Ustawa o Krajowym Systemie Certyfikacji Cyberbezpieczeństwa

Cyberpolicy NASK

Autorzy:

- Emilia Zalewska-Czajczyńska
- Paulina Popow
- Piotr Słowiński

NASK-PIB **NIP:** 521 04 17 157 nask@nask.pl
ul. Kolska 12 **Regon:** 010464542 +48 22 380 82 00
01–045 Warszawa **KRS:** 0000012938 +48 22 380 82 01 nask.pl

NASK

Spis treści

1. Wstęp

28 lipca opublikowana została ustawa z 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa. Zgodnie ze wskazanym w treści vacatio legis ustawa weszła w życie 28 sierpnia 2025 r. Zgodnie z założeniami krajowy system certyfikacji cyberbezpieczeństwa, oparty na unijnym Akcie o cyberbezpieczeństwie, umożliwia wprowadzenie dobrowolnych certyfikatów dla produktów i usług ICT, które będą uznawane w całej UE. Wzmocni tym samym ochronę przed cyberzagrożeniami, zwiększy bezpieczeństwo produktów oraz usług, a także przetwarzanych przez nie danych i ułatwi podmiotom funkcjonowanie na wspólnym rynku.

2. Przedmiot regulacji i definicje

Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa (KSCC) określa ramy prawne dla funkcjonowania systemu certyfikacji w Polsce. Jej głównym celem jest zapewnienie spójnych i przejrzystych zasad weryfikacji bezpieczeństwa produktów, usług oraz procesów ICT, a także wskazanie określenie zasad i obowiązków podmiotów tworzących system certyfikacji oraz sposób nadzoru tych podmiotów i koordynacji ich działań. Tym samym ustawa realizuje dwa równoległe cele:

- organizację krajowego systemu certyfikacji cyberbezpieczeństwa, w tym ustanowienie procedur niezbędnych do zapewnienia prawidłowego i jednolitego przebiegu procesów certyfikacyjnych;
- ustanowienie mechanizmów nadzoru i kontroli nad przestrzeganiem przepisów ustawy oraz zasad funkcjonowania systemu certyfikacji.

Wprowadzenie przepisów jest podyktowane koniecznością zapewnienia zgodności z unijnym Aktem o cyberbezpieczeństwie. W art. 2 ustawy zawarte są definicje podstawowych pojęć, na których opiera się funkcjonowanie krajowego systemu certyfikacji cyberbezpieczeństwa

Tabela 1. Wybór najistotniejszych definicji z ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa

Pojęcie	Definicja
produkt ICT	każde urządzenie, oprogramowanie lub komponent służący do przetwarzania, przechowywania lub przesyłania danych;
usługa ICT	usługi świadczone w oparciu o technologie teleinformatyczne, w tym usługi chmurowe, hostingowe, komunikacyjne czy platformowe.

	Certyfikacja obejmuje nie tylko same produkty, lecz również sposób ich wykorzystania;
proces ICT	zestaw działań lub procedur wykonywanych z użyciem technologii ICT;
europejski program certyfikacji cyberbezpieczeństwa	zestaw przepisów, wymagań technicznych, norm oraz procedur ustanowionych na poziomie Unii Europejskiej, służący ocenie zgodności i certyfikacji wybranych produktów, usług i procesów z obszaru ICT, a także usług zarządzanych w zakresie bezpieczeństwa;
krajowy program certyfikacji cyberbezpieczeństwa	zbiór krajowych regulacji, wymagań technicznych, standardów i procedur opracowanych oraz zatwierdzonych przez właściwy organ publiczny, służących certyfikacji lub ocenie zgodności produktów ICT, usług ICT, procesów ICT oraz zarządzanych usług bezpieczeństwa objętych zakresem danego programu.

3. Struktura krajowego systemu certyfikacji

Ustawa określa także strukturę krajowego systemu certyfikacji cyberbezpieczeństwa oraz rolę organów państwa w tym zakresie. Minister właściwy do spraw informatyzacji (dalej w tekście również jako ,,minister") pełni funkcję **krajowego organu ds. certyfikacji cyberbezpieczeństwa**. Oznacza to sprawowanie nadzoru i kontroli nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa, a także współpracę z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, ale również z europejskimi organami, takimi jak Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz Europejska Grupa do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG).

Kolejnym organem, który ma wskazane zadanie w ramach ustawy, jest Polskie Centrum Akredytacji. Ono z kolei jest odpowiedzialne za nadzór nad jednostkami oceniającymi zgodność w zakresie przyznanej akredytacji, obejmujący obszar danego europejskiego programu certyfikacji cyberbezpieczeństwa lub krajowego schematu certyfikacji cyberbezpieczeństwa.

W skład struktury krajowego systemu certyfikacji wchodzą również inne podmioty zaangażowane w proces certyfikacji. Należą do nich **jednostki odpowiedzialne za ocenę zgodności** oraz **dostawcy,** którzy podlegają ocenie zgodności swoich produktów ICT, usług ICT, procesów ICT lub zarządzanych usług w zakresie bezpieczeństwa zgodnie z wymaganiami europejskich programów certyfikacji lub krajowych schematów certyfikacji cyberbezpieczeństwa.

Ponadto system obejmuje **osoby fizyczne**, których wiedza i praktyczne umiejętności są oceniane w ramach krajowego schematu certyfikacji cyberbezpieczeństwa, a także **podmioty**, które podlegają ocenie zgodności stosowanych przez siebie systemów zarządzania cyberbezpieczeństwem zgodnie z krajowym schematem certyfikacji cyberbezpieczeństwa.

3.1. Zasady oceny zgodności oraz rola jednostek oceniających zgodność

Głównym zadaniem jednostek oceniających zgodność jest prowadzenie oceny 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. Na tej podstawie wydawany jest europejski lub krajowy certyfikat.

W ustawie określono zasady oceny zgodności produktów ICT, usług ICT, procesów ICT oraz systemów zarządzania cyberbezpieczeństwem w ramach europejskiego i krajowego schematu certyfikacji cyberbezpieczeństwa. Ocena zgodności odbywa się na podstawie umowy zawartej między dostawcą (lub odpowiednim podmiotem), a jednostką oceniającą zgodność.

W przypadku **europejskiego programu certyfikacji**, ocena obejmuje produkty ICT, usługi ICT, procesy ICT oraz usługi zarządzania cyberbezpieczeństwem, a certyfikat jest wydawany zgodnie z poziomami uzasadnienia zaufania określonymi w Akcie o cyberbezpieczeństwie. Umowa reguluje zakres certyfikacji, szczegóły programu, poziom zaufania oraz obowiązki stron, ze szczególnym uwzględnieniem ochrony tajemnic handlowych, innych informacji poufnych oraz praw własności intelektualnej.

Krajowy schemat certyfikacji obejmuje szerszy zakres oceny zgodności, uwzględniając nie tylko produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa, ale także systemy zarządzania cyberbezpieczeństwem oraz wiedzę i umiejętności praktyczne osób fizycznych z obszaru cyberbezpieczeństwa. Również w tym przypadku ocena opiera się na umowie określającej szczegóły dotyczące zakresu certyfikacji, obowiązków stron oraz ochrony poufnych informacji i praw własności intelektualnej.

3.2. Krajowy certyfikat

Krajowy certyfikat może zostać wydany, jeżeli oceniany produkt ICT, usługa ICT, proces ICT, usługa zarządzania w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem zapewniają odpowiedni poziom ochrony danych i usług, tj. dostępność, autentyczność, integralność oraz poufność. Certyfikat może zostać również przyznany osobie fizycznej, o ile posiada ona wiedzę i praktyczne umiejętności niezbędne do realizacji zadań z zakresu cyberbezpieczeństwa.

Sposób weryfikacji spełnienia wymagań zależny jest od rodzaju certyfikowanego podmiotu. W przypadku produktów, usług, procesów czy systemów zarządzania cyberbezpieczeństwem stosuje się różne metody: **analizę dokumentacji technicznej, audyty** oraz **badania konkretnych właściwości**. Natomiast w przypadku osób fizycznych przeprowadza się **testy teoretyczne i praktyczne** w celu potwierdzenia wiedzy i umiejętności praktycznych.

Krajowe certyfikaty muszą zawierać:

- informacje identyfikujące podmiot, który go uzyskał, a w przypadku osoby fizycznej, jej dane osobowe;
- nazwę jednostki oceniającej zgodność, która wydała krajowy certyfikat;
- oznaczenie produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem, które podlegają certyfikacji;
- w przypadku osoby fizycznej zakres certyfikacji;
- oznaczenie krajowego schematu certyfikacji cyberbezpieczeństwa, w ramach którego został wydany;
- okres, na jaki certyfikat został przyznany;
- datę wydania certyfikatu oraz podpis osoby reprezentującej podmiot dokonujący certyfikacji.

Certyfikat wydawany jest na od 2 do 5 lat i może zostać przedłużony, jeśli dany produkt, usługa, system lub osoba nadal spełniają wymogi określone w odpowiednim schemacie certyfikacji. Wniosek o przedłużenie musi zostać złożony co najmniej miesiąc przed upływem ważności certyfikatu. Wymagane jest także przedstawienie dokumentacji potwierdzającej spełnianie warunków certyfikacji, a w przypadku osób fizycznych ponowne sprawdzenie ich kompetencji.

Zgodnie przepisami ustawy utrzymanie zgodności jest obowiązkiem certyfikowanego podmiotu przez cały okres ważności certyfikatu. Oznacza to konieczność ciągłego spełniania szczegółowych wymogów technicznych i organizacyjnych określonych w krajowym schemacie certyfikacji cyberbezpieczeństwa.

3.3. Obowiązki posiadacza krajowego certyfikatu

Posiadacz krajowego certyfikatu musi zapewnić, że spełnia wymogi określone w danym krajowym schemacie certyfikacji cyberbezpieczeństwa przez cały okres ważności certyfikatu. Jednostka oceniająca zgodność może zażądać od niego informacji i dokumentów, które ten stan potwierdzają. Ponadto powinien przekazywać do jednostki oceniającej zgodność wszelkie informacje istotne z punktu widzenia spełniania tych wymogów, takie jak wykrycie podatności w certyfikowanym produkcie, usłudze lub procesie.

W sytuacji, gdy jednostka oceniająca zgodność stwierdzi, że wymogi określone w danym krajowym schemacie certyfikacji przestały być spełnione, informuje o tym posiadacza certyfikatu i zwraca się o przedstawienie propozycji działań zaradczych. Ma on **14 dni na ich zaproponowanie i przekazanie**, a jeżeli zostaną one zaakceptowane, posiadacz certyfikatu ma **2 miesiące na ich zrealizowanie i usunięcie niezgodności**. Rezultat wspomnianych działań jest następnie weryfikowany przez jednostkę oceniającą zgodność.

Jeżeli posiadacz krajowego certyfikatu nie przedstawi w wymaganym terminie propozycji działań naprawczych, nie usunie niezgodność lub uniemożliwi weryfikację działań zaradczych, jednostka oceniająca zgodność cofa certyfikat.

3.4. Rola ministra właściwego do spraw informatyzacji

Ustawa przyznaje szereg kompetencji ministrowi . Przede wszystkim pełni on funkcję **krajowego organu do spraw certyfikacji cyberbezpieczeństwa**. W ramach niej wykonuje takie zadania, jak m. in.:

- nadzór nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa oraz przeprowadzanie ich kontroli;
- monitorowanie spełniania przez jednostki oceniające zgodność wymogów określonych w Akcie o cyberbezpieczeństwie;
- przygotowywanie krajowych schematów certyfikacji cyberbezpieczeństwa;
- wyrażanie zgody na wydanie europejskich certyfikatów o poziomie uzasadnienia zaufania „wysoki;
- rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez nie działań w ramach europejskich programów certyfikacji cyberbezpieczeństwa;
- przeprowadzanie lub zlecanie badań produktu ICT, usługi ICT, procesu ICT, usługi zarządzanej w zakresie bezpieczeństwa lub systemu zarządzania cyberbezpieczeństwem, dla których zostały wydane odpowiednio deklaracja zgodności albo europejski lub krajowy certyfikat;
- prowadzenie współpracy na poziomie unijnym, w tym uczestniczenie w pracach Europejskiej Grupy do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) i przeprowadzanie wzajemnych przeglądów z organami ds. certyfikacji z innych krajów członkowskich.

W przypadku, gdy dany europejski program certyfikacji cyberbezpieczeństwa zawiera szczegółowe lub dodatkowe wymogi dla jednostek oceniających zgodność w zakresie ich kwalifikacji technicznych do oceny wymogów cyberbezpieczeństwa, minister ma kompetencję do wydania zezwolenia na wykonywanie przez daną jednostkę czynności w ramach oceny zgodności. Jest ono wydawane w drodze decyzji, na wniosek jednostki oceniającej zgodność, jeżeli spełnia ona wymogi określone w programie i posiada odpowiednią akredytację. Minister może z urzędu cofnąć lub zawiesić takie zezwolenie, jeżeli jednostka naruszy przepisy Aktu o cyberbezpieczeństwie, ustawy lub danego europejskiego programu certyfikacji cyberbezpieczeństwa.

Dodatkowo minister określa **krajowe schematy certyfikacji** w drodze rozporządzenia, zawiera ono:

- szczegółowe wymogi dla produktów, usług, procesów, usług zarządzanych w zakresie bezpieczeństwa, systemów zarządzania cyberbezpieczeństwem podlegających ocenie zgodności lub osób fizycznych, których wiedza i umiejętności podlegają ocenie zgodności;
- szczegółowe metody stosowane w celu wykazania spełnienia takich wymogów;
- szczegółowy sposób monitorowania zgodności z wymogami;
- szczegółowe warunki wydawania, utrzymywania i przedłużania ważności krajowych certyfikatów;
- szczegółowy zakres dokumentacji technicznej dotyczącej certyfikacji, okres oraz sposób jej przechowywania i niszczenia;
- okres, na jaki jest wydawany krajowy certyfikat;
- wzór certyfikatu.

Wydając rozporządzenie minister powinien uwzględnić szereg różnych czynników, w zależności od tego, czego dotyczy dany krajowy schemat certyfikacji. W przypadku produktów, usług, procesów i usług zarządzanych będzie to np. ich funkcja i wpływ na funkcjonowanie systemów teleinformatycznych, a osób fizycznych – odpowiednie przygotowanie i zakres wiedzy niezbędny do skutecznej realizacji zadań z zakresu cyberbezpieczeństwa.

3.5. Rola Polskiego Centrum Akredytacji

Polskie Centrum Akredytacji (PCA) wydaje akredytacje jednostkom oceniającym zgodność w zakresie określonego europejskiego programu certyfikacji cyberbezpieczeństwa albo krajowego schematu certyfikacji cyberbezpieczeństwa. Jest ona wydawana na okres nie dłuższy niż 5 lat.

PCA informuje ministra o każdej wydanej akredytacji w terminie 14 dni, wskazując przy tym, jakiej jednostce oceniającej zgodność dotyczy, jaki jest jej zakres, data wydania i okres ważności oraz numer i oznaczenie certyfikatu akredytacji. Analogicznie, Polskie Centrum Akredytacji informuje ministra o odmowie, cofnięciu, zawieszeniu lub ograniczeniu zakresu akredytacji.

Ponadto PCA pełni funkcję nadzorczą w zakresie udzielonej akredytacji nad jednostkami oceniającymi zgodność w obszarze objętym danym europejskim programem certyfikacji cyberbezpieczeństwa albo danym krajowym schematem certyfikacji cyberbezpieczeństwa.

3.6. Rola państwowych instytutów badawczych

Państwowe instytuty badawcze, które podlegają nadzorowi ministra, pełnią w krajowym systemie certyfikacji przede wszystkim funkcje doradcze i wspierające. Do ich zadań należy m. in.:

- przygotowywanie opinii, ekspertyz i analiz;

- weryfikacja dokumentów pochodzących od podmiotów krajowego systemu certyfikacji pod kątem zgodności z wymogami określonymi w Akcie o cyberbezpieczeństwie, ustawie oraz danym europejskim programie lub krajowym schemacie certyfikacji;
- przeprowadzanie badań produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa lub systemów zarządzania cyberbezpieczeństwem, w tym dokonywanie określonych czynności z zakresu oceny zgodności;
- publikacja wykazów specyfikacji technicznych, norm i standardów;
- udział w pracach międzynarodowych grup normalizacyjnych z zakresu cyberbezpieczeństwa;
- opracowywanie i walidacja procesów badawczych;
- przygotowywanie projektów krajowych schematów certyfikacji cyberbezpieczeństwa;
- organizowanie porównań międzylaboratoryjnych lub badań biegłości w danym europejskim programie lub krajowym schemacie certyfikacji;
- weryfikacja, czy dana osoba fizyczna posiada odpowiednie kwalifikacje techniczne i zawodowe, doświadczenie w realizacji zadań z zakresu oceny zgodności, wiedzę z zakresu cyberbezpieczeństwa, uprawnienia do przeprowadzania oceny zgodności w ramach danego europejskiego programu lub krajowego schematu certyfikacji.

Dany instytut badawczy nie może realizować powyższych zadań, jeżeli uczestniczył w procesie certyfikacji, których te czynności dotyczą.

Państwowe instytuty badawcze powinny rozwijać swój potencjał badawczo-rozwojowy oraz zdolności w obszarze oceny zgodności i certyfikacji, aby móc realizować powyższe działania. W szczególności powinny to robić poprzez utrzymywanie stałej sprawności operacyjnej oraz pozyskiwanie i utrzymywanie ekspertów. Minister może udzielić im dotacji celowej z części budżetu państwa, której jest dysponentem.

Wymienione wyżej zadania minister może także, w uzasadnionych przypadkach, zlecić podmiotom innym niż państwowe instytuty badawcze, jeżeli dysponują odpowiednią wiedzą i kompetencjami.

4. Uprawnienia nadzorcze ministra właściwego do spraw informatyzacji

Minister pełni centralną rolę w nadzorze nad krajowym systemem certyfikacji cyberbezpieczeństwa, posiadając szeroki zakres uprawnień weryfikacyjnych, decyzyjnych i kontrolnych. Jego działania obejmują zarówno nadzór nad procesem certyfikacji, jak i bezpośrednią kontrolę nad podmiotami.

4.1. Nadzór nad procesem certyfikacji i wydawaniem certyfikatów

Minister posiada kluczowe uprawnienia nadzorcze nad procesem certyfikacji, w szczególności w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa. Może on, w drodze decyzji, wyrazić zgodę na wydanie europejskiego certyfikatu. Cały proces rozpoczyna się od przeprowadzenia certyfikacji. Po jego zakończeniu, jednostka oceniająca zgodność przesyła do Ministra, drogą elektroniczną, wniosek o zgodę na wydanie europejskiego certyfikatu. Termin na złożenie wniosku wynosi maksymalnie 14 dni od dnia zakończenia certyfikacji. Wniosek ten musi zawierać wskazanie produktu ICT, usługi ICT, procesu ICT albo usługi zarządzanej w zakresie bezpieczeństwa, które podlegały certyfikacji, oraz europejskiego programu certyfikacji cyberbezpieczeństwa, w ramach którego przeprowadzono certyfikację. Do wniosku należy dołączyć raport z certyfikacji.

Obowiązek ten dotyczy certyfikatów odwołujących się do poziomu uzasadnienia zaufania "wysoki" – czyli takiego, który zgodnie z unijnym aktem o cyberbezpieczeństwie daje uzasadnione zaufanie, że produkty ICT, usługi ICT i procesy ICT, dla których wydany został ten certyfikat, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności w zakresie bezpieczeństwa, oraz zostały ocenione na poziomie, który minimalizuje ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach i dysponujących znaczącymi zasobami.

Odmowa wydania zgody następuje w przypadku naruszenia przepisów aktu o cyberbezpieczeństwie, ustawy lub danego europejskiego programu certyfikacji cyberbezpieczeństwa w ramach certyfikacji. Ponadto Minister ma także prawo cofnąć europejski certyfikat, jeżeli został on wydany niezgodnie z przepisami lub jeżeli certyfikowany produkt, usługa, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa.

4.2. Obowiązki informacyjne jednostek oceniających zgodność wobec Ministra

Jednostki oceniające zgodność mają szczegółowo określone obowiązki informacyjne wobec Ministra. Nie później niż w terminie 14 dni od dnia podjęcia danego rozstrzygnięcia, mają obowiązek przekazania Ministrowi dane dotyczące dostawcy, osoby fizycznej, która poddała swoją wiedzę i umiejętności praktyczne ocenie zgodności, albo podmiotu, który poddał ocenie zgodności wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem. Przekazywane dane muszą obejmować informacje o podmiotach:

- którym wydano albo przedłużono europejski certyfikat albo krajowy certyfikat, wraz z kopią tego certyfikatu;
- którym cofnięto europejski certyfikat albo krajowy certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia;
- którym odmówiono wydania europejskiego certyfikatu albo krajowego certyfikatu, wraz ze wskazaniem przyczyn odmowy.

Dane te są szczegółowo określone –w przypadku osoby prawnej konieczne jest przekazanie nazwy (firmy), adresu siedziby, numeru we właściwym rejestrze (o ile został nadany) oraz numer identyfikacji podatkowej (NIP). Z kolei w przypadku osoby fizycznej wystarczy jej imię i nazwisko oraz numer PESEL.

Przekazywanie danych odbywa się drogą elektroniczną, a Minister przechowuje kopie europejskiego certyfikatu albo krajowego certyfikatu przez cały okres jego ważności oraz przez 5 lat po jego wygaśnięciu. W przypadku przekazania niepełnych danych, Minister wzywa jednostkę oceniającą zgodność do ich uzupełnienia w terminie 14 dni od dnia otrzymania wezwania.

4.3. Obowiązki informacyjne podmiotów wobec Ministra

W ramach sprawowanego nadzoru, Minister może wezwać do przedstawienia informacji na temat produktów, usług, procesów w zakresach objętych europejskimi lub krajowymi certyfikatami bądź deklaracjami zgodności określone rodzaje podmiotów:

- jednostki oceniające zgodność,
- dostawców poddających ocenie zgodności swoje produkty, usługi i procesy lub usługi zarządzane w zakresie bezpieczeństwa,
- osoby fizyczne, które poddają swoją wiedzę i umiejętności praktyczne ocenie zgodności,
- podmioty, które poddają wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności.

Minister może również żądać informacji o liczbie wydanych europejskich certyfikatów albo krajowych certyfikatów wraz ze wskazaniem programów lub schematów certyfikacji oraz poziomów uzasadnienia zaufania, a także o liczbie wydanych deklaracji zgodności. Dodatkowo, Minister może wymagać przekazania informacji dotyczących innych kwestii istotnych dla funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa. Termin na przekazanie informacji to 21 dni od dnia otrzymania stosownego wniosku.

4.4. Kontrole prowadzone przez Ministra

Minister, w ramach nadzoru, prowadzi kontrole jednostek oceniających zgodność, dostawców produktów, usług i procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa oraz podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności.

Do kontroli przeprowadzanych wobec dostawców będących przedsiębiorcami stosuje się przepisy Prawa przedsiębiorców oraz przepisy ustawy o krajowym systemie cyberbezpieczeństwa. Natomiast wobec dostawców niebędących przedsiębiorcami stosuje się przepisy ustawy o kontroli w administracji rządowej.

4.5. Badania produktów, usług i systemów w ramach nadzoru

W ramach kontroli minister może poddać badaniom lub zlecić ich przeprowadzenie wobec określonych elementów, urządzeń bądź rozwiązań w celu sprawdzenia, czy spełniają one wymogi europejskiego programu lub krajowego schematu certyfikacji. Badaniom podlegają:

- produkt, usługa lub proces ICT lub usługa zarządzana w zakresie bezpieczeństwa dla których został wydany europejski certyfikat albo krajowy certyfikat albo została wydana deklaracja zgodności;
- system zarządzania cyberbezpieczeństwem, dla którego został wydany krajowy certyfikat.

Badania produktów, usług i procesów ICT są prowadzone na próbkach, które dostawca jest zobowiązany przekazać. Próbką w myśl przepisów ustawy jest pojedynczy produkt ICT danego rodzaju albo jego określony element. Z jej przekazania sporządza się protokół zawierający obowiązkowo kluczowe dane, takie jak: nazwa produktu, oznaczenie certyfikatu lub wydanej deklaracji zgodności, dane identyfikacyjne (np. numer seryjny), daty oraz dane osoby przekazującej i odbierającej próbkę, a także ich podpisy. Koszty całego procesu pokrywa dostawca lub podmiot, który poddał system ocenie.

W przypadku europejskiego certyfikatu, który odnosi się do poziomu uzasadnienia zaufania „wysoki", Minister cofa certyfikat, jeżeli wykryte nieprawidłowości:

- mają znaczący wpływ na dostępność, autentyczność, integralność lub poufność danych, sieci i systemów informatycznych danego podmiotu wykorzystującego system zarządzania cyberbezpieczeństwem, lub
- mają znaczący wpływ na użytkownika produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, lub są nieodwracalne.

Natomiast Minister tylko zawiesza certyfikat, jeżeli wykryte nieprawidłowości nie mają znaczącego wpływu oraz są odwracalne. Decyzję ta wydawana jest na okres nie dłuższy niż 6 miesięcy. W przypadku przywrócenia zgodności z wymogami, Minister cofa decyzję o zawieszeniu certyfikatu w drodze decyzji. Ponadto, Minister, w przypadku uzasadnionego podejrzenia, że certyfikowany produkt ICT, usługa ICT, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoby fizyczne nie spełniają wymogów, informuje o tym podejrzeniu jednostkę oceniającą zgodność, która wydała dany certyfikat.

W przypadku, gdy badanie wykaże, że produkt, usługa czy proces ICT bądź usługa zarządzana w zakresie bezpieczeństwa nie spełniają wymogów określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa, Minister podaje o tym informację do publicznej wiadomości na swojej stronie podmiotowej w Biuletynie Informacji Publicznej.

Tabela 2. Uprawnienia nadzorcze ministra właściwego do spraw informatyzacji

Typ uprawnienia	Opis uprawnienia

Wzywanie do przedstawienia informacji	Minister może wezwać podmioty do przedstawienia informacji na temat produktów, usług, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa, a także liczby wydanych certyfikatów i deklaracji zgodności. Informacje muszą zostać przekazane w terminie 21 dni.
Prowadzenie kontroli	Minister prowadzi kontrole jednostek oceniających zgodność, dostawców produktów, usług, procesów ICT oraz podmiotów, które poddały systemy zarządzania cyberbezpieczeństwem ocenie zgodności. Do kontroli stosuje się odpowiednie przepisy prawa.
Prowadzenie lub zlecanie badań	W ramach kontroli minister może poddać badaniom lub zlecić ich przeprowadzenie w celu weryfikacji, czy spełniane są wymogi certyfikacji. Koszty badań ponosi dostawca produktu lub podmiot, który poddał system ocenie.
Przeprowadzanie badań na próbkach	Badania mogą być przeprowadzane na próbkach produktów ICT. Dostawca produktu jest zobowiązany do przekazania próbki na żądanie ministra, a z przekazania sporządza się protokół.
Podawanie do publicznej wiadomości informacji o niespełnianiu wymogów	Jeśli badanie wykaże, że produkt, usługa, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa nie spełniają wymogów, minister podaje tę informację do publicznej wiadomości w Biuletynie Informacji Publicznej.
Cofanie lub zawieszanie europejskiego certyfikatu	Minister może cofnąć certyfikat, jeśli wykryte nieprawidłowości mają znaczący wpływ na dane, sieci i systemy informatyczne lub są nieodwracalne. Może zawiesić certyfikat na okres do 6 miesięcy, jeśli nieprawidłowości są odwracalne i nie mają znaczącego wpływu.
Poinformowanie jednostki oceniającej zgodność o podejrzeniach niespełniania wymogów	W przypadku uzasadnionego podejrzenia, że produkt, usługa, proces ICT, usługa zarządzana w zakresie bezpieczeństwa, system zarządzania cyberbezpieczeństwem lub osoba fizyczna nie spełniają wymogów, minister informuje o tym jednostkę oceniającą zgodność, która wydała certyfikat.

5. Procedura skargowa w krajowym systemie certyfikacji cyberbezpieczeństwa

5.1. Skarga na działania jednostki oceniającej zgodność

Każdy podmiot ma prawo złożyć skargę na działania jednostki oceniającej zgodność, podjęte podczas procesu oceny zgodności. Jednostka ta jest zobowiązana rozpatrzyć skargę w terminie nie dłuższym niż 2 miesiące od dnia jej złożenia. Ważnym elementem zapewniającym bezstronność jest wymóg, aby skargę rozpatrywały osoby, które nie brały udziału w zaskarżonych działaniach. Ponadto jednostka oceniająca zgodność ma obowiązek publikowania na swojej stronie internetowej informacji o postępowaniu ze skargami osób fizycznych i prawnych, w tym o stanie postępowania, terminie rozpatrzenia skargi i podjętej decyzji.

Wymóg publikowania informacji o postępowaniu ze skargami oraz rozpatrywania skarg przez personel niezwiązany z pierwotnymi działaniami, których dotyczy skarga, wskazuje na dążenie do przejrzystości i bezstronności w samych jednostkach oceniających zgodność. Te przepisy są kluczowe dla zapewnienia wiarygodności i integralności pracy oraz procesów jednostki oceniającej zgodność. Odzwierciedla to najlepsze praktyki w zarządzaniu jakością i akredytacji.

5.2. Skarga na dostawcę lub jednostkę oceniającą zgodność do Ministra

Skarga składana bezpośrednio do Ministra może dotyczyć:

- dostawcy, 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;
- jednostki oceniającej zgodność prowadzącej ocenę produktów ICT, usług ICT, procesów ICT, osób fizycznych, systemów zarządzania cyberbezpieczeństwem lub usług zarządzanych w zakresie bezpieczeństwa w zakresie cyberbezpieczeństwa.

Minister rozpatruje skargi w sposób i na zasadach określonych w danym europejskim programie certyfikacji cyberbezpieczeństwa. W przypadku, gdy program certyfikacji nie określa sposobu ani zasad rozpatrywania skarg, stosuje się odpowiednio przepisy kodeksu postępowania administracyjnego. Skargę należy rozpatrzyć nie później niż w terminie 2 miesięcy od dnia jej złożenia. Ponadto każdemu, czyj interes prawny lub uprawnienie zostały naruszone przez bezczynność organu, przysługuje prawo wniesienia skargi na bezczynność organu do sądu administracyjnego.

5.3. Nakładanie, ustalanie wysokości i uiszczanie kar pieniężnych

System krajowej certyfikacji cyberbezpieczeństwa przewiduje mechanizmy nakładania kar pieniężnych za określone naruszenia przepisów, co ma na celu egzekwowanie zgodności z przepisami ustawy oraz ewentualne dyscyplinowanie podmiotów za naruszenia.

Kary pieniężne nakłada w drodze decyzji Minister właściwy do spraw informatyzacji, na co przysługuje skarga do sądu administracyjnego. Ustalając wysokość kar pieniężnych konieczne jest uwzględnienie zakresu lub charakteru naruszenia oraz dotychczasowej działalności kontrolowanego podmiotu. Wpływy z tytułu nałożonych kar stanowią przychód Funduszu Cyberbezpieczeństwa (FC) i uiszcza się je w terminie 14 dni od dnia uprawomocnienia się decyzji.

Tabela 3. Rodzaje naruszeń podlegających karom pieniężnym

Naruszenie	Naruszający	Wysokość kary pieniężnej
Brak przekazania Ministrowi danych, niepełne przekazanie lub przekazanie nieprawdziwych danych dostawcy, osoby fizycznej, która poddała swoją wiedzę i umiejętności praktyczne ocenie zgodności, albo podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności	Jednostka oceniająca zgodność	10-KROTNOŚĆ PRZECIĘTNEGO WYNAGRODZENIA
Wydanie europejskiego albo krajowego certyfikatu, działając bez wymaganej akredytacji		DO 20-KROTNOŚCI PRZECIĘTNEGO WYNAGRODZENIA
Nieprzekazanie osobom prowadzącym czynności kontrolne wskazanej przez nie próbki produktu ICT (pojedynczego produktu ICT danego rodzaju lub jego określony element)	Dostawca produktów ICT	
Nieudostępnienie krajowemu organowi ds. certyfikacji cyberbezpieczeństwa unijnej deklaracji zgodności, dokumentacji technicznej oraz wszelkich istotnych informacji związanych ze zgodnością z europejskim programem certyfikacji cyberbezpieczeństwa w terminie w nim przewidzianym	Dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa	

Uniemożliwianie lub utrudnianie Ministrowi przeprowadzenia kontroli w ramach nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa	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	
	Jednostka oceniająca zgodność	
Nieudostępnienie publicznie dodatkowych informacji na temat cyberbezpieczeństwa produktów, usług lub procesów ICT, w przypadku których została wydana unijna deklaracja zgodności	Dostawca certyfikowanych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa w ramach europejskich programów certyfikacji cyberbezpieczeństwa	
	Dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w przypadku których wydana została deklaracja zgodności	
Nieprzekazanie na wezwanie Ministra informacji dotyczących produktów, usług lub procesów dla których został wydany europejski lub krajowy certyfikat, bądź unijna deklaracja zgodności, a także na temat liczby wydanych europejskich albo krajowych certyfikatów wraz ze wskazaniem europejskich programów albo krajowych schematów certyfikacji cyberbezpieczeństwa, w ramach których zostały wydane oraz poziomów uzasadnienia zaufania	Jednostka oceniająca zgodność	
	Dostawcy, poddający 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, poddające swoją wiedzę i umiejętności praktyczne ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa	

	Podmioty poddające wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa	

6. Przepisy przejściowe i końcowe – wpływ na ekosystem cyberbezpieczeństwa

W ramach przepisów przejściowych ustawa reguluje status akredytacji i certyfikatów wydanych przed wejściem w życie ustawy. Akredytacje udzielone przez Polskie Centrum Akredytacji (PCA) jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie ustawy stają się akredytacjami w rozumieniu ustawy. W stosunku do certyfikatów wydanych przez PCA stosuje się przepisy dotychczasowe.

W terminie 14 dni od dnia wejścia w życie ustawy PCA ma obowiązek przekazać Ministrowi informacje o udzielonych akredytacjach oraz wydanych certyfikatach, dochowując jednocześnie obowiązków informacyjnych wobec europejskich lub krajowych certyfikatów na gruncie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa.

Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia tj. **28 sierpnia 2025 r.**

7. Podsumowanie i wnioski

- Ustawa tworzy kompleksowy i wielopodmiotowy krajowy system certyfikacji w obszarze cyberbezpieczeństwa, a także fundament pod rozwój krajowych schematów certyfikacji, które mogą być dostosowywane do nowych technologii i zagrożeń, zapewniając elastyczność i ciągłą aktualność systemu. Harmonizuje jednocześnie krajowe regulacje z unijnym Aktem o cyberbezpieczeństwie, co umożliwia uznawanie certyfikatów w całej UE. Zwiększa to interoperacyjność i ułatwia polskim podmiotom konkurowanie na jednolitym rynku cyfrowym.
- Wprowadzenie certyfikacji podnosi poziom bezpieczeństwa produktów i usług, co przekłada się na większe zaufanie konsumentów do producentów, jak i sektora publicznego.
- Krajowy system certyfikacji cyberbezpieczeństwa obejmuje nie tylko produkty i usługi ICT, ale także procesy, systemy zarządzania cyberbezpieczeństwem oraz kompetencje osób fizycznych. Zapewnia to bardziej kompleksowe podejście do bezpieczeństwa produktów z elementami cyfrowymi.

- Centralna rola ministra właściwego do spraw informatyzacji oraz współpraca z PCA i ENISA zapewniają wielopoziomowy nadzór. To minimalizuje ryzyko nadużyć i zwiększa transparentność procesu certyfikacji.
- Włączenie państwowych instytutów badawczych i wymóg utrzymywania ekspertów sprzyjają budowie krajowego know-how w obszarze certyfikacji i oceny zgodności.
- Stopniowana reakcja na niezgodność (publiczne ujawnienie, zawieszenie, cofnięcie w zależności od wagi i ewentualna weryfikacja oraz cofnięcie decyzji) w połączeniu z obowiązkiem informowania jednostki oceniającej zgodność wydającej certyfikat, wskazuje na strategię egzekwowania prawa opartą na ocenie ryzyka. Jednocześnie sprzyja to proaktywnej postawie podmiotów i ogranicza ryzyko eskalacji incydentów.
- Powiązanie kar z przeciętnym wynagrodzeniem, czyni je dynamicznymi i potencjalnie znaczącymi, zapewniając, jednocześnie że pozostają realnym, dostosowanym do rzeczywistości środkiem odstraszającym. System wymiaru kar jest elastyczny, co umożliwia na praktyczne i proporcjonalne jej nakładanie w zależności od wagi i charakteru naruszenia. Ponadto uwzględnienie w procesie oceny dotychczasowej działalności kontrolowanego podmiotu pozwala na wzięcie pod uwagę zarówno pozytywnych, jak i negatywnych działań.
- Dynamiczne kary powiązane z przeciętnym wynagrodzeniem oraz ich przeznaczenie na Fundusz Cyberbezpieczeństwa tworzą mechanizm, który nie tylko dyscyplinuje, ale też wspiera rozwój krajowego systemu bezpieczeństwa, co jest też spójne z innymi działaniami legislacyjnymi w obszarze cyberbezpieczeństwa w Polsce.
- Nowe obowiązki mogą jednocześnie generować koszty i wymagać dostosowania procesów w podmiotach, szczególnie w sektorze MŚP.