Projekt z dnia 20.05.2024 r.

U S T A W A

z dnia ….

o krajowym systemie certyfikacji cyberbezpieczeństwa[1)]

Art. 1. Ustawa określa:

1) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu;
2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy.

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 oraz Dz. Urz. UE L 169 z 29.06.2019, str. 1), zwanym dalej „rozporządzeniem 765/2008”;
2) cyberbezpieczeństwo – cyberbezpieczeństwo, o którym mowa w art. 2 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanym dalej „rozporządzeniem 2019/881”;
3) deklaracja zgodności – oświadczenie dostawcy produktu ICT, usługi ICT lub procesu ICT, że dany produkt ICT, dana usługa ICT lub dany proces ICT, jest zgodny z europejskim programem certyfikacji cyberbezpieczeństwa;
4) 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

---

[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).

niezbędne do certyfikacji, w celu harmonizacji oceny, w szczególności w odniesieniu do domen technicznych lub profili zabezpieczeń;

5) dostawca – producenta, upoważnionego przedstawiciela, importera lub dystrybutora, o których mowa w art. 2 pkt 3–6 rozporządzenia 765/2008;
6) europejski certyfikat – europejski certyfikat cyberbezpieczeństwa, o którym mowa w art. 2 pkt 11 rozporządzenia 2019/881;
7) europejski program certyfikacji cyberbezpieczeństwa – europejski program certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 9 rozporządzenia 2019/881;
8) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia 765/2008;
9) krajowy certyfikat – dokument poświadczający, że dany produkt ICT, dana usługa ICT lub dany proces ICT zostały ocenione pod względem zgodności z wymogami bezpieczeństwa określonymi w krajowym programie certyfikacji cyberbezpieczeństwa;
10) krajowy program certyfikacji cyberbezpieczeństwa – krajowy program certyfikacji cyberbezpieczeństwa, o którym mowa w art. 2 pkt 10 rozporządzenia 2019/881;
11) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia 765/2008;
12) proces ICT – proces ICT, o którym mowa w art. 2 pkt 14 rozporządzenia 2019/881;
13) produkt ICT – produkt ICT, o którym mowa w art. 2 pkt 12 rozporządzenia 2019/881;
14) usługa ICT – usługa ICT, o której mowa w art. 2 pkt 13 rozporządzenia 2019/881.

Art. 3. 1. Krajowy system certyfikacji cyberbezpieczeństwa 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.

2. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:

1) ministra właściwego do spraw informatyzacji;
2) Polskie Centrum Akredytacji;
3) jednostki oceniające zgodność prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa;
4) 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.

Art. 4. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności na podstawie określonego europejskiego programu certyfikacji cyberbezpieczeństwa na warunkach określonych w umowie zawartej przez dostawcę i jednostkę oceniającą zgodność.

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.

Art. 5. 1. Produkt ICT, usługa ICT lub proces ICT może być poddany ocenie zgodności na podstawie określonego krajowego programu certyfikacji cyberbezpieczeństwa, na warunkach określonych w umowie zawartej przez dostawcę i jednostkę oceniającą zgodność.

2. Produkt ICT, usługa ICT lub proces ICT w ramach oceny zgodności, o której mowa w ust. 1, podlega ocenie zgodności z wymogami bezpieczeństwa określonymi w krajowym programie certyfikacji cyberbezpieczeństwa.

Art. 6. Minister właściwy do spraw informatyzacji może określić, w drodze rozporządzeń, krajowe programy certyfikacji cyberbezpieczeństwa dla wybranych produktów ICT, usług ICT lub procesów ICT, zawierające:

1) wymogi dla produktów ICT, usług ICT lub procesów ICT podlegających ocenie zgodności,
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,
3) warunki wydawania, utrzymywania, przedłużania i odnawiania ważności krajowych certyfikatów,
4) sposób monitorowania zgodności produktów ICT, usług ICT lub procesów ICT z wymogami krajowych programów certyfikacji cyberbezpieczeństwa, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa,
5) dokumentację techniczną i sposób jej przechowywania,
6) treść i wzór graficzny krajowych certyfikatów,
7) okres dostępności dokumentacji technicznej oraz innych istotnych informacji

– biorąc pod uwagę rodzaje produktów ICT, usług ICT lub procesów ICT, ich znaczenie dla bezpieczeństwa systemów teleinformatycznych oraz zagrożenia, na jakie są narażone.

