|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TABELA ZGODNOŚCI** | | | | |
| **TYTUŁ PROJEKTU** | | Ustawa o zmianie ustawy o krajowym systemie cyberbezpieczeństwa | | |
| **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 termin na implementację aktu o cyberbezpieczeństwie – 28 czerwca 2021. | | |
| **l.p.** | **jednostka redakcyjna**  **aktu o cyberbezpieczeństwie** | treść przepisu UE | **jednostka redakcyjna**  **ustawy** | **treść przepisu/przepisów projektu ustawy** |
|  | Art. 2 pkt 1 | 1) „cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami; | Art. 2 ust 1 pkt 4 | cyberbezpieczeństwo – działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;”, |
|  | 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 ust. 1 pkt 17 | „17) cyberzagrożenie – wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku systemów informacyjnych, użytkowników takich systemów oraz innych osób;”, |
|  | Art. 2 pkt 12- 15 | 12) „produkt ICT” oznacza element lub grupę elementów sieci lub systemów informatycznych;  13) „usługa ICT” oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych;  14) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;  15) „akredytacja” oznacza akredytację zgodnie z definicją w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008; | Art. 2 ust 1 pkt 20-23 | 20) produkt ICT – element lub grupę elementów systemów informacyjnych;  21) usługa ICT – usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem systemów informacyjnych;  22) proces ICT – zestaw czynności wykonywanych w celu projektowania, budowy, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT;  23) akredytacja – akredytację, o której mowa w art. 2 pkt 10 rozporządzenia (WE) nr 765/2008; |
|  | Art. 2 pkt 17-18 | 17)„ocena zgodności” oznacza ocenę zgodności zgodnie z definicją w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008;  18) „jednostka oceniająca zgodność” oznacza jednostkę oceniającą zgodność zgodnie z definicją w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008; | Art. 2 ust. 1 pkt 24-25 | 24) ocena zgodności – ocenę zgodności, o której mowa w art. 2 pkt 12 rozporządzenia (WE) nr 765/2008;  25) jednostka oceniająca zgodność – jednostkę oceniającą zgodność, o której mowa w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008; |
|  | 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 i procesów ICT.  PL 7.6.2019 Dziennik Urzędowy Unii Europejskiej L 151/53    2. Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa i potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenia dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. | Art. 1 ust.1 pkt 1a oraz Art. 59a | „1a) organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zasady i tryb certyfikacji produktu ICT, usługi ICT lub procesu ICT w zakresie cyberbezpieczeństwa określonych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06.2019, str. 15), zwanego dalej, „rozporządzeniem 2019/881”  Art. 59a. Krajowy system certyfikacji cyberbezpieczeństwa ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT. |
|  | Art. 53 | Europejski program certyfikacji cyberbezpieczeństwa może zezwalać na ocenę zgodności przez stronę pierwszą przeprowadzaną na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów ICT, usług ICT lub procesów ICT. Na ocenę zgodności przez stronę pierwszą zezwala się jedynie w przypadku produktów ICT, usług ICT lub procesów ICT, które stwarzają niewielkie ryzyko odpowiadające poziomowi uzasadnienia zaufania „podstawowy”. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT może wydać unijną deklarację zgodności stwierdzającą, że wykazano spełnienie wymogów określonych w programie. Wydając taką deklarację, wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT przyjmuje na siebie odpowiedzialność za zgodność produktu ICT, usługi ICT lub procesu ICT z wymogami określonymi w tym programie.  3. Wytwórca lub dostawca produktów ICT, usług ICT lub procesów ICT udostępnia – przez okres przewidziany w odpowiednim europejskim programie certyfikacji cyberbezpieczeństwa – krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 ust. 1, unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT lub usług ICT z programem. Kopię unijnej deklaracji zgodności przedkłada się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA.  4. Wydanie unijnej deklaracji zgodności jest dobrowolne, o ile prawo Unii lub prawo państw członkowskich nie stanowi inaczej.  5. Unijne deklaracje zgodności są uznawane we wszystkich państwach członkowskich. | Art. 59m pkt 1 | Art. 59m. Podczas dokonywania oceny zgodności produkt ICT, usługę ICT lub proces ICT poddaje się przed wydaniem:   1. deklaracji zgodności - badaniom przez wytwórcę lub dostawcę, jeżeli nie jest wymagane przeprowadzenie badań przez laboratorium niezależne od dostawcy i odbiorcy, |
|  | Art. 56  ust. 6 | W przypadku gdy europejski program certyfikacji cyberbezpieczeństwa przyjęty na podstawie art. 49 wymaga poziomu uzasadnienia zaufania „wysoki”, europejski certyfikat cyberbezpieczeństwa wydawany w ramach tego programu może być wydany wyłącznie przez krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – w następujących przypadkach – przez jednostkę oceniającą zgodność:  a) po uprzednim zatwierdzeniu przez krajowy organ ds. certyfikacji cyberbezpieczeństwa każdego europejskiego certyfikatu cyberbezpieczeństwa wydanego przez daną jednostkę oceniającą zgodność; lub  b) na podstawie ogólnego powierzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność. | Art. 59o | 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji przesyła do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:   1. w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania „wysoki”; 2. w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania „wysoki”.   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 ustawą lub programami, o których mowa w ust. 1.   3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego lub krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.  4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg procesu oceny zgodności.  5. Jeżeli wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, zawiera braki formalne, organ administracji publicznej wzywa organ wnioskujący do ich uzupełnienia w terminie czternastu dni od dnia doręczenia wezwania.  6. Jeżeli organ wnioskujący nie uzupełni w terminie braków formalnych wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, nie podlega rozpatrzeniu i jest zwracany organowi wnioskującemu.  7. Minister właściwy do spraw informatyzacji cofa certyfikat, jeśli jest on niezgodny z rozporządzeniem 2019/881, europejskim lub krajowym programem certyfikacji cyberbezpieczeństwa lub z ustawą.  8. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji. |
|  | Art. 58  ust. 1-6 | 1. Każde państwo członkowskie wyznacza na swoim terytorium przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa lub – za zgodą innego państwa członkowskiego – wyznacza przynajmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa ustanowiony na terytorium tego innego państwa członkowskiego jako organ odpowiedzialny za zadania związane z nadzorem w wyznaczającym państwie członkowskim.  2. Każde państwo członkowskie informuje Komisję o wyznaczonych krajowych organach ds. certyfikacji cyberbezpieczeństwa, a w przypadku gdy państwo członkowskie wyznacza więcej niż jeden organ, informuje ono również Komisję o zadaniach powierzonych każdemu z tych organów.  3. Bez uszczerbku dla art. 56 ust. 5 lit. a) i art. 56 ust. 6 każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa pozostaje niezależny od jednostek, nad którymi sprawuje nadzór, w zakresie swojej organizacji, decyzji w sprawie finansowania, struktury prawnej i procesu podejmowania decyzji.  4. Państwa członkowskie zapewniają, by działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, była ściśle oddzielona od ich działalności związanej z nadzorem określonej w niniejszym artykule i by oba rodzaje tej działalności były wykonywane niezależnie od siebie.  5. Państwa członkowskie zapewniają, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa posiadały odpowiednie zasoby na potrzeby wykonywania swoich uprawnień i wywiązywania się ze swoich zadań w skuteczny i wydajny sposób.  6. W celu skutecznego wdrożenia niniejszego rozporządzenia zasadnym jest, aby organy te uczestniczyły w pracach ECCG w aktywny, skuteczny, wydajny i bezpieczny sposób. | Art. 59c | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z oceną zgodności wyrobów;  2) monitorowanie wdrażania i stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;  3) przeprowadzanie kontroli w stosunku do podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa, o których mowa w art. 59b ust. 1 pkt. 3-4;  4) przeprowadzanie wzajemnego przeglądu o którym mowa art. 59 rozporządzenia 2019/881;  5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;  6) zatwierdzanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki”;  7) zatwierdzanie krajowych certyfikatów cyberbezpieczeństwa