UZASADNIENIE

1. Cel i potrzeba wydania ustawy

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), zwane dalej „rozporządzeniem 2019/881", ustanowiło europejskie ramy certyfikacji cyberbezpieczeństwa, wprowadzając możliwość tworzenia europejskich programów certyfikacyjnych oraz wspólne zasady w zakresie uzyskiwania certyfikatów. Dzięki temu certyfikaty z zakresu cyberbezpieczeństwa będą automatycznie honorowane na całym obszarze Unii Europejskiej, co zapobiegnie rozdrobnieniu rynku w tej dziedzinie i ułatwi działania przedsiębiorcom z poszczególnych krajów. Do tej pory certyfikacja w obszarze cyberbezpieczeństwa była obszarem nieuregulowanym, w którym miały zastosowanie ogólne zasady prawa cywilnego i prawa umów.

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

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

Ponadto, w ramach uzupełnienia europejskiego systemu certyfikacji, zostaną również wprowadzone krajowe schematy certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. W tym zakresie występuje już wiele certyfikatów prywatnych, które są wykorzystywane na rynku. Bardzo trudno jest jednak zweryfikować prawdziwą wartość takiego certyfikatu, ponieważ każdorazowo ustala to właściciel takiego „programu certyfikacji". W efekcie często certyfikaty nie realizują swojej

funkcji informowania o produktach spełniających określone normy. W związku z tym konieczne jest wprowadzenie oficjalnych schematów certyfikacji cyberbezpieczeństwa, określonych w przepisach, których zasady przyznawania i wymogi będą zawarte w przepisach prawa. Takie regulacje przyjęte w postaci niewiążącej, np. uchwały, nie będą spełniały podobnej roli, gdyż nie będą formalnie różnić się od certyfikatów prywatnych.

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

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

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

Takie rozwiązanie jest zgodne z rozporządzeniem 2019/881 w zakresie, w jakim odnosi się ono do krajowych schematów certyfikacji cyberbezpieczeństwa. Rozporządzenie to odnosi się do nich tylko w kontekście programów dotyczących produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które są również objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa. W takim wypadku krajowe schematy certyfikacji cyberbezpieczeństwa odnoszące się do tych produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa przestają działać, a państwo nie może przyjmować nowych programów. W związku z tym wprowadzenie krajowych

schematów certyfikacyjnych odnoszących się do osób oraz systemów zarządzania cyberbezpieczeństwem nie będzie w żaden sposób kolidowało z przepisami rozporządzenia 2019/881 w tym zakresie, gdyż będą one dotyczyły innych obszarów merytorycznych.

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

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

Krajowy system certyfikacji cyberbezpieczeństwa będzie stanowił zbiór podmiotów, o których mowa w art. 3 ust. 2 (ministra właściwego do spraw informatyzacji; Polskie Centrum Akredytacji, zwane dalej „PCA"; jednostki oceniające zgodność; 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; osoby fizyczne, które poddają swoją wiedzę i umiejętności praktyczne ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa; podmioty, które poddają wykorzystywane przez siebie systemy zarządzania cyberbezpieczeństwem ocenie zgodności w ramach danego krajowego schematu certyfikacji cyberbezpieczeństwa), oraz procedur związanych z certyfikacją produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w ramach europejskich programów certyfikacji cyberbezpieczeństwa albo krajowych schematów certyfikacji cyberbezpieczeństwa oraz procedur w zakresie certyfikacji systemów certyfikacji cyberbezpieczeństwa lub osób fizycznych w ramach krajowych schematów certyfikacji cyberbezpieczeństwa, wspierających:

1) wytwarzanie wysokiej jakości produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa;
2) budowę systemów zarządzania cyberbezpieczeństwem;
3) zapewnienie:
a) wykwalifikowanych specjalistów w obszarze cyberbezpieczeństwa,
b) spełniania przez produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa wymogów w zakresie ochrony dostępności, autentyczności, integralności i poufności przetwarzanych danych,
c) bezpieczeństwa oferowanych lub dostępnych produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa w trakcie ich całego cyklu życia oraz powiązanych z nimi funkcji.

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

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

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

Rozporządzenie 2019/881 przewiduje trzy poziomy uzasadnienia zaufania – podstawowy, istotny i wysoki, określające poziom cyberbezpieczeństwa, jaki gwarantuje dany

produkt. W odniesieniu do każdego z tych poziomów będą określane odrębne wymagania, jakie musi spełniać produkt, by uzyskać certyfikat danego poziomu. Wymagania dla konkretnych produktów będą zawarte w określonych europejskich programach certyfikacji cyberbezpieczeństwa. Każdy z wydawanych certyfikatów będzie musiał wskazywać, jakiego poziomu dotyczy. Również szczegóły związane z opisem wymagań bezpieczeństwa i procesem badania produktów będą określane w europejskich programach certyfikacji.

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

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

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

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

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

Przyjęte zostały rozwiązania oparte na otwarciu rynku i nie została wyznaczona jedna państwowa jednostka oceniająca zgodność, która wydawałaby certyfikaty odwołujące się do poziomu uzasadnienia zaufania „wysoki”. Przyjęcie alternatywnego rozwiązania mogłoby stanowić barierę w rozwoju prywatnych jednostek oceniających zgodność. Alternatywne

rozwiązanie w tym zakresie nie pozwala więc osiągnąć wszystkich celów projektowanej ustawy w zakresie rozwoju rynku certyfikacji w Polsce.

Krajowy organ do spraw certyfikacji cyberbezpieczeństwa będzie dysponował:

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

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

2. Omówienie projektowanych przepisów

Zakres ustawy

Projektowana ustawa określa organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, a także sposób sprawowania nadzoru, kontroli i koordynacji w zakresie stosowania przepisów ustawy.

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

Definicje

Projektowana ustawa wprowadza szereg definicji odwołujących się do rozporządzenia 2019/881 oraz innych aktów prawa unijnego. Zapewnia to niezbędną precyzję wykorzystywanych w ustawie sformułowań oraz zapobiega powstaniu wątpliwości interpretacyjnych. Na potrzeby ustawy będzie wykorzystywana nowa definicja cyberbezpieczeństwa, która została zawarta w rozporządzeniu 2019/881. Należy podkreślić, że ta definicja będzie wykorzystywana jedynie na potrzeby niniejszej ustawy, gdyż definiuje ona cyberbezpieczeństwo inaczej niż w podstawowej dla tego obszaru ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 i 1222), zwaną dalej „uksc". Harmonizacja obu tych obszarów nastąpi w momencie implementacji do polskiego porządku prawnego dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14

grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2), tzw. dyrektywy NIS2, co ma zostać dokonane poprzez przyjęcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (UC32). Zgodnie z obowiązującą dziś definicją cyberbezpieczeństwa zawartą w art. 2 ust. 4 uksc, cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i niezaprzeczalność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Przyjęte rozwiązanie pozwoli na wprowadzenie przepisów o certyfikacji bez konieczności czekania na wejście w życie innych aktów prawnych.

Projektowana ustawa przewiduje też wprowadzenie pojęcia krajowych schematów certyfikacji cyberbezpieczeństwa, które będą obejmować zarówno krajowe programy certyfikacji zdefiniowane w art. 2 pkt 10 rozporządzenia 2019/881, jak również dokumenty określające wymogi z zakresu cyberbezpieczeństwa na potrzeby certyfikacji osób oraz systemów zarządzania cyberbezpieczeństwem. Wprowadzenie pojęcia „schematu" jest konieczne, aby możliwe było przygotowanie dokumentów analogicznych dla programów certyfikacji dla osób i systemów zarządzania, a zarazem zachować zgodność z prawem europejskim, które określa, że krajowe programy certyfikacji mogą dotyczyć tylko produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.

Określenie celu krajowego systemu certyfikacji cyberbezpieczeństwa i jego podmiotów

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

Dobrowolność certyfikacji

Przepisy projektowanej ustawy wskazują, że certyfikacja produktów ICT, usług ICT, procesów

ICT i usług zarządzanych w zakresie bezpieczeństwa będzie odbywać się dobrowolnie, na podstawie umowy zawartej między dostawcą, a jednostką oceniającą zgodność. Podstawą dla tej umowy będą wymogi zawarte w odpowiednim krajowym schemacie certyfikacji cyberbezpieczeństwa lub europejskim programie certyfikacji cyberbezpieczeństwa. Ponadto krajowe schematy certyfikacji cyberbezpieczeństwa będą umożliwiały również certyfikację osób oraz systemów zarządzania cyberbezpieczeństwem. Umowa będzie podstawą wzajemnych zobowiązań pomiędzy jednostką oceniającą zgodność, a jej klientami, w szczególności będzie określała cenę za usługi jednostki oceniającej zgodność. Równocześnie jednak bardzo wiele elementów samego procesu oceny zgodności będzie określone w konkretnym programie certyfikacji oraz w przepisach go dotyczących. Ponadto, w projektowanych przepisach przesądzono jakie kwestie będzie musiała określać umowa o certyfikację. W szczególności umowa będzie musiała regulować zagadnienia związane z ochroną informacji przekazywanych przez klienta, w tym ochronę tajemnic przedsiębiorstwa. Certyfikacja będzie więc procesem dobrowolnym, o rozpoczęciu którego będzie każdorazowo decydował podmiot dysponujący danym produktem ICT, usługą ICT, procesem ICT, usługą zarządzaną w zakresie bezpieczeństwa, systemem zarządzania czyberbezpieczeństwem czy osoba fizyczna, która chce poddać swoją wiedzę i umiejętności ocenie zgodności. Wskazano również wyraźnie, że ocena zgodności w ramach europejskiego programu certyfikacji cyberbezpieczeństwa będzie dotyczyła wymogów określonych w przewidzianym dla jednego z trzech poziomów uzasadnienia zaufania – podstawowego, istotnego i wysokiego. Poziomy te są zdefiniowane w art. 52 rozporządzenia 2019/881. Im wyższy poziom uzasadnienia zaufania, tym większą gwarancję bezpieczeństwa daje produkt ICT, usługa ICT, proces ICT lub usługa zarządzane w zakresie bezpieczeństwa która została certyfikowana. To, jakiego poziomu będzie dotyczyła certyfikacja, będzie określone w umowie między dostawcą a jednostką oceniającą zgodność. W ramach krajowych schematów certyfikacji cyberbezpieczeństwa nie będzie osobnych poziomów uzasadnienia zaufania. Zamiast nich będą jednolite wymogi dla danych produktów, usług, procesów czy systemów zarządzania cyberbezpieczeństwem oraz osób.

Krajowe certyfikaty cyberbezpieczeństwa

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

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

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

W przypadku krajowych certyfikatów dotyczących osób sprawdzenie ich kompetencji będzie następować w drodze testu wiedzy i umiejętności praktycznych.

Zastosowane metody pozwolą kompleksowo sprawdzić przedmiot certyfikacji i ocenić spełnienie przez niego wymagań określonych w schemacie.

Każdy certyfikat będzie wskazywał dla kogo został wydany, w ramach jakiego schematu certyfikacji cyberbezpieczeństwa, okres na który został wydany, a także przedmiot certyfikacji oraz datę jego wydania i podpis. Ponadto każdy certyfikat będzie posiadał swoje indywidualne oznaczenie. Każdy certyfikat będzie wydawany na wzorze ustalonym dla danego schematu. Zapewni to transparentność certyfikatów, ułatwi posługiwanie się nimi oraz pozwoli na skuteczną promocję krajowych schematów certyfikacji cyberbezpieczeństwa.

Krajowy certyfikat będzie mógł być wydawany na okres nie krótszy niż 2 lata i nie dłuższy niż 5 lat. Cyberbezpieczeństwo to obszar bardzo szybko rozwijający się, gdzie ciągle pojawiają się nowe technologie i związane z nimi zagrożenia. W związku z tym certyfikat wydany wcześniej może już nie być gwarancją odpowiedniego poziomu cyberbezpieczeństwa. Równocześnie minimalny czas ważności certyfikatu musi być na tyle długi by miał on znaczenie na rynku. Podmiot, który otrzymał certyfikat będzie mógł wnioskować o jego przedłużenie. W takim wypadku krajowy schemat certyfikacji cyberbezpieczeństwa będzie przewidywał, jakie czynności są niezbędne do utrzymania certyfikatu. Pozwoli to uniknąć powtarzania całego procesu certyfikacji, co ograniczy koszty i ułatwi działanie przedsiębiorców w tym obszarze. Dla zapewnienia prawidłowego przebiegu procesu certyfikacji podmiot ubiegający się o certyfikat będzie obowiązany do przekazania jednostce oceniającej zgodność wszystkich niezbędnych informacji związanych z przedmiotem certyfikacji. Jest to niezbędne dla prawidłowego przebiegu procesu certyfikacji oraz monitorowania czy przedmiot certyfikacji spełnia wymogi przez cały okres na jaki został wydany certyfikat.

Projektowana ustawa przewiduje, że dokumentacja techniczna dotycząca przedmiotu certyfikacji będzie musiała być przechowywana przez okres 10 lat od wygaśnięcia certyfikatu. Jest to niezbędne dla potrzeb monitorowania i ewentualnej kontroli prawidłowości działań jednostek oceniających zgodność.

Środki zaradcze

W przypadku wykrycia niezgodności w produkcie ICT, usłudze ICT, procesie ICT, usłudze zarządzanej w zakresie bezpieczeństwa lub systemie zarządzania cyberbezpieczeństwem, dla którego został wydany krajowy certyfikat, posiadacz tego certyfikatu będzie musiał przedstawić w ciągu 14 dni propozycję działań zaradczych, które przywrócą zgodność z wymogami krajowego schematu certyfikacji cyberbezpieczeństwa. Następnie będzie musiał, we współpracy z jednostką, która wydała certyfikat, przeprowadzić te działania i zapewnić zgodność z wymogami danego krajowego schematu certyfikacji cyberbezpieczeństwa w ciągu 2 miesięcy. W przypadku, gdy posiadacz krajowego certyfikatu nie zrealizuje tych obowiązków, jednostka oceniająca zgodność cofa certyfikat. To rozwiązanie gwarantuje, że po wykryciu niezgodności posiadacz certyfikatu nie będzie go od razu tracił, ale będzie mógł przywrócić zgodność z wymogami. Dzięki temu nie będzie musiał przechodzić ponownie całego procesu certyfikacji, co ograniczy koszty, jakie będzie musiał ponieść.

Tworzenie krajowych schematów certyfikacji cyberbezpieczeństwa

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

Celem krajowych schematów certyfikacji cyberbezpieczeństwa będzie zapewnienie, by produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa

certyfikowane zgodnie z takimi schematami, spełniały określone wymogi w celu ochrony dostępności, autentyczności, integralności i poufności przechowywanych, przekazywanych lub przetwarzanych danych lub powiązanych funkcji bądź usług oferowanych lub dostępnych za pośrednictwem tych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa na poziomie ustawy. Produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami ICT, usługami ICT, procesami ICT lub usługami zarządzanymi w zakresie bezpieczeństwa są tak zróżnicowane, że opracowanie ogólnych wymogów cyberbezpieczeństwa obowiązujących dla wszystkich przypadków jest bardzo skomplikowane, w szczególności mając na uwadze, że dotyczy to tak różnych produktów jak drukarki, programy komputerowe czy usługi chmurowe. Metody osiągania celów cyberbezpieczeństwa w przypadku określonych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa należy doprecyzować na poziomie poszczególnych schematów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych w przypadku, gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować krajowe schematy certyfikacji cyberbezpieczeństwa do konkretnych produktów, zapewni ich skuteczność.

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

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

Rola PCA

Projektowana ustawa wprowadza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne PCA. Aby prowadzić ocenę zgodności produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa systemów

zarządzania cyberbezpieczeństwem oraz osób, zainteresowane podmioty będą musiały uzyskać akredytację PCA. Wymagania dla zainteresowanych zostały określone w załączniku nr 1 do rozporządzenia 2019/881. Podstawą działania PCA w tym zakresie będzie rozdział 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Są to przepisy, na podstawie których PCA działa w innych gałęziach gospodarki, w związku z czym nie będzie to wymagało dodatkowego przygotowania ze strony PCA.

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

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

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

Zadania ministra

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

Minister będzie dysponował również uprawnieniami w zakresie przeprowadzania kontroli przestrzegania przepisów projektowanej ustawy w zakresie certyfikacji cyberbezpieczeństwa. W tym zakresie będą stosowane przepisy dotychczas zawarte w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dzięki temu możliwe będzie prowadzenie efektywnego nadzoru praktycznie od początku obowiązywania projektowanej ustawy.

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

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

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

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

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

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

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

Zlecanie wykonania określonych czynności na rzecz ministra

Rynek certyfikacji cyberbezpieczeństwa jest obszarem wymagającym wysokich kwalifikacji oraz specjalistycznej wiedzy. Minister będzie rozwijał swoje zdolności w tym zakresie, ale również ze względu na różnorodność programów certyfikacyjnych, do realizacji swoich zadań będzie musiał korzystać z wiedzy ekspertów zewnętrznych. Podstawowym źródłem takiej wiedzy będą państwowe instytuty badawcze, które są nadzorowane przez tego ministra,

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

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

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

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

Regulacją tą będą objęte również jednostki organizacyjne podległe Ministerstwu Obrony Narodowej. Jednostki te również mają doświadczenie w obszarze certyfikacji cyberbezpieczeństwa w związku z czym uwzględnienie ich w ramach krajowego systemu

certyfikacji cyberbezpieczeństwa pozwoli na lepszą koordynację polityki państwa w tym obszarze.

