UZASADNIENIE

1. Cel i potrzeba 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 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.

Projektowane rozwiązania zakładają mieszany model certyfikacji cyberbezpieczeństwa, w którym podstawową rolę odgrywają podmioty prywatne. Certyfikacja w dziedzinie cyberbezpieczeństwa będzie odbywała się na zasadach rynkowych, a klienci będą mogli swobodnie wybierać spośród podmiotów działających na rynku.

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 oraz procesów ICT.

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. 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 lub procesu ICT, równocześnie nie będąc do tego zobowiązanym.

Projektowane rozwiązania służą również realizacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zwanej dalej „Strategią”. Ustanowienie krajowego organu do spraw certyfikacji cyberbezpieczeństwa oraz utworzenie krajowego systemu certyfikacji cyberbezpieczeństwa stanowią działania służące realizacji drugiego celu szczegółowego Strategii – podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. 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). Stosowane 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 zarówno z potrzeby dania impulsu do rozwoju rynku w obszarze certyfikacji oraz zapewnienie konsumentom bezpiecznych produktów ICT, usług ICT oraz procesów ICT, 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.

Nowe przepisy stworzą również ramy tworzenia i funkcjonowania krajowych programów certyfikacji cyberbezpieczeństwa. Umożliwi to wpływanie na bezpieczeństwo produktów ICT, usług ICT oraz procesów ICT również w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Będzie to również szansa dla rozwoju rynku certyfikacja oraz tworzenie usług dostosowanych ściśle do potrzeb krajowego rynku oraz jego specyfiki. Również ta certyfikacja będzie całkowicie dobrowolna.

Krajowy system certyfikacji cyberbezpieczeństwa będzie też stanowił cenne uzupełnienie krajowego systemu cyberbezpieczeństwa. Stworzy bowiem precyzyjny system oceny produktów ICT, usług ICT oraz procesów ICT, 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.

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.

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 i kontroli 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 tym akcie prawnym i jest bezpośrednio stosowana. Projektowana ustawa skupia się więc na ustanowieniu roli organów państwa w tym obszarze oraz uszczegółowieniu środków kontroli i nadzoru.

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 lica 2028 r. o krajowym systemie cyberbezpieczeństwie (Dz. U. z 2023 r. poz. 913 i 1703). 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. Przyjęte rozwiązanie pozwoli na wprowadzenie przepisów o certyfikacji bez konieczności czekania na wejście w życie innych aktów prawnych.

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 Polskie Centrum Akredytacji, minister właściwy do spraw informatyzacji, zwany dalej „ministrem”, zainteresowane jednostki oceniające zgodność oraz przedsiębiorcy certyfikujący swoje produkty. 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 dostawców.

Dobrowolność certyfikacji

Przepisy projektowanej ustawy wskazują, że certyfikacja produktów ICT, usług ICT i procesów ICT będzie odbywać się dobrowolnie, na podstawie umowy zawartej między dostawcą,

a jednostką oceniającą zgodność. Certyfikacja będzie więc procesem dobrowolnym, o rozpoczęciu którego będzie każdorazowo decydował podmiot dysponujący danym produktem ICT, usługą ICT czy procesem ICT. Wskazano również wyraźnie, że ocena zgodności będzie dotyczyła wymogów określonych w europejskim programie certyfikacji cyberbezpieczeństwa 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 lub proces ICT, który został certyfikowany. To, jakiego poziomu będzie dotyczyła certyfikacja, będzie określone w umowie między dostawcą, a jednostką oceniającą zgodność.

Krajowe programy certyfikacji cyberbezpieczeństwa

Krajowe programy 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. Dzięki temu programy certyfikacyjne będą brały pod uwagę konkretne potrzeby przedsiębiorców oraz będą promować w tym zakresie najlepsze rozwiązania z tej dziedziny. Podstawą działania krajowego systemu certyfikacji cyberbezpieczeństwa będą jednak europejskie programy certyfikacyjne, dlatego też przepis dający ministrowi uprawnienie do tworzenia krajowych programów certyfikacji cyberbepieczeństwa został ukształtowany jako fakultatywny. Gwarantuje to zapewnienie zgodności z prawem europejskim. Krajowe programy certyfikacyjne będą mogły być wydawane w sytuacji, gdy zostanie to uznane za korzystne dla rozwoju certyfikacji w Polsce. Przygotowanie projektu krajowego programu 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 czy Instytut Łączności. Rozporządzenia te będą wzorowane na rozporządzeniach z art. 9 i art. 10 ustawy z dnia 13 kwietnia 2016 r**.** o systemie oceny zgodności.

Celem krajowych programów certyfikacji cyberbezpieczeństwa będzie zapewnienie, by produkty ICT, usługi ICT lub procesy ICT, certyfikowane zgodnie z takimi programami, 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 lub procesów ICT w trakcie ich całego cyklu życia. Nie jest możliwe szczegółowe określenie wymogów cyberbezpieczeństwa odnoszących się do wszystkich produktów ICT,

usług ICT i procesów ICT na poziomie ustawy. Produkty ICT, usługi ICT lub procesy ICT oraz potrzeby w zakresie cyberbezpieczeństwa powiązane z tymi produktami ICT, usługami ICT lub procesami ICT 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 lub procesów ICT należy doprecyzować na poziomie poszczególnych programów certyfikacji, na przykład przez odesłanie do norm lub specyfikacji technicznych w przypadku, gdy nie istnieją odpowiednie normy. Tylko takie indywidualne podejście, które pozwoli dostosować programy do konkretnych produktów, zapewni skuteczność tych programów. Należy wskazać, że ta różnorodność wpływa na wszelkie aspekty krajowych programów 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 programie może wymagać zupełnie różnych metod. Ponadto każdy z programów będzie musiał być opracowywany przez innych ekspertów tak, by był jak najlepiej dostosowany do ściśle określonej dziedziny, której dotyczy.

Rola Polskiego Centrum Akredytacji

Projektowana ustawa wprowadza obowiązek akredytacji dla jednostek oceniających zgodność oraz wskazuje obowiązki informacyjne Polskiego Centrum Akredytacji, zwanego dalej „PCA". Aby prowadzić badania produktów ICT, usług ICT i procesów ICT 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.

Zadania ministra

Projektowana ustawa określa zadania ministra. Zadania te wynikają wprost z przepisów rozporządzenia 2019/881 i dotyczą nadzoru i 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) zatwierdzania 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. – Kodeksu 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 programów 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 programów.

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 Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, dalej „NASK–PIB", oraz Instytut Łączności. 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 programów certyfikacji cyberbezpieczeństwa.

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 informatzyacji w wykonywaniu zadań związanych z certyfikację cyberbezpieczeństwa. Gwarantuje to, że w kluczowym obszarze cyberbezpieczeństwa będzie możliwe wykorzystanie pełnego potencjału wiedzy, jaki posiadają państwowe instytuty

badawcze.

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.

Projektowany przepis zapewnia 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.

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, iż 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.

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. W przypadku, 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 powyższym 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 powyższym konieczne było ustanowienie odpowiedniej procedury w przepisach krajowych.

Zatwierdzanie certyfikatów odwołujących się do poziomu uzasadnienia zaufania wysoki

Przepisy projektowanej ustawy wprowadzają dodatkową gwarancję dla certyfikatów najwyższego poziomu. Taki certyfikat musi być zatwierdzony przez ministra. Odmowa zatwierdzenia 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.

Zgodnie z art. 147 ust. 2 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2023 r. poz. 285, 1860 i 2699) 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. Obecnie na mocy komunikatu Ministra Cyfryzacji z dnia 21 grudnia 2023 r. zmieniającego komunikat w sprawie określenia terminu wdrożenia rozwiązań technicznych niezbędnych do doręczania korespondencji z wykorzystaniem publicznej usługi rejestrowanego doręczenia elektronicznego lub publicznej usługi hybrydowej oraz udostępnienia w systemie teleinformatycznym punktu dostępu do usług rejestrowanego doręczenia elektronicznego w ruchu transgranicznym (Dz. U. poz. 2764) termin wdrożenia m.in. rozwiązań technicznych umożliwiających doręczanie przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego został wydłużony do dnia 1 października 2024 r. Jest to kolejne odroczenie ww. terminu, w związku z tym podjęto decyzję o dodaniu

przepisu przejściowego, w myśl którego do czasu wdrożenia przez ministra ww. rozwiązań technicznych doręczenie wniosku o zatwierdzenie certyfikatu na elektroniczną skrzynkę podawczą w ePUAP, w ramach usługi udostępnianej w ePUAP, jest równoważne z doręczeniem przy wykorzystaniu publicznej usługi rejestrowanego doręczenia elektronicznego.

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.

Rozpatrywanie skarg

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 lub proces ICT, dla którego 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.

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). W związku z tym prawa strony postępowania będą odpowiednio chronione. Pozwoli to na skuteczną realizację obowiązków nadzorczych.

Zasady prowadzenia kontroli

Projektowana ustawa wskazuje, że do kontroli będą stosowane odpowiednio przepisy art. 55–59 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, dalej „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. 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.

Wykrycie, że produkt ICT, usługa ICT lub proces ICT nie spełnia wymagań

Przepisy projektowanej ustawy określają uprawnienia ministra w przypadku, gdy okaże się, że określony produkt ICT, usługa ICT lub proces ICT nie spełnia wymagań określonych zawartych w określonym europejskim albo krajowym programie 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.

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 Sądu Okręgowego w Warszawie – Sądu Ochrony Konkurencji i Konsumentów. 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.

Reguła wydatkowa

Projektowana ustawa określa również limit wydatków na nowe zadania realizowane przez ministra. Wydatki przewidziane w 2024 r. dotyczą jedynie utworzenia w urzędzie obsługującym ministra zdolności do skutecznej realizacji zadań krajowego organu do spraw certyfikacji cyberbezpieczeństwa. 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.

Wejście w życie

Projektowana ustawa wejdzie w życie po upływie miesiąca od dnia jej ogłoszenia. Taki termin gwarantuje, że wszystkie podmioty, których dotyczą przygotowywane 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.

Projekt ustawy stosownie do wymogów art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) oraz zgodnie z § 52 ust. 1 uchwały nr 190 Rady Ministrów z dnia 29 października 2013 r. – Regulamin pracy Rady Ministrów (M.P. z 2022 r. poz. 348) został zamieszczony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji