Informacja w sprawie ustawy z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa

Celem ustawy jest dostosowanie polskiego porządku prawnego do obowiązków wynikających z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej do spraw Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), zwanego dalej „rozporządzeniem 2019/881".

Ustawa określa organizację krajowego systemu certyfikacji cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, w tym sposób sprawowania nadzoru nad działalnością podmiotów tego systemu, kontroli działalności tych podmiotów oraz koordynacji ich działalności. Ustawa zmierza ponadto do podniesienia poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcia zdolności do skutecznego zapobiegania i reagowania na incydenty.

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.

Zgodnie z ustawą krajowy system certyfikacji cyberbezpieczeństwa będzie stanowił zbiór podmiotów, o których mowa w art. 3 ust. 2 ustawy (minister właściwy do spraw informatyzacji, Polskie Centrum Akredytacji, zwane dalej „PCA", jednostki oceniające zgodność, dostawcy, 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 oraz 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. 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 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. Przepisy ustawy 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.

Ustawa pozwala również tworzyć krajowe schematy certyfikacji cyberbezpieczeństwa w obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Krajowe schematy certyfikacji cyberbezpieczeństwa będą mogły dotyczyć również systemów zarządzania cyberbezpieczeństwem oraz osób fizycznych. Dzięki temu przedsiębiorcy uzyskają możliwość otrzymania certyfikatu na cały stosowany u siebie system zarządzania cyberbezpieczeństwem. Z kolei certyfikaty dla poszczególnych osób fizycznych pozwolą potwierdzić posiadane kompetencje z zakresu cyberbezpieczeństwa. Kontrolę w podmiotach należących do krajowego systemu certyfikacji cyberbezpieczeństwa będzie przeprowadzał organ nadzorczy, którym będzie minister właściwy do spraw informatyzacji, zwany dalej „ministrem”. Minister będzie dysponował uprawnieniami do przeprowadzania kontroli u podmiotów krajowego systemu cyberbezpieczeństwa, do badania produktów ICT, usług ICT, procesów ICT oraz usług zarządzanych w zakresie bezpieczeństwa oraz uzyskiwania od podmiotów krajowego systemu cyberbezpieczeństwa informacji związanych z certyfikowanymi produktami, usługami i procesami.

Przepisy 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 (art. 5). Podstawą dla tej umowy będą wymogi zawarte w odpowiednim krajowym schemacie

certyfikacji cyberbezpieczeństwa lub europejskim programie certyfikacji cyberbezpieczeństwa. Umowa będzie podstawą wzajemnych zobowiązań między jednostką oceniającą zgodność a jej klientami. Ustawa wskazuje elementy, jakie będzie musiała określać umowa o certyfikację.

Zgodnie z ustawą 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. Krajowy certyfikat cyberbezpieczeństwa będzie mógł być wydany również osobie fizycznej, która posiada wiedzę i umiejętności praktyczne gwarantujące skuteczną realizację zadań z zakresu cyberbezpieczeństwa (art. 7 ust. 2). Krajowy certyfikat będzie mógł być wydawany na okres nie krótszy niż 2 lata i nie dłuższy niż 5 lat.

Istotną rolę w krajowym systemie certyfikacji cyberbezpieczeństwa ma odgrywać Polskie Centrum Akredytacji, zwane dalej „PCA", które będzie sprawowało nadzór w zakresie udzielonej akredytacji nad jednostkami oceniającymi zgodność w obszarze objętym danym europejskim programem certyfikacji cyberbezpieczeństwa albo danym krajowym schematem certyfikacji cyberbezpieczeństwa. Podstawą działania PCA w tym zakresie będzie rozdział 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku. Jednostki oceniające zgodność będą mogły prowadzić ocenę zgodności i wydawać certyfikaty w ramach krajowych schematów certyfikacji cyberbezpieczeństwa oraz europejskich programów certyfikacji cyberbezpieczeństwa. Przyjęty model zakłada, że będą one mogły wydawać certyfikaty odnoszące się do wszystkich poziomów zaufania, o których mowa w rozporządzeniu 2019/881. Minister będzie natomiast wyrażał zgodę na wydanie certyfikatów odwołujących się do poziomu zaufania „wysoki".

Ustawa wprowadza kary pieniężne za nierealizowanie określonych obowiązków (art. 33), w szczególności za:

- nieprzekazanie ministrowi określonych danych albo przekazanie danych niepełnych lub nieprawdziwych przez jednostkę oceniającą zgodność (w wysokości dziesięciokrotności przeciętnego wynagrodzenia);

- wydanie europejskiego certyfikatu albo krajowego certyfikatu przez jednostkę oceniającą zgodność działającą bez wymaganej akredytacji (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia);
- uniemożliwianie albo utrudnianie ministrowi przeprowadzenia kontroli (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia);
- brak udostępnienia unijnej deklaracji zgodności, dokumentacji technicznej i innych wymaganych informacji związanych ze zgodnością produktów ICT lub usług ICT z unijnym programem certyfikacji cyberbezpieczeństwa (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia);
- nieprzekazanie przeprowadzającemu kontrolę próbki produktu ICT (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia);
- nierealizowanie obowiązku publicznego udostępniania dodatkowych informacji na temat cyberbezpieczeństwa, zgodnie z art. 55 rozporządzenia 2019/881 (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia);
- nieprzekazanie ministrowi w terminie informacji na temat produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa, dla których zostały wydane europejski certyfikat, deklaracja zgodności lub krajowy certyfikat, a także na temat liczby wydanych certyfikatów (w wysokości do dwudziestokrotności przeciętnego wynagrodzenia).

Ustawa wprowadza ponadto niezbędne zmiany w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych, ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz ustawie z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

W przepisach przejściowych i dostosowujących ustawa przesądza, że akredytacje udzielone przez PCA jednostkom oceniającym zgodność w zakresie cyberbezpieczeństwa do dnia wejścia w życie ustawy stają się akredytacjami w rozumieniu uchwalonej ustawy. PCA w terminie 14 dni od dnia wejścia w życie ustawy będzie obowiązane poinformować ministra właściwego do spraw informatyzacji o akredytacjach udzielonych do dnia wejścia ustawy w życie. Z kolei certyfikaty wydane w ramach akredytacji udzielonych przed dniem wejścia ustawy w życie będą obowiązywały do końca terminu ich ważności. Znajdą do nich zastosowanie przepisy dotychczasowe. Jednostki oceniające zgodność w terminie 14 dni od dnia wejścia w życie ustawy poinformują ministra właściwego do spraw informatyzacji o wydanych certyfikatach. Ustawa określa limit wydatków z budżetu państwa dla części

budżetowej 27 – informatyzacja oraz wydatków PCA w latach 2025–2034, będących skutkiem finansowym jej wejścia w życie.

Ustawa wejdzie w życie po upływie 30 dni od dnia ogłoszenia.