| 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) | | | |
| **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 wszedł w życie w lutym 2025 r. | | | |
| **lp.** | **jed. red. aktu o cyberbezpieczeństwie** | **treść przepisu UE** | **jednostka redakcyjna ustawy** | **treść przepisu/przepisów projektu ustawy** |
| **1.** | art. 2 pkt 1, 10–12 i 15 | 10) „produkt ICT” oznacza element lub grupę elementów sieci lub systemów informatycznych;<br>11) „usługa ICT” oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych;<br>12) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;<br>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:<br>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.), zwanym dalej „rozporządzeniem 765/2008”; (…)<br>17) proces ICT – proces ICT, o którym mowa w art. 2 pkt 14 rozporządzenia 2019/881;<br>18) produkt ICT – produkt ICT, o którym mowa w art. 2 pkt 12 rozporządzenia 2019/881; (…)<br>22) usługa ICT – usługę ICT, o której mowa w art. 2 pkt 13 rozporządzenia 2019/881;<br>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: (…)<br>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;<br>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: (…)<br>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; (…)<br>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.<br>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 przechowywanych, przekazywanych lub przetwarzanych danych, lub funkcji lub usług oferowanych lub dostępnych | 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.<br>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:<br>1) wytwarzanie wysokiej jakości produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa;<br>2) budowę systemów zarządzania cyberbezpieczeństwem;<br>3) zapewnienie:<br>a) wykwalifikowanych specjalistów w obszarze cyberbezpieczeństwa, |

| | | | | |
|---|---|---|---|---|
| | | 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. | | 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,<br>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.<br>2. Krajowy system certyfikacji cyberbezpieczeństwa obejmuje:<br>1) ministra właściwego do spraw informatyzacji;<br>2) Polskie Centrum Akredytacji;<br>3) jednostki oceniające zgodność;<br>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;<br>5) osoby fizyczne, które poddają swoją wiedzę i umiejętności praktyczne ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa;<br>6) podmioty, które poddają wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa.<br>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.<br>2. Ocena zgodności, o której mowa w ust. 1, odnosi się do jednego z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881.<br>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.<br>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:<br>a) po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa każdego europejskiego certyfikatu cyberbezpieczeństwa wydanego przez daną jednostkę oceniającą zgodność; lub<br>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.<br>2. Minister właściwy do spraw informatyzacji:<br>1) wydaje, w drodze decyzji, zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1;<br>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.<br>3. We wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, wskazuje się:<br>1) produkt ICT, usługę ICT, proces ICT albo usługę zarządzaną w zakresie bezpieczeństwa, które podlegały certyfikacji;<br>2) europejski program certyfikacji cyberbezpieczeństwa, w ramach którego przeprowadzono certyfikację.<br>4. Do wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, dołącza się raport z certyfikacji.<br>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 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.<br>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.<br>8. Do postępowań w sprawie wydania decyzji, o których mowa w ust. 2 oraz ust. 5, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.<br>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.<br>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 ono również Komisję o zadaniach powierzonych każdemu z tych organów.<br>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. | 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.<br>2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>1) sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3–6;<br>2) przeprowadzanie kontroli podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3, 4 i 6;<br>3) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;<br>4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji;<br>5) wyrażanie zgody na wydanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”, o którym mowa w art. 52 ust. 7 rozporządzenia 2019/881;<br>6) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań w ramach europejskich programów certyfikacji cyberbezpieczeństwa;<br>7) prowadzenie postępowań w sprawie zezwoleń, o których mowa w art. 19; |

| | | | | |
|---|---|---|---|---|