o krajowym poziomie uzasadnienia zaufania „wysoki”;  8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa;  9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonych europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa;  10) rozpoznawanie skarg złożonych na jednostki oceniające zgodność;  11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;  12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b-d oraz ust. 8 rozporządzenia 2019/881;  13) uczestnictwo w pracach ECCG;  14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;  15) nadzorowanie i egzekwowanie zawartych w europejskich i krajowych programach certyfikacji bezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;  16) przygotowywanie propozycji krajowego programu certyfikacji cyberbezpieczeństwa. |
|  | Art. 58 ust. 7 pkt a-d | 7. Krajowe organy ds. certyfikacji cyberbezpieczeństwa:  a) nadzorują i egzekwują stosowanie zawartych w europejskich programach certyfikacji bezpieczeństwa na podstawie art. 54 ust. 1 lit. j) zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami europejskich certyfikatów cyberbezpieczeństwa wydanych na ich terytoriach, we współpracy z innymi odpowiednimi organami nadzoru rynku;  b)monitorują wykonywanie obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT, 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;  c) bez uszczerbku dla art. 60 ust. 3 aktywnie wspomagają i wspierają krajowe jednostki akredytujące w monitorowaniu i nadzorowaniu działalności jednostek oceniających zgodność do celów niniejszego rozporządzenia;  d) monitorują i nadzorują działalność podmiotów publicznych, o których mowa w art. 56 ust. 5;  34 | Art. 59c. ust. 1 pkt 1-2, 5, 15  Art. 59h ust. 2, 5-6, Art. 59l, art. 59 q, art. 59u, art. 59 x | Art. 59c  1.Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  1) sprawowanie nadzoru nad działalnością jednostek oceniających zgodność w zakresie prowadzenia przez te jednostki działań związanych z oceną zgodności wyrobów;  2) monitorowanie wdrażania i stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;  5) współpraca z Polskim Centrum Akredytacji w obszarze monitorowania i nadzorowania działalności jednostek oceniających zgodność w zakresie przestrzegania rozporządzenia 2019/881 oraz ustawy;  15) nadzorowanie i egzekwowanie zawartych w europejskich i krajowych programach certyfikacji bezpieczeństwa zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z wymogami certyfikatów wydanych, we współpracy z innymi odpowiednimi organami nadzoru rynku;  Art. 59h  2. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.  5. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o cofnięciu akredytacji, o której mowa w ust. 1.  6. Informacja o cofnięciu akredytacji, o której mowa w ust. 1, zawiera:   1. oznaczenie podmiotu, któremu cofnięto akredytację; 2. wskazanie przyczyny uzasadniającej cofnięcie akredytacji; 3. wskazanie daty cofnięcia akredytacji   Art. 59l  Jednostka oceniająca zgodność przekazuje ministrowi właściwemu do spraw informatyzacji dane podmiotu, któremu wydano certyfikat, albo podmiotu, któremu cofnięto certyfikat, wraz ze wskazaniem przyczyny jej cofnięcia.  Art. 59q. Po wydaniu deklaracji zgodności dostawca przesyłała jej kopię do ministra właściwego do spraw informatyzacji  Art. 59u. 1. W okresie, na jaki został wydany certyfikat, podmiot któremu go wydano, jest obowiązany spełniać kryteria obowiązujące na dzień jego wydania.  2. Jednostka oceniająca zgodność cofa certyfikat w przypadku stwierdzenia, że podmiot, któremu wydano certyfikat nie spełnia lub przestał spełniać kryteria certyfikacji.  3. Jednostka oceniająca zgodność informuje ministra właściwego do spraw informatyzacji o cofnięciu certyfikatu.  Art. 59x. Podmiot, o którym mowa w art. 59b ust. 1 pkt 3-4, na wniosek ministra właściwego do spraw informatyzacji, przedstawia informacje dotyczące:  1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;  2) wyjaśnienia związane z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa  3) liczby wydanych certyfikatów w tym programów w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;  4) liczby wydanych deklaracji zgodności w tym programów w ramach których zostały wydane;  5) liczby i sposobu rozpatrzenia skarg o których mowa w art. 59za. |
|  | Art. 58 ust. 7 pkt 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. 59c ust. 1 pkt 11 oraz art. 59i | Art. 59c  1.Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  11) prowadzenie postępowań w sprawie zezwoleń, o których mowa art. 59i;  Art. 59i. 1. W przypadku, gdy:  1) europejski program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881,  2) krajowy program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi o których mowa w art. 59g pkt 4  - minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie zadań w ramach takich programów wyłącznie jednostkom oceniającym zgodność spełniającym te wymogi.  2. Minister właściwy do spraw informatyzacji może cofnąć, ograniczyć lub zawiesić zezwolenie, o którym mowa w ust. 1, jeśli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa. Cofnięcie, ograniczenie lub zawieszenie zezwolenia, o którym mowa w ust. 1, następuje w drodze decyzji. |
|  | Art. 58 ust. 7 pkt 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. 59zb-zc | Art. 59zb. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na podmiot, który wydał unijną lub krajową deklarację zgodności, jeśli produkt ICT, usługa ICT lub proces ICT którego dana deklaracja dotyczy nie spełnia wymogów określonych w programie certyfikacji cyberbezpieczeństwa.  Art. 59zc. Do skarg, o których mowa w art. 59 za ust. 5 oraz art. 59zb, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego. |
|  | Art. 58 ust. 7 pkt 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. 59c ust. 1  pkt 12 | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  12) przekazywanie ENISA oraz Europejskiej Grupie do Spraw Certyfikacji Cyberbezpieczeństwa, zwanej dalej „ECCG”, corocznego raportu z działań przeprowadzonych na podstawie art. 58 ust. 7 lit. b-d oraz ust. 8 rozporządzenia 2019/881; |
|  | Art. 58 ust. 7 pkt 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 i procesów ICT, z wymogami niniejszego rozporządzenia lub z wymogami określonych europejskich programów certyfikacji cyberbezpieczeństwa; | Art. 59c ust. 1 pkt 9 | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonych europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa; |
|  | Art.58 ust. 7 pkt. i | i) monitorują odpowiednie zmiany w dziedzinie certyfikacji cyberbezpieczeństwa. | Art. 59c  ust. 1 pkt 8 | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  8) monitorowanie zmian w dziedzinie certyfikacji cyberbezpieczeństwa |
| 1100 | Art. 58 ust. 8 pkt a | 8. Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa ma co najmniej następujące uprawnienia do:  a) żądania od jednostek oceniających zgodność, posiadaczy europejskich certyfikatów cyberbezpieczeństwa oraz podmiotów, które wydały unijne deklaracje zgodności przekazania wszelkich informacji, których organ ten potrzebuje do wykonywania swoich zadań; | Art. 59x | Art. 59x. Podmiot, o którym mowa w art. 59b ust. 1 pkt 3-4, na wniosek ministra właściwego do spraw informatyzacji, przedstawia informacje dotyczące:  1) produktu ICT, usługi ICT lub procesu ICT, dla którego został wydany certyfikat lub deklaracja zgodności;  2) wyjaśnienia związane z funkcjonowaniem krajowego systemu certyfikacji cyberbezpieczeństwa  3) liczby wydanych certyfikatów w tym programów w ramach których zostały wydane oraz poziomów uzasadnienia zaufania do których się odwoływały;  4) liczby wydanych deklaracji zgodności w tym programów w ramach których zostały wydane;  5) liczby i sposobu rozpatrzenia skarg o których mowa w art. 59za. |
| 1. 100011 | Art. 58  ust. 8  pkt 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;  c) stosowania odpowiednich środków, zgodnie z prawem krajowym, w celu zapewnienia, by jednostki oceniające zgodność, posiadacze europejskich certyfikatów cyberbezpieczeństwa i podmioty, które wydały unijne deklaracje zgodności przestrzegali niniejszego rozporządzenia lub zachowywali zgodność z danym europejskim programem certyfikacji cyberbezpieczeństwa;  d) uzyskania dostępu do pomieszczeń jednostek oceniających zgodność oraz posiadaczy europejskich certyfikatów cyberbezpieczeństwa do celów prowadzenia postępowań zgodnie z prawem procesowym Unii lub państwa członkowskiego; | Art. 59y – zc | Art. 59y. 1. Minister właściwy do spraw informatyzacji, w ramach nadzoru, o którym mowa w art. 59b ust. 2, prowadzi kontrole wobec jednostek oceniających zgodność oraz dostawców produktów ICT, usług ICT lub procesów ICT.  2. Do kontroli, o której mowa w ust. 1, realizowanej wobec podmiotów:  1) będących przedsiębiorcami stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców;  2) niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej określające zasady i tryb przeprowadzania kontroli.  Art. 59z. Przepisy art. 55-59 stosuje się odpowiednio do kontroli, przeprowadzanej u przedsiębiorców, w ramach krajowego systemu certyfikacji cyberbezpieczeństwa.  Art. 59za. 1. Jednostki oceniające zgodność publikują na swojej stronie internetowej informacje o procedurze postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881. Procedura postępowania ze skargami określa termin załatwienia sprawy oraz przebieg procesu rozpatrywania skargi.  2. Skargę składa się w terminie 14 dni od dnia doręczenia rozstrzygnięcia. Jednostki oceniające zgodność mogą określić dłuższy termin na złożenie skargi.  3. Skargę rozpatrują osoby, które nie brały udziału w podejmowaniu rozstrzygnięcia, którego dotyczy skarga.  4. Jednostka oceniająca zgodność na każdym etapie informuje skarżącego o stanie postępowania oraz o przysługującym mu prawie skierowania sprawy do sądu.  5. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na jednostkę oceniającą zgodność.  Art. 59zb. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na podmiot, który wydał unijną lub krajową deklarację zgodności, jeśli produkt ICT, usługa ICT lub proces ICT którego dana deklaracja dotyczy nie spełnia wymogów określonych w programie certyfikacji cyberbezpieczeństwa.  Art. 59zc. Do skarg, o których mowa w art. 59 za ust. 5 oraz art. 59zb, stosuje się odpowiednio przepisy działu VIII ustawy z dnia 14 czerwca 1960 – Kodeks postępowania administracyjnego. |
|  | Art. 58 ust. 8 pkt 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. 59c  ust. 1  pkt.14  Art. 59o | Art. 59c.  1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  14) prowadzenie postępowań w zakresie cofnięcia certyfikatu;  Art. 59o. 1. Jednostka oceniająca zgodność po przeprowadzeniu certyfikacji przesyła do ministra właściwego do spraw informatyzacji wniosek o zatwierdzenie certyfikatu wydanego:  1) w ramach europejskiego programu certyfikacji w przypadku, gdy dany certyfikat odwołuje się do poziomu zaufania „wysoki”;  2) w ramach krajowego programu certyfikacji cyberbezpieczeństwa w przypadku, gdy dany certyfikat odwołuje się do krajowego poziomu uzasadnienia zaufania „wysoki”.  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 ustawą lub programami, o których mowa w ust. 1;  3. We wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, wskazuje się jaki produkt ICT, usługa ICT albo proces ICT podlegał certyfikacji oraz w ramach którego europejskiego lub krajowego programu certyfikacji cyberbezpieczeństwa była przeprowadzana certyfikacja.  4. Do wniosku o zatwierdzenie certyfikatu, o którym mowa w ust. 1, dołącza się dokumenty poświadczające przebieg procesu oceny zgodności.  5. Jeżeli wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, zawiera braki formalne, organ administracji publicznej wzywa organ wnioskujący do ich uzupełnienia w terminie czternastu dni od dnia doręczenia wezwania.  6. Jeżeli organ wnioskujący nie uzupełni w terminie braków formalnych wniosek o zatwierdzenie certyfikatu, o którym mowa w ust. 1, nie podlega rozpatrzeniu i jest zwracany organowi wnioskującemu.  7. Minister właściwy do spraw informatyzacji cofa certyfikat, jeśli jest on niezgodny z rozporządzeniem 2019/881, europejskim lub krajowym programem certyfikacji cyberbezpieczeństwa lub z ustawą.  8. Zatwierdzenie, odmowa zatwierdzenia oraz cofnięcie certyfikatu następuje w drodze decyzji. |
|  | Art. 58 ust. 8 pkt f | f) nakładania kar zgodnie z prawem krajowym, jak przewidziano w art. 65, oraz żądania natychmiastowego zaprzestania naruszeń obowiązków określonych w niniejszym rozporządzeniu. | Art. 59 c ust. 1 pkt 2 oraz Art. 73 ust. 1a-1c | Art. 59c  1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  2) monitorowanie wdrażania i stosowania przepisów w zakresie dotyczącym krajowego systemu certyfikacji cyberbezpieczeństwa, rozporządzenia 2019/881 oraz postanowień krajowych i europejskich programów certyfikacyjnych;  Art. 73  1a. Jednostka oceniająca zgodność, która:  1) nie przekazuje informacji, o których mowa w art. 59l i art. 59u ust. 3 lub przekazuje je nieprawdziwe lub niekompletne,  2) nie wykonuje obowiązku określonego w art. 59z ust. 1  - podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego 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 przepisów o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”.  1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotnego przeciętnego wynagrodzenia.  1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:  1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59x, podlega karze pieniężnej w wysokości do dwudziestokrotnego przeciętnego wynagrodzenia,  2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59x, podlega karze pieniężnej w wysokości do piętnastokrotnego przeciętnego wynagrodzenia,  3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,  4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji  - podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego przeciętnego wynagrodzenia. |
|  | 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 i procesów ICT. | Art. 59c  ust. 1 pkt 9 | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  9) współpraca z krajowymi organami do spraw certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym przez wymianę informacji w zakresie zgodności produktów ICT, usług ICT lub procesów ICT, z wymogami rozporządzenia 2019/881 lub z wymogami określonych europejskich lub krajowych programów certyfikacji cyberbezpieczeństwa; |
|  | Art. 59 | 1. W celu uzyskania równoważnych norm w całej Unii w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności krajowe organy ds. certyfikacji cyberbezpieczeństwa podlegają wzajemnemu przeglądowi.  2. Wzajemny przegląd przeprowadza się w oparciu o rzetelne i przejrzyste kryteria i procedury oceny, w szczególności w odniesieniu do wymagań dotyczących struktury, zasobów ludzkich i procedur, poufności i skarg.  3. W ramach wzajemnego przeglądu ocenia się:  a) w stosownych przypadkach – czy działalność krajowych organów ds. certyfikacji cyberbezpieczeństwa związana z wydawaniem europejskich certyfikatów cyberbezpieczeństwa, o których mowa w art. 56 ust. 5 lit. a) i art. 56 ust. 6, jest ściśle oddzielona od działalności związanej z nadzorem określonej w art. 58 i czy te działalności są wykonywane niezależnie od siebie;  b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT i procesów ICT z europejskimi certyfikatami cyberbezpieczeństwa na podstawie art. 58 ust. 7 lit. a);  c) procedury nadzorowania i egzekwowania obowiązków wytwórców lub dostawców produktów ICT, usług ICT lub procesów ICT na podstawie art. 58 ust. 7 lit. b);  d) procedury monitorowania, wydawania zezwoleń na działalność i nadzorowania działalności jednostek oceniających zgodność;  e) w stosownych przypadkach – czy członkowie personelu organów i jednostek wydających certyfikaty o poziomie uzasadnienia zaufania „wysoki” zgodnie z art. 56 ust. 6 mają odpowiednią wiedzę fachową.  4. Wzajemny przegląd musi być przeprowadzany przez co najmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisję i musi być przeprowadzany co najmniej raz na pięć lat. ENISA może uczestniczyć we wzajemnym przeglądzie.  5. Komisja może przyjmować akty wykonawcze ustanawiające plan wzajemnego przeglądu obejmujący okres co najmniej pięciu lat, ustanawiające kryteria dotyczące składu zespołu ds. wzajemnego przeglądu, metodykę wykorzystywaną do wzajemnego przeglądu, harmonogram, częstotliwość oraz inne zadania związane z wzajemnym przeglądem. Przyjmując te akty wykonawcze, Komisja należycie uwzględnia stanowisko ECCG. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.  6. Wyniki wzajemnych przeglądów analizuje ECCG, która sporządza podsumowania, które można podawać do wiadomości publicznej, i która, w razie potrzeby, wydaje wytyczne lub zalecenia dotyczące działań lub środków, jakie mają podjąć zainteresowane podmioty. | Art. 59c ust. 1 pkt 4 | Art. 59c. 1. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  4)przeprowadzanie wzajemnego przeglądu o którym mowa art. 59 rozporządzenia 2019/881 |
|  | Art. 60  ust. 1-2 | 1. Jednostki oceniające zgodność są akredytowane przez krajowe jednostki akredytujące wyznaczone na podstawie rozporządzenia (WE) nr 765/2008. Akredytacji takiej udziela się jedynie wtedy, gdy jednostki oceniające zgodność spełniają wymagania określone w załączniku do niniejszego rozporządzenia.  2. W przypadku gdy europejski certyfikat cyberbezpieczeństwa wydawany jest przez krajowy organ ds. certyfikacji cyberbezpieczeństwa na podstawie art. 56 ust. 5 lit. a) i art. 56 ust. 6, jednostkę certyfikującą krajowego organu ds. certyfikacji cyberbezpieczeństwa akredytuje się jako jednostkę oceniającą zgodność na podstawie ust. 1 niniejszego artykułu.  . | Art. 59h | Art. 59h.  1. Jednostka oceniająca zgodność podlega akredytacji na podstawie ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.  2. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.  3. Informacja o udzielonej akredytacji, o której mowa w ust. 1, zawiera:  1) oznaczenie podmiotu, któremu udzielono akredytacji;  2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.  4. Akredytacji udziela się na okres nie dłuższy niż 5 lat.  5. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o cofnięciu akredytacji, o której mowa w ust. 1.  6. Informacja o cofnięciu akredytacji, o której mowa w ust. 1, zawiera:  1) oznaczenie podmiotu, któremu cofnięto akredytację;  2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;  3) wskazanie daty cofnięcia akredytacji. |
|  | 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. 59i | Art. 59i. 1. W przypadku, gdy:  1) europejski program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi, o których mowa w art. 54 ust. 1 lit. f rozporządzenia 2019/881,  2) krajowy program certyfikacji cyberbezpieczeństwa określa szczególne lub dodatkowe wymogi o których mowa w art. 59g pkt 4  - minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na wykonywanie zadań w ramach takich programów wyłącznie jednostkom oceniającym zgodność spełniającym te wymogi.  2. Minister właściwy do spraw informatyzacji może cofnąć, ograniczyć lub zawiesić zezwolenie, o którym mowa w ust. 1, jeśli podmiot naruszył postanowienia ustawy, rozporządzenia 2019/881 lub europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa. Cofnięcie, ograniczenie lub zawieszenie zezwolenia, o którym mowa w ust. 1, następuje w drodze decyzji. |
|  | 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. 59d oraz  art. 59h | Art. 59d. Polskie Centrum Akredytacji sprawuje nadzór nad jednostkami oceniającymi zgodność, w zakresie spełniania przez nie wymagań, o których mowa w art. 24 ust. 3 ustawy z dnia 13 kwietnia 2016 r. o systemie oceny zgodności i nadzoru rynku (Dz. U. z 2019 r. poz. 544 oraz z 2020 r. poz. 1086) oraz w załączniku nr 1 do rozporządzenia 2019/881.  Art. 59h. 1. Jednostka oceniająca zgodność podlega akredytacji na podstawie ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku.  2. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o udzielonej akredytacji z zakresu krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.  3. Informacja o udzielonej akredytacji, o której mowa w ust. 1, zawiera:  1) oznaczenie podmiotu, któremu udzielono akredytacji;  2) wskazanie zakresu, daty wydania oraz okresu ważności udzielonej akredytacji.  4. Akredytacji udziela się na okres nie dłuższy niż 5 lat.  5. Polskie Centrum Akredytacji informuje ministra właściwego do spraw informatyzacji o cofnięciu akredytacji, o której mowa w ust. 1.  6. Informacja o cofnięciu akredytacji, o której mowa w ust. 1, zawiera:  1) oznaczenie podmiotu, któremu cofnięto akredytację;  2) wskazanie przyczyny uzasadniającej cofnięcie akredytacji;  3) wskazanie daty cofnięcia akredytacji. |
|  | Art. 62 | 1. Ustanawia się Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa („ECCG”).  2. W skład ECCG wchodzą przedstawiciele krajowych organów ds. certyfikacji cyberbezpieczeństwa lub przedstawiciele innych odpowiednich organów krajowych. Członek ECCG nie może reprezentować więcej niż dwóch państw członkowskich.  3. Interesariusze i odpowiednie strony trzecie mogą być zapraszani na posiedzenia ECCG i do udziału w jej pracach.  4. ECCG ma następujące zadania:  a) doradzanie i pomaganie Komisji przy pracach nad zapewnieniem spójnego wprowadzania i stosowania niniejszego tytułu, w szczególności w odniesieniu do unijnego kroczącego programu prac, kwestii związanych z polityką certyfikacji cyberbezpieczeństwa, koordynacji koncepcji politycznych oraz przygotowywania europejskich programów certyfikacji cyberbezpieczeństwa;  b) pomaganie, doradzanie i współpracowanie z ENISA w związku z przygotowywaniem propozycji programu na podstawie art. 49;  c) wydawanie opinii na temat propozycji programu przygotowanej przez ENISA na podstawie art. 49 niniejszego rozporządzenia;  d) zwracanie się do ENISA z wnioskiem o przygotowanie propozycji programu na podstawie art. 48 ust. 2;  e) wydawanie skierowanych do Komisji opinii dotyczących utrzymania i przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa;  f) monitorowanie odpowiednich zmian w dziedzinie certyfikacji cyberbezpieczeństwa oraz wymiana informacji i dobrych praktyk odnoszących się do programów certyfikacji cyberbezpieczeństwa;  g) ułatwianie współpracy pomiędzy krajowymi organami ds. certyfikacji cyberbezpieczeństwa w ramach niniejszego tytułu poprzez budowanie zdolności, wymianę informacji, a w szczególności poprzez ustanowienie metod efektywnej wymiany informacji związanych z kwestiami dotyczącymi certyfikacji cyberbezpieczeństwa;  h) wspieranie w zakresie wdrażania mechanizmów wzajemnej oceny zgodnie z zasadami ustanowionymi w danym europejskim programie certyfikacji cyberbezpieczeństwa na podstawie art. 54 ust. 1 lit. u);  i) ułatwianie dostosowywania europejskich programów cyberbezpieczeństwa do międzynarodowo uznanych norm, w tym przez dokonywanie przeglądu istniejących europejskich programów certyfikacji cyberbezpieczeństwa i, w stosownych przypadkach, wydawanie skierowanych do ENISA zaleceń dotyczących podjęcia współpracy z odpowiednimi międzynarodowymi organizacjami normalizacyjnymi w celu wyeliminowania braków lub luk w istniejących międzynarodowo uznanych normach.  5. Komisja, z pomocą ENISA, przewodniczy ECCG i zapewnia ECCG obsługę sekretariatu, zgodnie z art. 8 ust. 1 lit. e). | Art. 59c  ust. 1  pkt 13 | Art. 59c. Organem administracji rządowej właściwym w sprawach certyfikacji cyberbezpieczeństwa jest minister właściwy do spraw informatyzacji, do którego zadań należy:  13) uczestnictwo w pracach ECCG |
|  | Art. 63 | 1. Osoby fizyczne i prawne mają prawo do wniesienia skargi do podmiotu, który wydał europejski certyfikat cyberbezpieczeństwa lub, w przypadku gdy skarga dotyczy europejskiego certyfikatu cyberbezpieczeństwa wydanego przez jednostkę oceniającą zgodność, działającą zgodnie z art. 56 ust. 6 – do odpowiedniego krajowego organu ds. certyfikacji cyberbezpieczeństwa.  2. Organ lub jednostka, do których wniesiono skargę, informuje skarżącego o stanie postępowania i podjętej decyzji, a także informuje skarżącego o prawie do skutecznego środka prawnego przed sądem, o którym mowa w art. 64. | Art. 59za | Art. 59za. 1. Jednostki oceniające zgodność publikują na swojej stronie internetowej informacje o procedurze postępowania ze skargami, o których mowa w art. 63 rozporządzenia 2019/881. Procedura postępowania ze skargami określa termin załatwienia sprawy oraz przebieg procesu rozpatrywania skargi.  2. Skargę składa się w terminie 14 dni od dnia doręczenia rozstrzygnięcia. Jednostki oceniające zgodność mogą określić dłuższy termin na złożenie skargi.  3. Skargę rozpatrują osoby, które nie brały udziału w podejmowaniu rozstrzygnięcia, którego dotyczy skarga.  4. Jednostka oceniająca zgodność na każdym etapie informuje skarżącego o stanie postępowania oraz o przysługującym mu prawie skierowania sprawy do sądu.  5. Każdy może złożyć do ministra właściwego do spraw informatyzacji skargę na jednostkę oceniającą zgodność. |
| 1. 10 | Art. 65 | Państwa członkowskie ustanawiają przepisy o karach nakładanych w przypadku naruszenia niniejszego tytułu i naruszenia europejskich programów certyfikacji cyberbezpieczeństwa oraz stosują wszelkie niezbędne środki, aby zapewnić ich wykonanie. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie niezwłocznie powiadamiają Komisję o tych przepisach i środkach, a następnie powiadamiają ją o wszelkich zmianach mających wpływ na te przepisy. | Art. 73  ust. 1a-1c | 1a. Jednostka oceniająca zgodność, która:  1) nie przekazuje informacji, o których mowa w art. 59l i art. 59u ust. 3 lub przekazuje je nieprawdziwe lub niekompletne,  2) nie wykonuje obowiązku określonego w art. 59za ust. 1  - podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego 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 przepisów o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych, zwanego dalej „przeciętnym wynagrodzeniem”.  1b. Jednostka oceniająca zgodność, która wydaje certyfikat dla produktów ICT, usług ICT lub procesów ICT niespełniających wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa podlega karze pieniężnej w wysokości stanowiącej równowartość do dwudziestokrotnego przeciętnego wynagrodzenia.  1c. Osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która:  1) uniemożliwia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, podlega karze pieniężnej w wysokości do dwudziestokrotnego przeciętnego wynagrodzenia,  2) utrudnia właściwym organom prowadzenie czynności kontrolnych w ramach nadzoru, o którym mowa w art. 59y, podlega karze pieniężnej w wysokości do piętnastokrotnego przeciętnego wynagrodzenia,  3) wprowadza klientów w błąd co do spełnienia przez produkt ICT, usługę ICT lub proces ICT wymagań określonych w krajowym lub europejskim programie certyfikacji cyberbezpieczeństwa,  4) działa jako jednostka oceniająca zgodność bez wymaganej akredytacji  - podlega karze pieniężnej w wysokości stanowiącej równowartość do dziesięciokrotnego przeciętnego wynagrodzenia. |