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

Projektowane przepisy zapewniają ponadto podstawę prawną do zlecania określonych czynności podmiotom innym niż państwowe instytuty badawcze. Jak wskazano powyżej rozwój europejskich programów certyfikacji może spowodować, że konieczne będzie wykorzystanie kompetencji w obszarze, w którym instytuty badawcze nie dysponują odpowiednią wiedzą. Innym przykładem sytuacji, w której zastosowanie tego przepisu będzie konieczne, to sytuacja konfliktu interesów, np. jeśli minister będzie musiał ocenić czynności dokonane przez któryś z instytutów badawczych. W takiej sytuacji musi istnieć możliwość skorzystania z wiedzy innych podmiotów. Jest to jednak szczególna sytuacja i podstawowymi podmiotami wspierającymi ministra mają być państwowe instytuty badawcze. Jest to niezbędne dla zapewnienia skutecznej realizacji zadań krajowego organu administracji rządowej właściwego w sprawach certyfikacji cyberbezpieczeństwa w niezwykle szybko zmieniającym się obszarze cyberbezpieczeństwa. W związku z wprowadzonymi zmianami, dla zapewnienia spójności przepisów, zostanie wskazane w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2024 r. poz. 534), że wsparcie ministra właściwego do spraw informatyzacji w tym obszarze należy do kompetencji instytutów badawczych.

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

Zezwolenie na prowadzenie oceny zgodności

Projektowana ustawa reguluje sytuację, w której określony europejski program certyfikacji cyberbezpieczeństwa przewiduje specjalne wymagania dla jednostek oceniających zgodność. W takim przypadku oprócz akredytacji jednostki te będą musiały uzyskać zezwolenia ministra. Zezwolenia wynikają wprost z obowiązku wdrożenia rozporządzenia 2019/881. Jeśli bowiem europejskie programy certyfikacyjne będą zawierały postanowienia o szczególnych wymaganiach w zakresie jednostek oceniających zgodność, musi istnieć organ sprawdzający te wymagania oraz zezwalający na działanie jednostek w ramach określonego programu certyfikacji. Należy podkreślić, że w związku z tym, że postępowanie to dotyczy spełnienia formalnych kryteriów, zdecydowano o zastosowaniu w tym przypadku przepisów ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego dotyczących

postępowania uproszczonego. Pozwoli to maksymalnie przyśpieszyć postępowanie oraz ograniczy formalności. Minister w ramach sprawowanego nadzoru będzie mógł również zmieniać zakres udzielonego zezwolenia, jak również je cofnąć w przypadku, gdy dana jednostka przestanie spełniać określone wymagania. Gwarantuje to zachowanie odpowiedniej jakości usług świadczonych przez jednostki oceniające zgodność.

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

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

Trzyletni termin dotyczący przesłanki powtarzania się niezgodności został przyjęty tak, aby nie mogła wystąpić sytuacja, w której w danym podmiocie ciągle występuje to samo naruszenie.

Równocześnie uwzględniona została długość procesu oceny zgodności, który w przypadku bardziej skomplikowanych metodologii, jak np. w programie EUCC, może trwać nawet powyżej roku.

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

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

Rezygnacja z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy

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

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

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

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

Projektowane przepisy ustawy wprowadzają dodatkową gwarancję dla certyfikatów najwyższego poziomu. Wydanie takiego certyfikatu będzie możliwe tylko po otrzymaniu zgody ministra na jego wydanie. Zezwolenie będzie wydane po wydaniu decyzji certyfikacyjnej przez jednostkę oceniającą zgodność, ale przed wydaniem certyfikatu. Na tym etapie sam proces certyfikacji został już zakończony i można ocenić prawidłowość jego przeprowadzenia. Odmowa wydania zezwolenia jest możliwa w przypadku, gdy certyfikat został wydany wbrew przepisom rozporządzenia 2019/881, ustawy lub postanowieniom określonego europejskiego

programu certyfikacji cyberbezpieczeństwa, w ramach którego prowadzona była procedura. Do postępowania będą stosowane przepisy ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, które zapewnią niezbędne gwarancje procesowe dla jego stron. Do wniosku o zatwierdzenie takiego certyfikatu muszą być dołączone dokumenty potwierdzające przebieg procesu oceny zgodności. Projektowane przepisy przewidują ponadto, że w przypadku, gdy będzie to konieczne, minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów naukowych o wypowiedzenie się w kwestii danego programu certyfikacji. Wymóg ten służy przyśpieszeniu postępowania przez przekazanie do ministra potrzebnych mu dokumentów wraz z wnioskiem wszczynającym postępowanie. Bez tego przepisu minister musiałby wystąpić do jednostki, która wydała certyfikat o te dokumenty, co przedłużyłoby cały proces.

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

W celu zapewnienia możliwości usunięcia nieprawidłowości minister cofa certyfikat jedynie w przypadku jeżeli wykryte nieprawidłowości:

a) mają znaczący wpływ na dostępność, autentyczność, integralność lub poufność danych, sieci i systemów informatycznych danego podmiotu wykorzystującego system zarządzania cyberbezpieczeństwem lub

b) mają znaczący wpływ na użytkownika produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa lub

c) są nieodwracalne.

Każdy z tych trzech przypadków jest związany z zagrożeniem dla użytkowników danych produktów i usług czy kontrahentów podmiotów, które poddały certyfikacji swoje systemy zarządzania cyberbezpieczeństwem. W związku z powyższym w takich przypadkach konieczne jest podjęcie zdecydowanych działań i cofnięcie certyfikatu. W innych przypadkach certyfikat zostanie zawieszony, a jego posiadacz będzie miał możliwość usunięcia nieprawidłowości. W przypadku gdy w wyznaczonym terminie nie będzie w stanie tego uczynić certyfikat zostanie

cofnięty. Takie rozwiązanie pozwoli na zapewnienie trwałości wydanych certyfikatów. Możliwość usunięcia niewielkich niezgodności będzie dodatkową zachętą do inwestowania w europejskie i krajowe certyfikaty cyberbezpieczeństwa.

Zgodnie z art. 147 ust. 2 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2024 r. poz. 1045 i 1841), doręczenie korespondencji nadanej przez osobę fizyczną lub podmiot niebędący podmiotem publicznym, będące użytkownikami konta w ePUAP, do podmiotu publicznego posiadającego elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne w skutkach prawnych z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego, do czasu zaistnienia obowiązku stosowania ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, przez ten podmiot publiczny. Innymi słowy do czasu rozpoczęcia stosowania przez ministra przepisów ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych sprzeciw będzie mógł być złożony na jego elektroniczną skrzynkę podawczą ePUAP. W związku ze zmianą rozporządzenia 2019/881 przepisy te objęły również certyfikaty wydane dla usług zarządzanych w zakresie bezpieczeństwa. Zmiana ta jest niezbędna dla zapewnienia prawidłowego wykonania prawa europejskiego. Zapewni to również jednolite traktowanie wszystkich europejskich certyfikatów odwołujących się do poziomu uzasadnienia zaufania „wysoki".

Przekazanie informacji o wydaniu lub cofnięciu certyfikatu

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

Rozpatrywanie skarg

Każdy będzie mógł złożyć skargę na działania jednostki certyfikującej. Dokładną procedurę postępowania z taką skargą będą określały same jednostki oceniające zgodność i publikowały ją na swoich stronach internetowych. Będą jednak musiały zagwarantować, że skargę rozpatrują inne osoby niż te, które podejmowały dane działanie podjęte podczas certyfikacji. Rozstrzygnięcie skargi nie może trwać dłużej niż 2 miesiące, co gwarantuje, że decyzja zostanie podjęta w odpowiednim terminie. Możliwość zgłaszania skarg do jednostek wydających certyfikaty gwarantuje art. 63 rozporządzenia 2019/881. Równocześnie jest to rozwiązanie elastyczne, które pozwoli jednostkom oceniającym zgodność ustalić procedury dostosowane do ich wewnętrznej struktury. Projektowana ustawa wskazuje, że minister jest organem

właściwym do rozpatrywania skarg na podmioty, które wydały deklaracje zgodności zgodnie z określonym europejskim programem certyfikacji cyberbezpieczeństwa. Takie skargi umożliwią ministrowi wszczęcie postępowań kontrolnych w przypadku uzasadnionych podejrzeń, że produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa dla których wystawiono deklarację zgodności, nie spełnia wymagań zawartych w określonym europejskim programie certyfikacji cyberbezpieczeństwa. To uprawnienie dla ministra wynika wprost z przepisów rozporządzenia 2019/881. Należy zauważyć, że przepisy dotyczące skarg tworzą tylko ogólne ramy dla rozpatrywania skarg. Szczegółowo kwestie te będą regulowane w rozporządzeniach wykonawczych wydawanych przez Komisję Europejską dla poszczególnych programów certyfikacyjnych. Należy podkreślić, że będą one odrębnie określane dla każdego kolejnego programu co sprawia, że konieczne jest pozostawienie wielu kwestii nieuregulowanych w przepisach krajowych. Skargi składane do ministra rozpatrywane będą zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Ze względu na to, że będą one dotyczyły jednostek niezależnych od ministra wskazano, że przepisy te będą stosowane odpowiednio.

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

Obie opisane procedury skargowe są od siebie niezależne i mogą być stosowane równolegle.

Przekazywanie informacji do ministra

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

Kontrola

Przepisy projektowanej ustawy ustanawiają podstawę prawną dla prowadzenia przez ministra kontroli podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Do kontroli przeprowadzanej wobec podmiotów administracyjnych będą stosowane przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. z 2020 r. poz. 224), a wobec przypadku przedsiębiorców – przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo

przedsiębiorców (Dz. U. z 2024 r. poz. 236, 1222 i 1871 oraz z 2025 r. poz. 222). W związku z tym, prawa strony postępowania będą odpowiednio chronione. Pozwoli to na skuteczną realizację obowiązków nadzorczych. Przepisy o kontroli nie będą dotyczyły osób fizycznych, które poddały swoją wiedzę i umiejętności ocenie w ramach krajowych schematów certyfikacji cyberbezpieczeństwa. Wskazane przepisy dotyczące kontroli odnoszą się do organizacji i w związku z tym nie byłoby możliwe zastosowanie ich do osób. Ponadto, nie służą one sprawdzaniu wiedzy i kompetencji osób.

Zasady prowadzenia kontroli

Projektowana ustawa wskazuje, że do kontroli będą stosowane odpowiednio przepisy art. 55–59 uksc. Dzięki temu minister będzie mógł oprzeć się na dotychczasowej praktyce w zakresie prowadzenia kontroli, co pozwoli na najszybsze wdrożenie się do nowych obowiązków. W art. 55 pkt 1–6 uksc wskazany jest zakres uprawnień przysługujących osobom przeprowadzającym kontrolę. Warto zaznaczyć, że uprawnienia wynikające z art. 55 uksc dotyczą tylko czynności wykonywanych w celu przeprowadzenia kontroli w określonym zakresie. Nie jest dopuszczalne, aby korzystać z danych uprawnień rozszerzająco, np. na czynności związane z innymi kontrolami. Biorąc pod uwagę zakres działania niektórych przedsiębiorców objętych ustawą (którzy mogą należeć również do infrastruktury krytycznej), konieczne jest zaakcentowanie, że uprawnienia te nie mogą być nadużywane przez kontrolerów celem dostępu do pomieszczeń czy dokumentów niezwiązanych z zakresem kontroli. Swobodny dostęp jest ograniczony celem i zakresem kontroli. Przepis art. 57 uksc wskazuje, że osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Przebieg przeprowadzonej kontroli osoba przeprowadzająca kontrolę ma przedstawić w protokole kontroli (art. 58 uksc). W sposób szczegółowy opisano także treść protokołu kontroli. Zasadą jest, iż protokół podpisują osoba przeprowadzająca kontrolę oraz osoba reprezentująca podmiot kontrolowany. Podmiot kontrolowany może zgłosić do protokołu pisemne zastrzeżenia, które osoba przeprowadzająca czynności kontrolne jest obowiązana przeanalizować i w razie potrzeby podjąć dodatkowe czynności kontrolne. W przypadku odmowy podpisania protokołu przez podmiot kontrolowany osoba przeprowadzająca czynności kontrolne czyni o tym wzmiankę w protokole. W art. 59 uksc wskazano, że jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia wskazanych nieprawidłowości. Natomiast podmiot kontrolowany jest obowiązany w wyznaczonym terminie, poinformować organ właściwy lub

ministra o sposobie wykonania zaleceń. Pozwala bowiem podmiotowi kontrolowanemu na usunięcie wskazanych w protokole kontroli naruszeń, co z kolei może pozwolić mu na uniknięcie nałożenia kary pieniężnej.