| | | 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.<br>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.<br>6. W celu skutecznego wdrożenia niniejszego rozporządzenia zasadnym jest, aby organy te uczestniczyły w pracach ECCG w aktywny, skuteczny, wydajny i bezpieczny sposób. | | 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;<br>9) uczestniczenie w pracach Europejskiej Grupy do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) na podstawie art. 58 ust. 6 rozporządzenia 2019/881;<br>10) wyrażanie zgody na rezygnację z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy, jeżeli dany europejski program certyfikacji cyberbezpieczeństwa to przewiduje;<br>11) ustalanie zmian w metodyce oceny, która ma być stosowana w przypadku, gdy dany europejski program certyfikacji cyberbezpieczeństwa to przewiduje;<br>12) przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa;<br>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;<br>14) monitorowanie spełniania przez jednostki oceniające zgodność wymogów określonych w załączniku do rozporządzenia 2019/881;<br>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.<br>3. Minister właściwy do spraw informatyzacji jest administratorem danych osobowych przetwarzanych w celu realizacji jego zadań, obowiązków lub uprawnień wynikających z ustawy.<br>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.<br>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:<br>1) przygotowanie opinii, ekspertyz i analiz;<br>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;<br>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;<br>4) publikację wykazów specyfikacji technicznych, norm i standardów;<br>5) udział w pracach międzynarodowych grup normalizacyjnych z zakresu cyberbezpieczeństwa zgodnie z zasadami normalizacji krajowej i międzynarodowej;<br>6) opracowanie i walidację procesów badawczych;<br>7) przygotowanie projektów krajowych schematów certyfikacji cyberbezpieczeństwa;<br>8) organizowanie porównań międzylaboratoryjnych lub badań biegłości w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa;<br>9) weryfikację, czy dana osoba fizyczna posiada:<br>a) kwalifikacje techniczne i zawodowe, obejmujące wszystkie czynności z zakresu cyberbezpieczeństwa lub oceny zgodności,<br>b) odpowiednie doświadczenie do realizacji zadań z zakresu oceny zgodności,<br>c) wiedzę z zakresu cyberbezpieczeństwa, w szczególności w zakresie wymagań wynikających z danego europejskiego programu certyfikacji cyberbezpieczeństwa albo danego krajowego schematu certyfikacji cyberbezpieczeństwa,<br>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:<br>1) przygotowanie opinii, ekspertyz i analiz;<br>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;<br>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;<br>4) publikację wykazów specyfikacji technicznych, norm i standardów;<br>5) udział w pracach międzynarodowych grup normalizacyjnych z zakresu cyberbezpieczeństwa zgodnie z zasadami normalizacji krajowej i międzynarodowej;<br>6) opracowanie i walidację procesów badawczych;<br>7) przygotowanie projektów krajowych schematów certyfikacji cyberbezpieczeństwa;<br>8) organizowanie porównań międzylaboratoryjnych lub badań biegłości w danym europejskim programie certyfikacji cyberbezpieczeństwa albo danym krajowym schemacie certyfikacji cyberbezpieczeństwa.<br>9) weryfikację, czy dana osoba fizyczna posiada:<br>a) kwalifikacje techniczne i zawodowe, obejmujące wszystkie czynności z zakresu cyberbezpieczeństwa lub oceny zgodności,<br>b) odpowiednie doświadczenie do realizacji zadań z zakresu oceny zgodności,<br>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.<br>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.<br>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:<br>1) utrzymywanie stałej sprawności operacyjnej;<br>2) pozyskiwanie i utrzymanie ekspertów.<br>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.<br>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.<br>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.<br>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. …).”.<br>Art. 39. 1. Maksymalny limit wydatków z budżetu państwa dla części budżetowej 27 – informatyzacja, będący skutkiem finansowym wejścia w życie ustawy, wynosi:<br>1) w 2025 r. – 9 720 tys. zł;<br>2) w 2026 r. – 11 600 tys. zł;<br>3) w 2027 r. – 11 880 tys. zł;<br>4) w 2028 r. – 12 190 tys. zł;<br>5) w 2029 r. – 12 500 tys. zł;<br>6) w 2030 r. – 12 820 tys. zł;<br>7) w 2031 r. – 13 150 tys. zł;<br>8) w 2032 r. – 13 490 tys. zł;<br>9) w 2033 r. – 13 840 tys. zł;<br>10) w 2034 r. – 14 200 tys. zł.<br>2. Maksymalny limit wydatków Polskiego Centrum Akredytacji, będący skutkiem finansowym wejścia w życie ustawy wynosi:<br>1) w 2025 r. – 300 tys. zł;<br>2) w 2026 r. – 310 tys. zł;<br>3) w 2027 r. – 320 tys. zł;<br>4) w 2028 r. – 330 tys. zł;<br>5) w 2029 r. – 340 tys. zł;<br>6) w 2030 r. – 350 tys. zł;<br>7) w 2031 r. – 360 tys. zł;<br>8) w 2032 r. – 360 tys. zł;<br>9) w 2033 r. – 370 tys. zł;<br>10) w 2034 r. – 380 tys. zł.<br>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.<br>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.<br>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:<br>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;<br>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 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;<br>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;<br>d) monitorują i nadzorują działalność podmiotów publicznych, o których mowa w art. 56 ust. 5;<br>34 | art. 4, art. 17, art. 23 i art. 27 | Art. 4. 1. 1. Minister właściwy do spraw informatyzacji jest krajowym organem do spraw certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 rozporządzenia 2019/881.<br>2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>1) sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3–6;<br>2) przeprowadzanie kontroli podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3, 4 i 6;<br>3) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881;<br>4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji;<br>5) wyrażanie zgody na wydanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”, o którym mowa w art. 52 ust. 7 rozporządzenia 2019/881;<br>6) rozpoznawanie skarg złożonych na jednostki oceniające zgodność w zakresie prowadzonych przez te jednostki działań w ramach europejskich programów certyfikacji cyberbezpieczeństwa;<br>7) prowadzenie postępowań w sprawie zezwoleń, o których mowa w art. 19;<br>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;<br>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;<br>11) ustalanie zmian w metodyce oceny, która ma być stosowana w przypadku, gdy dany europejski program certyfikacji cyberbezpieczeństwa to przewiduje;<br>12) przygotowanie krajowych schematów certyfikacji cyberbezpieczeństwa;<br>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;<br>14) monitorowanie spełniania przez jednostki oceniające zgodność wymogów określonych w załączniku do rozporządzenia 2019/881;<br>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.<br>3. Minister właściwy do spraw informatyzacji jest administratorem danych osobowych przetwarzanych w celu realizacji jego zadań, obowiązków lub uprawnień wynikających z ustawy.<br>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.<br>Art. 17. 1. Akredytacji jednostki oceniającej zgodność udziela Polskie Centrum Akredytacji.<br>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).<br>3. Akredytacji udziela się na okres nie dłuższy niż 5 lat.<br>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.<br>5. Informacja o udzieleniu akredytacji, o której mowa w ust. 3, zawiera:<br>1) oznaczenie jednostki oceniającej zgodność, której udzielono akredytacji;<br>2) wskazanie zakresu udzielonej akredytacji, daty udzielenia akredytacji oraz okresu ważności udzielonej akredytacji;<br>3) numer i oznaczenie certyfikatu akredytacji.<br>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.<br>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:<br>1) załączniku do rozporządzenia 2019/881;<br>2) europejskich programach certyfikacji cyberbezpieczeństwa;<br>3) krajowych schematach certyfikacji cyberbezpieczeństwa.<br>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:<br>1) którym wydano albo przedłużono europejski certyfikat albo krajowy certyfikat, wraz z kopią tego certyfikatu;<br>2) którym cofnięto europejski certyfikat albo krajowy certyfikat, wraz ze wskazaniem przyczyny jego cofnięcia;<br>3) którym odmówiono wydania europejskiego certyfikatu albo krajowego certyfikatu, wraz ze wskazaniem przyczyn odmowy.<br>2. Dane, o których mowa w ust. 1, obejmują:<br>1) w przypadku osoby prawnej:<br>a) nazwę (firmę), |

| | | | | |
|---|---|---|---|---|
| | | | | b) adres i siedzibę,<br>c) numer we właściwym rejestrze, o ile taki numer został nadany, oraz numer identyfikacji podatkowej (NIP);<br>2) w przypadku osoby fizycznej:<br>a) imię i nazwisko,<br>b) numer PESEL.<br>3. Dane, o których mowa w ust. 1, jednostka oceniająca zgodność przekazuje drogą elektroniczną ministrowi właściwemu do spraw informatyzacji.<br>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.<br>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.<br>Art. 27. 1. 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:<br>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;<br>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;<br>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 zostały te deklaracje zostały wydane;<br>5) innych kwestii istotnych dla funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa.<br>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:<br>(…)<br>7) prowadzenie postępowań w sprawie zezwoleń, o których mowa w art. 19;<br>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.<br>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.<br>3. Wniosek, o którym mowa w ust. 2, zawiera:<br>1) nazwę (firmę) wnioskodawcy;<br>2) adres i siedzibę wnioskodawcy;<br>3) wskazanie europejskiego programu certyfikacji cyberbezpieczeństwa, którego dotyczy wniosek;<br>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.<br>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.<br>6. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się, jeżeli:<br>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;<br>2) naruszenie, o którym mowa w ust. 5, jest odwracalne.<br>7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na czas określony, nie dłuższy niż 2 lata.<br>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.<br>9. Minister właściwy do spraw informatyzacji cofa decyzję o zezwoleniu, o którym mowa w ust. 2, jeżeli:<br>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;<br>2) naruszenie, o którym mowa w ust. 5, jest nieodwracalne;<br>3) upłynął okres, na który wydano decyzję, o której mowa w ust. 6, oraz nie ustało naruszenie, o którym mowa w ust. 5.<br>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.<br>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.<br>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 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; | art. 25 i art. 26 | Art. 25. 1. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na:<br>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 zawartych w danym europejskim programie certyfikacji cyberbezpieczeństwa;<br>2) jednostkę oceniającą zgodność prowadzącą ocenę produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa w zakresie cyberbezpieczeństwa.<br>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.<br>3. Rozpatrzenie skargi, o której mowa w ust. 1, następuje nie później niż w terminie 2 miesięcy od dnia jej złożenia.<br>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. (…)<br>2. Do zadań ministra właściwego do spraw informatyzacji należy: (…)<br>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 lub z wymogami określonych europejskich programów certyfikacji cyberbezpieczeństwa; | 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. (…)<br>2. Do zadań ministra właściwego do spraw informatyzacji należy: (…)<br>4) współpraca z innymi podmiotami, w szczególności z Polskim Centrum Akredytacji, w zakresie certyfikacji; |
| **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 | a) Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa ma co najmniej następujące uprawnienia do:<br>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:<br>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;<br>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;<br>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;<br>4) liczby wydanych deklaracji zgodności wraz ze wskazaniem europejskich programów certyfikacji cyberbezpieczeństwa, w ramach których zostały te deklaracje zostały wydane; |

| | | | | |
|---|---|---|---|---|
| | | | | 5) innych kwestii istotnych dla funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa.<br>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<br>ust. 8<br>lit. b–d | b) prowadzenia postępowań, w formie audytów, w stosunku do jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa i podmiotów, które wydały unijne deklaracje zgodności, w celu weryfikacji przestrzegania przez nie niniejszego tytułu;<br>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;<br>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; | 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 ICT lub usług zarządzanych w zakresie bezpieczeństwa oraz podmiotu, który poddał wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności.<br>2. Do kontroli, o której mowa w ust. 1, przeprowadzonej wobec dostawców:<br>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);<br>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).<br>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.<br>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.<br>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.<br>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.<br>4. Protokół, o którym mowa w ust. 3, zawiera:<br>1) nazwę produktu ICT;<br>2) oznaczenie europejskiego certyfikatu albo krajowego certyfikatu wydanego dla produktu ICT lub deklaracji zgodności wydanej dla produktu ICT;<br>3) wielkość próbki produktu ICT przekazanej do badania;<br>4) dane identyfikujące produkt ICT, w szczególności numer seryjny przekazanego jako próbka egzemplarza produktu ICT;<br>5) imię i nazwisko osoby przekazującej próbkę produktu ICT;<br>6) imię i nazwisko osoby odbierającej próbkę produktu ICT;<br>7) datę przekazania próbki produktu ICT;<br>8) podpis osoby sporządzającej protokół.<br>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.<br>2. W przypadku certyfikatu, o którym mowa w art. 22 ust. 1, minister właściwy do spraw informatyzacji:<br>1) cofa certyfikat, jeżeli wykryte nieprawidłowości:<br>a) mają znaczący wpływ na dostępność, autentyczność, integralność lub poufność danych, sieci i systemów informatycznych danego podmiotu wykorzystującego system zarządzania cyberbezpieczeństwem lub<br>b) mają znaczący wpływ na użytkownika produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa lub |

| | | | | |
|---|---|---|---|---|
| | | | | c) są nieodwracalne;<br>2) zawiesza certyfikat, jeżeli wykryte nieprawidłowości nie mają znaczącego wpływu, o którym mowa w pkt 1 lit. a i b , oraz są odwracalne.<br>3. Decyzję o zawieszeniu europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, wydaje się na czas określony, nie dłuższy niż 6 miesięcy.<br>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.<br>5. Cofnięcie albo zawieszenie europejskiego certyfikatu, o którym mowa w art. 22 ust. 1, następuje w drodze decyzji ministra właściwego do spraw informatyzacji.<br>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<br>ust. 8<br>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<br>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.<br>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.<br>2. Minister właściwy do spraw informatyzacji:<br>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.<br>3. We wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, wskazuje się:<br>1) produkt ICT, usługę ICT, proces ICT albo usługę zarządzaną w zakresie bezpieczeństwa, które podlegały certyfikacji;<br>2) europejski program certyfikacji cyberbezpieczeństwa, w ramach którego przeprowadzono certyfikację.<br>4. Do wniosku o zgodę na wydanie europejskiego certyfikatu, o którym mowa w ust. 1, dołącza się raport z certyfikacji.<br>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.<br>6. Minister właściwy do spraw informatyzacji przed wydaniem decyzji, o których mowa w ust. 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.<br>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.<br>8. Do postępowań w sprawie wydania decyzji, o których mowa w ust. 2 oraz ust. 5, stosuje się przepisy działu II rozdziału 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.<br>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.<br>2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>1) sprawowanie nadzoru nad podmiotami krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 3 ust. 2 pkt 3–6; (…)<br>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.<br>2. Jednostka oceniająca zgodność, która wydaje europejski certyfikat albo krajowy certyfikat albo , działając bez wymaganej akredytacji, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Art. 34. 1. Kary pieniężne, o których mowa w art. 33, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.<br>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.<br>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).<br>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.<br>5. Od decyzji ministra właściwego do spraw informatyzacji w sprawie nałożenia kary pieniężnej, o której mowa w art. 33, przysługuje skarga do sądu administracyjnego.<br>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 produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa. | 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.<br>2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>(…)<br>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.<br>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.<br>3. W ramach wzajemnego przeglądu ocenia się:<br>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;<br>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);<br>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);<br>d) procedury monitorowania, wydawania zezwoleń na działalność i nadzorowania działalności jednostek oceniających zgodność;<br>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.<br>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 | 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.<br>2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>(…)<br>3) przeprowadzanie wzajemnego przeglądu, o którym mowa w art. 59 rozporządzenia 2019/881; |

| | | | | |
|---|---|---|---|---|
| | | pięć lat. ENISA może uczestniczyć we wzajemnym przeglądzie.<br>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.<br>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.<br>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.<br>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).<br>3. Akredytacji udziela się na okres nie dłuższy niż 5 lat.<br>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.<br>5. Informacja o udzieleniu akredytacji, o której mowa w ust. 3, zawiera:<br>1) oznaczenie jednostki oceniającej zgodność, której udzielono akredytacji;<br>2) wskazanie zakresu udzielonej akredytacji, daty udzielenia akredytacji oraz okresu ważności udzielonej akredytacji;<br>3) numer i oznaczenie certyfikatu akredytacji.<br>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.<br>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:<br>1) załączniku do rozporządzenia 2019/881;<br>2) europejskich programach certyfikacji cyberbezpieczeństwa;<br>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.<br>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.<br>3. Wniosek, o którym mowa w ust. 2, zawiera:<br>1) nazwę (firmę) wnioskodawcy;<br>2) adres i siedzibę wnioskodawcy;<br>3) wskazanie europejskiego programu certyfikacji cyberbezpieczeństwa, którego dotyczy wniosek;<br>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.<br>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.<br>6. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się, jeżeli:<br>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;<br>2) naruszenie, o którym mowa w ust. 5, jest odwracalne.<br>7. Decyzję o zawieszeniu zezwolenia, o którym mowa w ust. 2, wydaje się na czas określony, nie dłuższy niż 2 lata.<br>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.<br>9. Minister właściwy do spraw informatyzacji cofa decyzję o zezwoleniu, o którym mowa w ust. 2, jeżeli:<br>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;<br>2) naruszenie, o którym mowa w ust. 5, jest nieodwracalne;<br>3) upłynął okres, na który wydano decyzję, o której mowa w ust. 6, oraz nie ustało naruszenie, o którym mowa w ust. 5.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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 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. | 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 podstawie umowy zawartej przez dostawcę i jednostkę oceniającą zgodność.<br>2. Ocena zgodności, o której mowa w ust. 1, odnosi się do jednego z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881.<br>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.<br>Art. 17. 1. Akredytacji jednostki oceniającej zgodność udziela Polskie Centrum Akredytacji.<br>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).<br>3. Akredytacji udziela się na okres nie dłuższy niż 5 lat.<br>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.<br>5. Informacja o udzieleniu akredytacji, o której mowa w ust. 3, zawiera:<br>1) oznaczenie jednostki oceniającej zgodność, której udzielono akredytacji;<br>2) wskazanie zakresu udzielonej akredytacji, daty udzielenia akredytacji oraz okresu ważności udzielonej akredytacji;<br>3) numer i oznaczenie certyfikatu akredytacji.<br>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.<br>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:<br>1) załączniku do rozporządzenia 2019/881;<br>2) europejskich programach certyfikacji cyberbezpieczeństwa;<br>3) krajowych schematach certyfikacji cyberbezpieczeństwa. |

| | | | | |
|---|---|---|---|---|
| **22.** | art. 62 | 1. Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („ECCG”).<br>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.<br>3. Interesariusze i odpowiednie strony trzecie mogą być zapraszani na posiedzenia ECCG i do udziału w jej pracach.<br>4. ECCG ma następujące zadania:<br>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;<br>b) pomaganie, doradzanie i współpracowanie z ENISA w związku z przygotowywaniem propozycji programu na podstawie art. 49;<br>c) wydawanie opinii na temat propozycji programu przygotowanej przez ENISA na podstawie art. 49 niniejszego rozporządzenia;<br>d) zwracanie się do ENISA z wnioskiem o przygotowanie propozycji programu na podstawie art. 48 ust. 2;<br>e) wydawanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa;<br>f) monitorowanie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk odnoszących się do programów certyfikacji cyberbezpieczeństwa;<br>g) ułatwianie współpracy pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa w ramach | art. 4 ust. 2 pkt 9 | Art. 4. 2. Do zadań ministra właściwego do spraw informatyzacji należy:<br>9) uczestniczenie w pracach Europejskiej Grupy do Spraw Certyfikacji Cyberbezpieczeństwa (ECCG) na podstawie art. 58 ust. 6 rozporządzenia 2019/881; (…) |

| | | | | |
|---|---|---|---|---|
| | | niniejszego tytułu poprzez budowanie zdolności, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa;<br>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);<br>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.<br>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.<br>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.<br>2. Jednostka oceniająca zgodność rozpatruje skargę w terminie nie dłuższym niż 2 miesiące od dnia złożenia skargi.<br>3. Skargę rozpatrują osoby, które nie brały udziału w działaniach, których dotyczy skarga.<br>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 | 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. |

| | | | | |
|---|---|---|---|---|
| | | 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. | | 2. Jednostka oceniająca zgodność, która wydaje europejski certyfikat albo krajowy certyfikat albo , działając bez wymaganej akredytacji, podlega karze pieniężnej w wysokości do dwudziestokrotności przeciętnego wynagrodzenia.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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).<br>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.<br>5. Od decyzji ministra właściwego do spraw informatyzacji w sprawie nałożenia kary pieniężnej, o której mowa w art. 33, przysługuje skarga do sądu administracyjnego.<br>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. |