Art. 7. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację w obszarze objętym jednym z europejskich albo krajowych programów certyfikacji cyberbezpieczeństwa.

Art. 8. 1. Akredytacji jednostki oceniającej zgodność dokonuje Polskie Centrum Akredytacji.

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).

3. Polskie Centrum Akredytacji informuje niezwłocznie ministra właściwego do spraw informatyzacji, nie później niż w terminie 14 dni, o udzieleniu akredytacji w obszarze objętym jednym z europejskich albo krajowych programów certyfikacji cyberbezpieczeństwa.

4. Informacja o udzielonej akredytacji, o której mowa w ust. 3, zawiera:

1) oznaczenie jednostki oceniającej zgodność, której udzielono akredytacji;
2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji;
3) numer i oznaczenie certyfikatu akredytacji.

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

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

7. Polskie Centrum Akredytacji sprawuje nadzór w zakresie udzielonej akredytacji nad jednostkami oceniającymi zgodność produktów ICT, usług ICT lub procesów ICT w obszarze objętym jednym z europejskich albo krajowych programów 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 programach certyfikacji cyberbezpieczeństwa.

Art. 9. 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:

1) sprawowanie nadzoru nad funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa;

2) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3 i 4;
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 cyberbezpieczeństwa;
5) zatwierdzanie 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. 11;
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;
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, gdy określony europejski program certyfikacji cyberbezpieczeństwa to przewiduje;
11) ustalanie zakresu zmian w metodyce oceny, która ma być stosowana w przypadku, gdy określony europejski program certyfikacji cyberbezpieczeństwa to przewiduje;
12) przygotowanie krajowych programów certyfikacji cyberbezpieczeństwa.

Art. 10. 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. 9 ust. 2, w szczególności przez:

1) przygotowanie opinii, ekspertyz i analiz;
2) weryfikację dokumentów pochodzących od podmiotów, o których mowa w art. 3 ust. 2 pkt 3 i 4;
3) przeprowadzania badań produktów ICT;
4) publikację specyfikacji technicznych, norm i standardów;
5) reprezentację interesów krajowych w międzynarodowych grupach normalizacyjnych;

6) opracowanie i walidację procedur badawczych;
7) realizowanie czynności z zakresu oceny zgodności;
8) przygotowanie krajowych programów certyfikacji cyberbezpieczeństwa.

2. Minister właściwy do spraw informatyzacji może udzielić państwowemu instytutowi badawczemu wspierającemu go w realizacji zadań, o których mowa w art. 9 ust. 2, dotacji celowej z części budżetu państwa, której jest dysponentem.

3. Państwowe instytuty badawcze, które nie są nadzorowane przez ministra właściwego do spraw informatyzacji, mogą, w zakresie swoich kompetencji oraz za zgodą organu nadzorującego dany instytut, wspierać tego ministra w realizacji zadań, o których mowa w art. 9 ust. 2, w szczególności przez:

1) przygotowanie opinii, ekspertyz i analiz;
2) weryfikację dokumentów pochodzących od podmiotów, o których mowa w art. 3 ust. 2 pkt 3 i 4;
3) przeprowadzania badań produktów ICT;
4) publikację specyfikacji technicznych, norm i standardów;
5) reprezentację interesów krajowych w międzynarodowych grupach normalizacyjnych;
6) opracowanie i walidację procedur badawczych;
7) realizowanie czynności z zakresu oceny zgodności;
8) przygotowanie krajowych programów certyfikacji cyberbezpieczeństwa.

4. Państwowe instytuty badawcze wspierające ministra właściwego do spraw informatyzacji w realizacji zadań, o których mowa w art. 9 ust. 2, rozwijają potencjał badawczo-rozwojowy oraz zdolności w obszarze oceny zgodności i certyfikacji cyberbezpieczeństwa, w szczególności przez:

1) utrzymanie stałej sprawności operacyjnej w zakresie opracowywania i walidacji procedur badawczych, metod i technik oceny oraz wytwarzania materiałów odniesienia;
2) pozyskiwanie i utrzymanie ekspertów umożliwiających sprawną realizację ich zadań.

5. W szczególnie uzasadnionych przypadkach minister właściwy do spraw informatyzacji może, na podstawie umowy, zlecić podmiotom dysponującym wiedzą i kompetencjami w zakresie technologii produktów ICT, usług ICT lub procesów ICT, innym niż podmiot wskazany w ust. 1 oraz w ust. 3, wykonanie określonych usług związanych z realizacją zadań, o których mowa w art. 9 ust. 2, w szczególności zlecić przygotowanie projektów, dokumentów, opinii, ekspertyz i analiz oraz weryfikację dokumentów pochodzących od podmiotów, o których mowa w art. 3 ust. 2 pkt 3 i 4.

Art. 11. 1. W przypadku, gdy określony 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 zadań w ramach określonego europejskiego programu certyfikacji cyberbezpieczeństwa, na wniosek jednostki oceniającej zgodność, która spełniła wymogi określone w tym programie.

3. Minister właściwy do spraw informatyzacji może z urzędu, w drodze decyzji, cofnąć, albo zawiesić zezwolenie, o którym mowa w ust. 2, jeżeli jednostka oceniająca zgodność naruszyła przepisy rozporządzenia 2019/881, ustawy lub określonego europejskiego programu certyfikacji cyberbezpieczeństwa.

4. Decyzję o zawieszeniu zezwolenia wydaje się na czas określony, nie dłuższy niż 2 lata.

5. W przypadku przywrócenia zgodności z rozporządzeniem 2019/881, ustawą lub określonym europejskim programem certyfikacji cyberbezpieczeństwa, minister właściwy do spraw informatyzacji cofa decyzję o zawieszeniu zezwolenia.

6. Minister właściwy do spraw informatyzacji cofa zezwolenie, jeżeli upłynął okres, na który wydano decyzję, o której mowa w ust. 4, oraz nie ustało naruszenie przepisów rozporządzenia 2019/881, ustawy lub określonego europejskiego programu certyfikacji cyberbezpieczeństwa.

7. Minister właściwy do spraw informatyzacji przed wydaniem zezwolenia, jego zawieszeniem albo cofnięciem może zasięgnąć opinii innych podmiotów, w szczególności instytutów badawczych nadzorowanych przez tego ministra, w zakresie zgodności certyfikacji z określonym 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 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.

8. Do postępowań, o których mowa w ust. 3, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.

Art. 12. 1. W przypadku, gdy określony 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 takie działanie.

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.

3. W postępowaniu, o którym mowa w ust. 1, stosuje się art. 11 ust. 7 i 8.

Art. 13. 1. W przypadku, gdy określony 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 wraz z ich uzasadnieniem.

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

3. W postępowaniu, o którym mowa w ust. 1, stosuje się art. 11 ust. 7 i 8.

Art. 14. 1. Po przeprowadzeniu certyfikacji jednostka oceniająca zgodność niezwłocznie, nie później niż w terminie 14 dni, przesyła do ministra właściwego do spraw informatyzacji, na adres do doręczeń elektronicznych, o którym mowa w art. 2 pkt 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285, 1860 i 2699), wniosek o zatwierdzenie europejskiego certyfikatu w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania wysoki, o którym mowa w art. 57 ust. 2 rozporządzenia 2019/881.

2. Minister właściwy do spraw informatyzacji:

1) zatwierdza certyfikat, o którym mowa w ust. 1;
2) odmawia zatwierdzenia certyfikatu, o którym mowa w ust. 1, jeżeli certyfikat został wydany niezgodnie z przepisami rozporządzenia 2019/881, ustawy lub określonym europejskim programem certyfikacji cyberbezpieczeństwa.

3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się:

1) produkt ICT, usługę ICT albo proces ICT, który podlegał certyfikacji;

2) europejski program certyfikacji cyberbezpieczeństwa, w ramach którego przeprowadzono certyfikację;
3) numer wydanego certyfikatu.

4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się sprawozdanie z certyfikacji przewidziane w określonym europejskim programie certyfikacji cyberbezpieczeństwa.

5. Minister właściwy do spraw informatyzacji cofa certyfikat, o którym mowa w ust. 1, jeżeli został on wydany w sposób niezgodny z przepisami rozporządzenia 2019/881, ustawy lub określonym europejskim programem certyfikacji cyberbezpieczeństwa lub jeśli produkt ICT, usługa ICT lub proces ICT, dla którego wydany został certyfikat, nie spełnia wymogów zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa.

6. Zatwierdzenie certyfikatu, odmowa jego zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji.

7. W postępowaniu, o którym mowa w ust. 1, stosuje się art. 11 ust. 7 i 8.

Art. 15. 1. Jednostka oceniająca zgodność niezwłocznie, nie później niż w terminie 14 dni, przekazuje ministrowi właściwemu do spraw informatyzacji dane dostawcy, któremu wydano europejski albo krajowy certyfikat, wraz z kopią tego certyfikatu, dane dostawcy, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia, albo dane dostawcy, któremu odmówiono wydania certyfikatu, wraz ze wskazaniem przyczyn odmowy.

2. Dane dostawcy, o których mowa w ust. 1, obejmują:
1) nazwę (firmę);
2) adres siedziby;
3) numer w Krajowym Rejestrze Sądowym, o ile taki numer posiada, oraz numer identyfikacji podatkowej (NIP).

Art. 16. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:
1) dostawcę, który wydał deklarację zgodności, jeżeli produkt ICT, usługa ICT lub proces ICT, którego dana deklaracja dotyczy, nie spełnia wymogów zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa;
2) jednostkę oceniającą zgodność.

2. Minister właściwy do spraw informatyzacji rozpatruje skargi, o których mowa w ust. 1, w sposób i na zasadach zawartych w określonym europejskim programie certyfikacji

cyberbezpieczeństwa, a w przypadku, jeżeli program nie określa sposobu i zasad rozpatrywania skarg, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego.

Art. 17. Na wniosek ministra właściwego do spraw informatyzacji podmiot, o którym mowa w art. 3 ust. 2 pkt 3 i 4, przedstawia informacje dotyczące:

1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany europejski certyfikat, krajowy certyfikat lub deklaracja zgodności;
2) liczby wydanych certyfikatów, wraz ze wskazaniem europejskich albo krajowych programów certyfikacji cyberbezpieczeństwa, w ramach których zostały wydane oraz poziomów uzasadnienia zaufania, o których mowa w art. 52 rozporządzenia 2019/881, do których się odwoływały;
3) liczby wydanych deklaracji zgodności, wraz ze wskazaniem europejskich programów certyfikacji cyberbezpieczeństwa, w ramach których zostały wydane;
4) innych kwestii istotnych z punktu widzenia funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa.

Art. 18. 1. Minister właściwy do spraw informatyzacji w ramach nadzoru, o którym mowa w art. 9 ust. 2 pkt 1, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.

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),
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)

– określające zasady i tryb przeprowadzania kontroli.

Art. 19. Do kontroli przeprowadzanej u przedsiębiorców w ramach krajowego systemu certyfikacji cyberbezpieczeństwa stosuje się przepisy art. 55 – art. 59 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2023 r. poz. 913 i 1703).

Art. 20. Minister właściwy do spraw informatyzacji w ramach przeprowadzanej kontroli może poddać produkt ICT, usługę ICT lub proces ICT, dla których został wydany europejski albo krajowy certyfikat albo deklaracja zgodności, badaniom lub zlecić ich przeprowadzenie w celu ustalenia, czy są spełnione wymogi zawarte w określonym europejskim programie certyfikacji cyberbezpieczeństwa.

Art. 21. 1. Badanie, o którym mowa w art. 20, może zostać przeprowadzone na próbkach produktu ICT.

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

3. Protokół zawiera nazwę produktu ICT, oznaczenie certyfikatu wydanego dla tego produktu ICT lub deklaracji zgodności wydanej dla tego produktu ICT, wielkość próbki przekazanej do badania, dane identyfikujące produkt ICT, takie jak numer seryjny przekazanego jako próbka egzemplarza produktu ICT, datę przekazania próbki oraz podpis osoby sporządzającej protokół.

4. Jeżeli przeprowadzone badania wykazały, że produkt ICT nie spełnia wymogów zawartych w określonym europejskim albo krajowym programie certyfikacji cyberbezpieczeństwa, minister właściwy do spraw informatyzacji podaje do publicznej wiadomości w Biuletynie Informacji Publicznej na stronie podmiotowej ministra właściwego do spraw informatyzacji informację o niespełnianiu przez produkt ICT wymogów określonych w tym programie.

5. W przypadku certyfikatów zatwierdzanych przez ministra właściwego do spraw informatyzacji, minister ten uchyla decyzję o zatwierdzeniu certyfikatu, o której mowa w art. 14 ust. 2 pkt 1.

6. Uchylenie, o którym mowa w ust. 5, następuje w drodze decyzji ministra właściwego do spraw informatyzacji.

7. Koszty badań, o których mowa w art. 20, ponosi dostawca.

Art. 22. Minister właściwy do spraw informatyzacji w przypadku stwierdzenia, że produkt ICT nie spełnia wymogów zawartych w określonym europejskim albo krajowym programie certyfikacji cyberbezpieczeństwa, informuje o tym jednostkę oceniającą zgodność, która wydała dany certyfikat.

Art. 23. 1. Jednostka oceniająca zgodność, która, będąc do tego obowiązaną, nie przekazuje wszystkich danych, o których mowa w art. 15 ust. 2, lub przekazuje je nieprawdziwe lub niekompletne, podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotności przeciętnego wynagrodzenia miesięcznego w gospodarce narodowej za rok poprzedzający rok wymierzenia tej kary, ogłaszanego 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 2023 r. poz. 1251, 1429 i 1672), zwanego dalej „przeciętnym wynagrodzeniem”.

2. Jednostka oceniająca zgodność, która działa bez wymaganej akredytacji, podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

3. Dostawca produktów ICT, usług ICT lub procesów ICT albo jednostka oceniająca zgodność produktów ICT, usług ICT lub procesów ICT, która uniemożliwia lub utrudnia ministrowi właściwemu do spraw informatyzacji prowadzenie czynności kontrolnych, o których mowa w art. 18, podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

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

5. Dostawca produktów ICT, usług ICT lub procesów ICT, który poddaje swoje produkty ICT, usługi ICT lub procesy ICT ocenie zgodności w ramach określonego europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa, który nie wykonuje obowiązku, o którym mowa w art. 21 ust. 2, podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotności przeciętnego wynagrodzenia.

Art. 24. 1. Karę pieniężną, o której mowa w art. 23, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.

2. Ustalając wysokość kary pieniężnej minister właściwy do spraw informatyzacji uwzględnia zakres lub charakter naruszenia oraz dotychczasową działalność podmiotu.

3. Wpływy z tytułu kar pieniężnych, o których mowa w art. 23, 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 2023 r. poz. 667), w zakresie maksymalnej kwoty prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego, o którym mowa w art. 5 tej ustawy.

4. Karę pieniężną, o której mowa w art. 23, uiszcza się na rachunek Funduszu Cyberbezpieczeństwa, w terminie 14 dni od dnia uprawomocnienia się decyzji ministra właściwego do spraw informatyzacji.

5. Od decyzji ministra właściwego do spraw informatyzacji w sprawie nałożenia kary pieniężnej przysługuje odwołanie do Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów.

6. Kary pieniężne podlegają egzekucji w trybie przepisów o postępowaniu egzekucyjnym w administracji w zakresie egzekucji obowiązków o charakterze pieniężnym.

Art. 25. Do czasu wdrożenia przez ministra właściwego do spraw informatyzacji rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej, doręczenie wniosku o zatwierdzenie certyfikatu, o którym mowa w art. 14 ust. 1, na elektroniczną skrzynkę podawczą w ePUAP w ramach usługi udostępnianej w ePUAP, jest równoważne z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego.

Art. 26. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie ustawy, wynosi:

1) w 2024 r. – 784,00 tys. zł;
2) w 2025 r. – 10 194,00 tys. zł;
3) w 2026 r. – 12 000,00 tys. zł;
4) w 2027 r. – 12 000,00 tys. zł;
5) w 2028 r. – 12 000,00 tys. zł;
6) w 2029 r. – 12 000,00 tys. zł;
7) w 2030 r. – 12 000,00 tys. zł;
8) w 2031 r. – 12 000,00 tys. zł;
9) w 2032 r. – 12 000,00 tys. zł;
10) w 2033 r. – 12 000,00 tys. zł.

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

3. 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 każdego kwartału, oceny wykorzystania limitu wydatków na dany rok. Wdrożenia

mechanizmów korygujących, o których mowa w ust. 2, dokonuje minister właściwy do spraw informatyzacji.

Art. 27. Ustawa wchodzi w życie po upływie miesiąca od dnia ogłoszenia.

ZA ZGODNOŚĆ POD WZGLĘDEM PRAWNYM,
LEGISLACYJNYM I REDAKCYJNYM
Anna Markowska
Zastępca Dyrektora Departamentu Prawnego
w Ministerstwie Cyfryzacji
/podpisano elektronicznie/