacji zabezpieczenia techniczne przed cyberzagrożeniami i atakami z internetu;
4) wprowadziło politykę tworzenia kopii zapasowych;
5) prawidłowo wykorzystuje środki identyfikacji elektronicznej oraz bezpiecznie korzysta z usług cyfrowych.

2. Definicje

1) klient – organizacja lub osoba odpowiedzialna wobec jednostki oceniającej zgodność za zapewnienie, że wymogi certyfikacyjne są spełnione;

2) ocena – niezależny, udokumentowany proces uzyskiwania dowodów, w celu określenia stopnia spełnienia wymogów, stanowiących kryteria certyfikacji;
3) organizacja (firma) –podmiot ubiegający się o uzyskanie certyfikatu;
4) system informatyczny – zestaw elementów sprzętu (hardware), programów (software), danych i użytkowników, które w połączeniu zapewniają możliwość przechowywania, transmisji, przetwarzania i odtwarzania informacji;
5) umowa – umowa o świadczenie usług certyfikacyjnych zawarta między jednostką oceniającą zgodność, a klientem, która obejmuje wykonanie przez jednostkę oceniającą zgodność na zlecenie klienta usług certyfikacyjnych.

3. Szczegółowe wymogi systemu zarządzania cyberbezpieczeństwem

3.1. Zabezpieczenie brzegowe (Firewall)

3.1.1. Organizacja zapewnia ochronę informacji w sieciach. Sieci są zarządzane i nadzorowane w celu zapewnienia bezpieczeństwa informacji w systemach i aplikacjach.

3.1.2. Organizacja zapewnia dostęp uprawnionym użytkownikom i zapobiega nieuprawnionemu dostępowi do systemów i usług przez zdefiniowanie konfiguracji zabezpieczeń dla sprzętu, oprogramowania, usług (np. usług w chmurze) i sieci, zarówno dla nowo zainstalowanych systemów, jak i dla eksploatowanych systemów przez cały okres ich użytkowania.

3.1.3. Organizacja zapewnia bezpieczeństwo usług sieciowych gwarantując, że wszystkie usługi sieciowe świadczone wewnętrznie lub zewnętrznie zawierają zidentyfikowane i właściwie skonfigurowane mechanizmy zabezpieczeń, określony poziom świadczenia usług oraz udokumentowane wymogi dotyczące zarządzania.

3.1.4. Organizacja zapewnia bezpieczeństwo usług sieciowych oraz skutecznie zapobiega nieuprawnionemu dostępowi do systemów i usług przez zdefiniowane konfiguracje zabezpieczeń dla sprzętu, oprogramowania i sieci.

3.1.5. Organizacja ustanawia, dokumentuje, zatwierdza, wdraża i nadzoruje zasady konfiguracji zabezpieczeń dla sprzętu, oprogramowania i sieci zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji.

3.1.6. Organizacja ustanawia, dokumentuje, zatwierdza, wdraża i nadzoruje zasady zarządzania zmianami konfiguracji zabezpieczeń dla sprzętu, oprogramowania i sieci zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji.

3.2. Bezpieczna konfiguracja

3.2.1. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji. Użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali uprawienia. Przyznane uprawnienia są odbierane lub dostosowywane do zaistniałych zmian w organizacji.

3.2.2. Organizacja ustanawia proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Domyślne informacje uwierzytelniające, predefiniowane lub dostarczone przez dostawców, są zmieniane natychmiast po instalacji systemów lub oprogramowania.

3.2.3. Organizacja ustanawia zasady instalacji oprogramowania i usług, zapewniając wyłączenie lub usunięcie zbędnego, niewykorzystywanego oprogramowania i usług (w tym aplikacji, narzędzi systemowych i usług sieciowych).

3.2.4. Organizacja wyłącza wszelkie funkcje automatycznego uruchamiania plików podczas pobierania, które umożliwiają wykonanie pliku bez autoryzacji użytkownika.

3.2.5. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

3.2.6. Organizacja zapewnia kontrolę dostępu i chroni urządzenia przed nieuprawnionym dostępem.

3.3. Zarządzanie aktualizacjami

3.3.1. Organizacja określa istotne wymogi prawne, regulacyjne, umowne oraz dotyczące łańcucha dostaw produktów w celu wdrożenia procesu zarządzania oprogramowaniem i wsparciem technicznym.

3.3.2. Organizacja określa istotne wymogi prawne, regulacyjne, umowne oraz dotyczące łańcucha dostaw produktów w celu wyłączenia lub usunięcia zbędnego, niewykorzystywanego lub niewspieranego oprogramowania i usług (w tym aplikacji, narzędzi systemowych i usług sieciowych).

3.3.3. Organizacja określa zasady zarządzania podatnościami technicznymi i podejmuje odpowiednie działania w celu przeciwdziałania materializacji ryzyka z tym związanego.

3.3.4. Organizacja określa zasady zarządzania podatnościami technicznymi o wysokim ryzyku lub krytycznym znaczeniu i podejmuje odpowiednie działania w celu przeciwdziałania materializacji ryzyka z tym związanego.

3.4. Kontrola dostępu użytkowników

3.4.1. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

3.4.2. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

3.4.3. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Użytkownicy mają dostęp wyłącznie do tych sieci i usług sieciowych, do których otrzymali uprawienia. Przyznane uprawnienia są odbierane lub dostosowywane do zaistniałych zmian w organizacji.

3.4.4. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Organizacja zapewnia kontrolę dostępu do urządzeń poprzez procedurę bezpiecznego logowania.

3.4.5. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników. Organizacja zapewnia zarządzanie prawami uprzywilejowanego dostępu.

3.4.6. Organizacja ustanawia i dokumentuje politykę kontroli dostępu zgodnie z wymogami biznesowymi i wymogami bezpieczeństwa informacji oraz ustanawia politykę haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem

użytkowników. Organizacja zapewnia zarządzanie prawami uprzywilejowanego dostępu. Organizacja monitoruje i regularnie przegląda prawa uprzywilejowanego dostępu.

3.5. Ochrona przed złośliwym oprogramowaniem

3.5.1. Organizacja wdraża ochronę przed złośliwym oprogramowaniem, w połączeniu ze szkoleniami użytkowników.

3.5.2. Organizacja zapewnia regularne, zgodnie z zaleceniami dostawcy, aktualizowanie zainstalowanego oprogramowania antywirusowego w celu zachowania jego ciągłej skuteczności do wykrywania złośliwego oprogramowania.

3.5.3. Organizacja wdraża listy dozwolonych aplikacji, zasady i mechanizmy kontrolne, które zapobiegają instalacji i uruchomieniu nieautoryzowanego oprogramowania, a także zapewnia konfigurację oprogramowania antywirusowego uniemożliwiającą uruchomienie złośliwego oprogramowania.

3.5.4. Organizacja wdraża zasady i mechanizmy kontrolne, które chronią przed ryzykiem instalacji i uruchomieniem złośliwego kodu dostarczanego poprzez sieć zewnętrzną lub na jakimkolwiek nośniku.

3.5.5. Organizacja wdraża mechanizmy kontrolne, które zapobiegają lub wykrywają korzystanie ze znanych lub podejrzanych złośliwych stron internetowych (np. listy blokowania), a także zapewnia skanowanie stron internetowych w poszukiwaniu złośliwego kodu i oprogramowania, po uzyskaniu do nich dostępu, w celu ochrony użytkownika.

3.6. Tworzenie kopii zapasowych danych

Organizacja chroni przed utratą danych poprzez regularne wykonywanie kopii zapasowych informacji, zgodnie z ustaloną polityką wykonywania kopii zapasowych.

3.7. Usługi cyfrowe i identyfikacja w sieci

3.7.1. Organizacja chroni dane podczas transmisji i spoczynku.

3.7.2. Organizacja wykorzystuje mechanizmy identyfikacji (rozpoznawania i uwierzytelniania użytkowników) w sieci w celu bezpiecznego dostępu do usług cyfrowych.

4. Szczegółowe metody oceny systemu zarządzania cyberbezpieczeństwem

W ramach oceny spełnienia wymogów określonych w pkt 3 jednostka oceniająca zgodność:

1) analizuje polityki bezpieczeństwa stosowane w danej organizacji;
2) bada środki techniczne i organizacyjne stosowane w celu spełnienia wymogów, o których mowa w pkt 3;
3) bada realne wykonanie polityk bezpieczeństwa;
4) analizuje informacje przekazane od klienta.

5. Szczegółowe warunki wydawania, utrzymywania i przedłużania certyfikatu

5.1. Jednostka oceniająca zgodność wydaje certyfikat, jeżeli spełnione są wszystkie następujące warunki:

1) przedmiot certyfikacji wchodzi w zakres akredytacji jednostki oceniającej zgodność;
2) wnioskodawca ubiegający się o certyfikację podpisał oświadczenie zawierające wszystkie zobowiązania wymienione w pkt 5.2;
3) jednostka oceniająca zgodność zakończyła ocenę bez zastrzeżeń zgodnie z normami, kryteriami i metodami oceny.

5.2. Wnioskodawca ubiegający się o certyfikację zobowiązuje się:

1) dostarczyć jednostce certyfikującej wszelkie niezbędne kompletne i prawidłowe informacje, a na żądanie jednostki certyfikującej dostarczyć dodatkowe niezbędne informacje;
2) nie promować swojego systemu jako posiadający certyfikat FBC, zanim certyfikat nie zostanie wydany;
3) natychmiast zaprzestać promowania swojego systemu zarządzania cyberbezpieczeństwem jako certyfikowanego w przypadku cofnięcia lub wygaśnięcia certyfikatu FBC.

5.3. System zarządzania cyberbezpieczeństwem musi spełniać wymogi przez cały okres ważności certyfikatu.

5.4. Jednostka oceniająca zgodność przedłuża certyfikat na wniosek posiadacza certyfikatu.

5.5. Posiadacz certyfikatu załącza do wniosku, o którym mowa w pkt 5.4, posiadane dokumenty potwierdzające dalsze spełnianie wymogów.

5.6. W przypadku gdy przekazane dokumenty nie wystarczą do oceny, czy przedmiot certyfikacji spełnia wymogi określone w schemacie, jednostka oceniająca zgodność może

ponownie przeprowadzić ocenę spełnienia tych wymogów zgodnie z art. 7 ust. 1 ustawy z dnia…… o krajowym systemie certyfikacji cyberbezpieczeństwa.

6. Szczegółowy sposób monitorowania zgodności systemu zarządzania cyberbezpieczeństwem z wymogami cyberbezpieczeństwa

6.1. Jednostka oceniająca monitoruje:

1) wykonywanie przez posiadaczy certyfikatu obowiązków spoczywających na nich na podstawie rozporządzenia i ustawy z dnia……..o krajowym systemie certyfikacji cyberbezpieczeństwa;
2) zgodność certyfikowanych przez nią systemów zarządzania cyberbezpieczeństwem z wymogami bezpieczeństwa.

6.2. Jednostka oceniająca podejmuje działania monitorujące na podstawie:

1) informacji dostarczonych na podstawie zobowiązań wnioskodawcy, wynikających z zawartej umowy, ubiegającego się o certyfikację, o których mowa w pkt 5.2;
2) informacji otrzymanych od krajowego organu do spraw certyfikacji cyberbezpieczeństwa;
3) informacji wynikających z działań właściwych organów nadzoru rynku;
4) otrzymanych skarg.

6.3. Posiadacz certyfikatu udostępnia jednostce oceniającej zgodność informacje niezbędne do oceny, czy certyfikowany system zarządzania cyberbezpieczeństwem nadal spełnia wymogi określone w schemacie.

6.4. W przypadku, gdy z otrzymanych informacji wynika, że certyfikowany system zarządzania cyberbezpieczeństwem nie spełnia wymogów określonych w schemacie, jednostka oceniająca zgodność może ponownie przeprowadzić ocenę spełnienia tych wymogów zgodnie z art. 7 ust. 1 ustawy z dnia …….o krajowym systemie certyfikacji cyberbezpieczeństwa.