Uprawnienie do badania produktów ICT

Dla zapewnienia realnej kontroli nad jakością produktów, które otrzymały certyfikaty, minister został wyposażony w uprawnienia do przeprowadzania badań produktów ICT, usług ICT, procesów ICT, usług zarządzanych w zakresie bezpieczeństwa oraz systemów zarządzania cyberbezpieczeństwem. W zakresie analizy technicznej produktów ICT minister będzie mógł zwrócić się do nadzorowanych przez siebie instytutów badawczych o wykonanie określonych czynności. Tego typu uprawnienie jest niezbędne dla zapewnienia realnego nadzoru nad jakością produktów na rynku. Należy podkreślić, że obecnie przygotowywane rozporządzenia wykonawcze Komisji Europejskiej, w których wprowadzane są programy certyfikacyjne, mają nakładać na krajowe organy do spraw certyfikacji obowiązek przeprowadzenia określonych liczby badań produktów. W związku z tym konieczne jest zapewnienie ministrowi odpowiedniego uprawnienia.

Procedura pobierania próbek i badania produktów ICT

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

Konsekwencje niespełniania wymagań po certyfikacji

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

Kary administracyjne

Projektowana ustawa przewiduje nałożenie kary administracyjnej na jednostkę oceniającą zgodność za działanie bez wymaganej akredytacji. Przypadki niewypełnienia innych

obowiązków, np. informacyjnych, utrudnianie przeprowadzenia kontroli, również są penalizowane w podobny sposób. Odpowiedzialności podlegać będą ponadto m.in. osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, które utrudniają lub uniemożliwiają właściwym organom prowadzenie czynności kontrolnych. Wysokość kar administracyjnych została odpowiednio zróżnicowana tak, by były one skuteczne, proporcjonalne do czynu oraz odstraszające. Kary będzie nakładał minister w ramach swojej roli jako krajowego organu do spraw certyfikacji cyberbezpieczeństwa. Kary będą stanowiły przychód Funduszu Cyberbezpieczeństwa. Pozwoli to zapewnić dodatkowe środki dla tego Funduszu i przyczyni się do wzrostu cyberbezpieczeństwa w podmiotach administracji publicznej. W związku z powyższym w ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1662) uzupełniono katalog przychodów Funduszu Cyberbezpieczeństwa o kary wydawane na podstawie projektowanej ustawy.

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

Przepisy przejściowe i dostosowujące

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

Reguła wydatkowa

Projektowana ustawa określa również limit wydatków na nowe zadania realizowane przez ministra. Wydatkowanie środków na cele rozwoju krajowego organu do spraw cyberbezpieczeństwa oraz publicznych jednostek oceniających zgodność rozpocznie się w 2025 r. Oznacza to konieczność zatrudnienia dodatkowych osób oraz zapewnienia im narzędzi pracy. W kolejnych latach wzrost wydatków wynika z zapewnienia możliwości certyfikacji w jednostkach publicznych oraz opłacenia zewnętrznych opinii.

Zmiany w innych ustawach

Konieczne jest również dostosowanie innych ustaw do rozwiązań zawartych w projektowanej ustawie. Pierwszą taką ustawą jest ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych, w której do katalogu działań jakie mogą podejmować instytuty badawcze, zostanie dodane wspieranie ministra właściwego do spraw informatyzacji w sprawach nadzoru nad krajowym systemem certyfikacji cyberbezpieczeństwa. Konkretne zadania w tym zakresie znajdują się w projektowanej ustawie. Ze względu na to, że są to zadania wymagające specjalistycznej wiedzy i kompetencji to instytuty badawcze są najlepiej przygotowanymi do tego zadania podmiotami. Zmiana ta jest również niezbędna dla zapewnienia spójności systemu prawnego.
Drugą niezbędną zmianą jest zmiana ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w której do katalogu przychodów Funduszu Cyberbezpieczeństwa zostaną dodane wpływy z kar pieniężnych, zawartych w projektowanej ustawie. Tę kwestię merytorycznie przesądza już ww. projekt, a zmiana w ustawie o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa służy zapewnieniu spójności obu tych regulacji.

Wejście w życie

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

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

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

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

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