7. Dokumentacja techniczna

7.1. Dokumentacja dotycząca bezpieczeństwa usług sieciowych, w tym zatwierdzone i wdrożone zasady konfiguracji zabezpieczeń dla sprzętu, oprogramowania i sieci.

7.2. Dokumentacja określająca politykę kontroli dostępu do informacji w tym polityka haseł, proces przydzielania informacji uwierzytelniających i zarządzania dostępem użytkowników.

7.3. Dokumentacja określająca listy dozwolonych aplikacji, zasady i mechanizmy kontrolne zapobiegające instalacji i uruchomieniu nieautoryzowanego oprogramowania, a także konfigurację oprogramowania antywirusowego uniemożliwiającą uruchomienie złośliwego oprogramowania.

8. Okres dostępności dokumentacji technicznej

Dokumentacja techniczna dotycząca certyfikacji systemu zarządzania cyberbezpieczeństwem przechowywana jest przez okres 5 lat od dnia wygaśnięcia certyfikatu.

Załącznik nr 2

WZÓR

CERTYFIKAT

zgodności systemu zarządzania cyberbezpieczeństwem z wymogami krajowego schematu certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo

……
(oznaczenie podmiotu, który otrzymał certyfikat)

……..
(nazwa podmiotu dokonującego certyfikacji)

…….
(oznaczenie np. produktu ICT podlegającego certyfikacji)

……..
(numer lub oznaczenie certyfikatu)

……..
(oznaczenie krajowego schematu, w ramach którego został wydany certyfikat)

……
(okres, na jaki został wydany certyfikat)

…….. ……..
(data) (podpis)

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 15 ust. 1 i 3 ustawy z dnia …… r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. …), zwanej dalej „ustawą”, i określa krajowy schemat certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo.

Firma Bezpieczna Cyfrowo to schemat certyfikacji cyberbezpieczeństwa systemów zarządzania cyberbezpieczeństwem przeznaczony dla przedsiębiorców. Jego celem jest podnoszenie świadomości cyfrowych i cyberbezpieczeństwa wśród małych i średnich firm, a także upowszechnienie i wdrożenie standardu cyberbezpieczeństwa dla firm w Polsce.

Cyberbezpieczeństwo to jeden z podstawowych wymogów pomyślnego rozwoju społecznego i ekonomicznego, jest to warunek konieczny do funkcjonowania państwa i nowoczesnej gospodarki. Wielu polskich przedsiębiorców zdaje sobie sprawę z wagi tematu i stara się zapewnić bezpieczeństwo swoich produktów poprzez korzystanie z certyfikowanych wyrobów IT, wszechstronnie przetestowanych i spełniających międzynarodowe normy. Są oni przykładem dobrych praktyk, które należy powielać.

W miarę postępującej cyfryzacji biznesu, ryzyko cyberataków stale wzrasta. Ważna jest świadomość tych zagrożeń oraz posiadanie wiedzy i umiejętności potrzebnych do efektywnego przeciwdziałania.

W dzisiejszych czasach większość firm korzysta z urządzeń podłączonych do internetu, takich jak smartfony i komputery, oraz usług cyfrowych, takich jak poczta e-mail, strony internetowe, czy handel elektroniczny.

Certyfikat wydawany w ramach niniejszego schematu będzie stanowił dowód dojrzałości przedsiębiorcy w obszarze cyberbezpieczeństwa i będzie jasnym sygnałem dla jego kontrahentów, że ich dane są odpowiednio chronione.

Zakres oceny w ramach Firmy Bezpiecznej Cyfrowo obejmuje infrastrukturę informatyczną używaną do prowadzenia biznesu. Są to wszystkie urządzenia, które mają dostęp do danych w przedsiębiorstwach, takich jak służbowe wiadomości e-mail, dane klientów, strona internetowa, usługi online oraz informacje, do których uzyskuje się dostęp zdalnie w chmurze.

Dzięki odpowiednim środkom zabezpieczającym i dobrym praktykom w dziedzinie cyberbezpieczeństwa, można znacząco zminimalizować ryzyko incydentów związanych z naruszeniem bezpieczeństwa.

Rozwiązania w zakresie monitorowania wydanych certyfikatów zagwarantują, że jednostka oceniająca zgodność będzie mogła wykryć przypadki niezgodności z wymogami i zareagować na nie.

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2025 r. poz. 468).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Wejście w życie rozporządzenia nie będzie miało wpływu na działalność mikroprzedsiębiorców, małych i średnich przedsiębiorców.

Projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535).

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie krajowego schematu certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo **Ministerstwo wiodące i ministerstwa współpracujące** **Ministerstwo Cyfryzacji** **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **…….** **Kontakt do opiekuna merytorycznego projektu** **……..**	**Data sporządzenia** **…….** **Źródło:** art. 15 ust. 1 i 3 ustawy z dnia ……. r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz. U. poz. ...) **Nr w wykazie prac ……..**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 15 ust. 1 i 3 ustawy z dnia …… r. o krajowym systemie certyfikacji cyberbezpieczeństwa, zwanej dalej „ustawą”, i określa krajowy schemat certyfikacji cyberbezpieczeństwa – Firma Bezpieczna Cyfrowo.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Firma Bezpieczna Cyfrowo to schemat certyfikacji cyberbezpieczeństwa systemów zarządzania cyberbezpieczeństwem przeznaczony dla przedsiębiorców. Jego celem jest podnoszenie świadomości cyfrowych i cyberbezpieczeństwa wśród małych i średnich firm, a także upowszechnienie i wdrożenie standardu cyberbezpieczeństwa dla firm w Polsce.

Cyberbezpieczeństwo to jeden z podstawowych wymogów pomyślnego rozwoju społecznego i ekonomicznego, jest to warunek konieczny do funkcjonowania państwa i nowoczesnej gospodarki. Wielu polskich przedsiębiorców zdaje sobie sprawę z wagi tematu i stara się zapewnić bezpieczeństwo swoich produktów przez korzystanie z certyfikowanych wyrobów IT, wszechstronnie przetestowanych i spełniających międzynarodowe normy. Są oni przykładem dobrych praktyk, które należy powielać. Zakres oceny w ramach Firmy Bezpiecznej Cyfrowo obejmuje infrastrukturę informatyczną używaną do prowadzenia biznesu. Są to wszystkie urządzenia, które mają dostęp do danych w przedsiębiorstwach, takich jak służbowe wiadomości e-mail, dane klientów, strona internetowa, usługi online oraz informacje, do których uzyskuje się dostęp zdalnie w chmurze.

Certyfikat wydawany w ramach niniejszego schematu będzie stanowił dowód dojrzałości przedsiębiorcy w obszarze cyberbezpieczeństwa i będzie jasnym sygnałem dla jego kontrahentów, że ich dane są odpowiednio chronione.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Przedsiębiorcy z branży IT	131 000	Informacja ogólnodostępna	Pozytywne. Uzyskają dostęp do certyfikatów obowiązujących w całej Unii Europejskiej. Przepisy ułatwią też rozwój własnych kompetencji w obszarze certyfikacji.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie przekazany do konsultacji publicznych i opiniowania, co najmniej z 10-dniowym terminem na zgłaszanie uwag.
Stosownie do postanowień art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248 oraz z 2024 r. poz. 1535), projekt zostanie udostępniony w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji. Ponadto zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2024 r. poz. 806), projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.
Szczegółowe omówienie konsultacji publicznych i opiniowania zostaną przedstawione w raporcie z konsultacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i							

	średnich przedsiębiorstw	
	rodzina, obywatele oraz gospodarstwa domowe	
Niemierzalne		
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń		

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy
Komentarz:	

9. Wpływ na rynek pracy

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	x☐ informatyzacja ☐ zdrowie
Omówienie wpływu		

11. Planowane wykonanie przepisów aktu prawnego

Rozporządzenie wejdzie w życie po upływie 14 dni od dnia ogłoszenia.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak.