Nazwa projektu Ustawa o krajowym systemie certyfikacji cyberbezpieczeństwa **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Paweł Olszewski, Sekretarz Stanu **Kontakt do opiekuna merytorycznego projektu** Łukasz Wojewoda, dyrektor Departamentu Cyberbezpieczeństwa e-mail: Sekretariat.DC@cyfra.gov.pl Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa e-mail: Sekretariat.DC@cyfra.gov.pl	**Data sporządzenia** 20.05.2024 r. **Źródło:** 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) (Dz. Urz. UE L 151 z 07.06.2019, str. 15) **Nr w wykazie prac: UC42**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowana ustawa ma na celu dostosowanie polskiego porządku prawnego do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia 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), zwanym dalej „rozporządzeniem 2019/881". Stanowi również realizację celu szczegółowego 2. Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 – podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty.

Rola sieci i systemów teleinformatycznych wzrosła niepomiernie w ostatnich latach sprawiając, że stały się one niezbędnym elementem współczesnej gospodarki. W związku z pandemią COVID-19 oraz atakiem Rosji na Ukrainę proces ten postępuje coraz szybciej. Jako, że społeczeństwa coraz bardziej będą polegały na produktach i usługach funkcjonujących w cyberprzestrzeni, tym istotniejsze staje się zapewnienie bezpieczeństwa działań podejmowanych na tej płaszczyźnie. Wprowadzenie jednolitych zasad przyznawania certyfikatów cyberbezpieczeństwa i ich wzajemne uznawanie w państwach Unii Europejskiej zapewnią, że przedsiębiorstwa będą w stanie lepiej zabezpieczyć swoje interesy w cyberprzestrzeni. Wzajemne uznawanie certyfikatów zapewni im ponadto lepszą pozycję w konkurencji na rynku europejskim. Działania te przyczynią się do ogólnego wzrostu bezpieczeństwa w cyberprzestrzeni poprzez promocję najbezpieczniejszych rozwiązań oraz dostarczenie konsumentom informacji o bezpieczeństwie produktów i usług. Wyraźne wsparcie państwa w zakresie certyfikacji powinno również przyczynić się do zwiększenia świadomości społecznej w kwestii cyberbezpieczeństwa.

Przyjęcie proponowanych przepisów może dać polskim przedsiębiorcom dużą szansę na pozyskanie klientów z sąsiednich krajów zainteresowanych certyfikacją swoich produktów. Będzie to więc szansą na znaczne poszerzenie bazy potencjalnych klientów. Z kolei producenci i dostawcy produktów uzyskają możliwość otrzymania certyfikatów dla swoich produktów i usług, które będą ważne na obszarze całej Unii Europejskiej. Należy podkreślić, że jeśli przepisy te nie zostałyby przyjęte, to polscy producenci musieliby korzystać z usług jednostek certyfikujących z innych krajów UE, co nie byłoby korzystne dla polskiej gospodarki.

Sama certyfikacja w zakresie cyberbezpieczeństwa jest procesem czasochłonnym i kosztownym, co ogranicza dostępność do certyfikatów. Wprowadzenie krajowego systemu certyfikacji powinno przyczynić się do zmiany tego stanu rzeczy.

Przyjęte w projektowanej ustawie rozwiązania umożliwią również tworzenie krajowych programów certyfikacyjnych. Dzięki temu możliwe będzie zwiększenie cyberbezpieczeństwa w obszarach uznanych za kluczowe.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Celem projektowanej ustawy jest:

1) organizacja systemu certyfikacji cyberbezpieczeństwa w Polsce, w szczególności ustanowienie procedur niezbędnych do zapewnienia prawidłowości procesów certyfikacyjnych;
2) określenie sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy.

Powyższe działania mają doprowadzić do rozwoju rynku certyfikacji cyberbezpieczeństwa w Polsce, a przez to do zwiększenia bezpieczeństwa w tej dziedzinie. Projektowana regulacja ma też ułatwić przedsiębiorstwom konkurowanie na rynku unijnym przez wzajemne uznawanie certyfikatów opartych o programy unijne.

Projektowana ustawa może też dać niezbędny impuls do rozwoju rynku certyfikacji cyberbezpieczeństwa w Polsce, który może być zdolny do przyciągnięcia klientów z całej Europy Środkowo-Wschodniej.

Należy zaznaczyć, że w Europie Środkowo-Wschodniej wiele krajów nie dysponuje zdolnościami w zakresie certyfikacji co

oznacza, że tamtejsi producenci muszą certyfikować swoje produkty za granicą. W związku z tym rozwój tego rynku w Polsce może przyczynić się do przyciągnięcia klientów z sąsiednich krajów, co będzie stanowiło dodatkowy czynnik sprzyjający rozwojowi rynku certyfikacji, jak również zwiększy renomę kraju na arenie międzynarodowej. Ponadto, dzięki wprowadzeniu krajowych programów certyfikacji cyberbezpieczeństwa będzie możliwe wspieranie cyberbezpieczeństwa produktów w określonych obszarach nieobjętych europejskimi programami certyfikacji cyberbezpieczeństwa. Zapewni to zachętę dla producentów do zapewnienia cyberbezpieczeństwa produktów w danych obszarach.

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 oraz uzyskiwania od tych podmiotów informacji związanych z certyfikowanymi produktami. Będzie również uczestniczył w pracach na forum Unii Europejskiej z tym związanych, zwłaszcza w ramach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa. W zakresie certyfikatów odwołujących się do poziomu zaufania „wysoki" minister będzie posiadał uprawnienia do zatwierdzania każdego wydanego certyfikatu. Projektowane rozwiązanie jest gwarantem, że ocena zgodności na najwyższym poziomie bezpieczeństwa będzie przeprowadzana zgodnie z najlepszymi standardami w tej dziedzinie. Model, w którym minister pełni taką rolę pojawia się w wielu krajach Europy, m.in. w Niderlandach, gdzie certyfikaty wydawane są przez jednostki prywatne pod nadzorem jednego z ministerstw. Przyjęty model był tam bardzo efektywny, gdyż Niderlandy wydawały ok. 3 razy więcej certyfikatów niż inne kraje uczestniczące w porozumieniu Common Criteria. Dlatego model ten został przyjęty za wzór dla proponowanych rozwiązań.

Istotną rolę będzie odgrywało również Polskie Centrum Akredytacji, zwane dalej „PCA", które będzie nadzorowało akredytowane podmioty. Podstawą działania PCA w tym zakresie będzie rozdział 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854). 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. Jednostki oceniające zgodność będą mogły prowadzić ocenę zgodności i wydawać certyfikaty w ramach europejskich programów certyfikacji cyberbezpieczeństwa. Przyjęty model zakłada, że będą one mogły wydawać certyfikaty odnoszące się do wszystkich poziomów zaufania. Certyfikaty odwołujące się do poziomu zaufania „wysoki" będą następnie zatwierdzane przez ministra. Takie rozwiązanie pozwoli na szeroki udział podmiotów prywatnych w procesie oceny zgodności, a równocześnie zagwarantuje prawidłowość procesów oceny zgodności na najwyższym poziomie uzasadnienia zaufania. Krajowe jednostki akredytacyjne będą pełnić podobną rolę w każdym państwie Unii Europejskiej.

Zgodnie z rozporządzeniem 2019/881 minister będzie wydawał decyzje zezwalając na dokonywanie określonych czynności w ramach procesu oceny zgodności, jeśli określony program certyfikacji to przewiduje.

W projekcie wprowadzone zostały kary administracyjne za nierealizowanie określonych obowiązków np. za nieprzekazanie ministrowi informacji w odpowiednim terminie. Prowadzone kontrole oraz nakładane kary zapewnią wysoki poziom certyfikowanych produktów ICT, usług ICT i procesów ICT.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Francja

W ramach Francuskiej Agencji Cyberbezpieczeństwa (The National Cybersecurity Agency of France, zwana dalej ANSSI) kwestiami certyfikacji zajmuje się Narodowe Centrum Certyfikacji. Agencja ta zajmuje się również licencjonowaniem laboratoriów w tym zakresie. ANSSI zostało również wyznaczone jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z aktem o cyberbezpieczeństwie.

Sama certyfikacja czy licencjonowanie nie podlega opłatom. Osoby wnioskujące ponoszą koszty badań laboratoryjnych ich produktów. Wynoszą one zwykle 600–700 euro na dzień, a sama certyfikacja trwa ok. 25–35 dni. Podmioty obsługiwane są w kolejności złożenia wniosków co często powoduje, iż zainteresowani muszą czekać na otrzymanie usługi. Certyfikacji można dokonać również u autoryzowanych podmiotów działających na wolnym rynku.

System francuski zasadniczo różni się od przyjętego w projektowanej ustawie. Wynika to przede wszystkim z uwarunkowań instytucjonalnych.

Niemcy

Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacji (BSI) wykonuje zadania niezwykle zbliżone do zadań wynikających z rozporządzenia 2019/881, jak również posiada zadania wykonywane w Polsce przez Agencję Bezpieczeństwa Wewnętrznego. BSI został również wyznaczony jako krajowy organ ds. certyfikacji cyberbezpieczeństwa zgodnie z ww. aktem. BSI przygotowuje również krajowe programy certyfikacyjne, takie jak niemiecki szybki program certyfikacji.

Szwecja

Kwestiami certyfikacji w Szwecji zajmuje się jedna z agencji rządowych – Swedish Defence Materiel Administration. Pobierane są liczne opłaty. Sam wniosek o certyfikację podlega bezzwrotnej opłacie w wysokości 20 000 koron. Agencja ta zajmuje się również zamówieniami dla szwedzkich sił zbrojnych oraz rozwojem technologii na potrzeby wojska.

To sprzężenie kwestii cyberbezpieczeństwa w wymiarze cywilnym i wojskowym stanowi zasadniczą różnicę między polskim, a szwedzkim systemem w tym zakresie.

Włochy

Przyjęty we Włoszech model certyfikacji oparty jest na działaniach organów administracji publicznej. Certyfikaty wydawane są przez odpowiednią komórkę w Ministerstwie Rozwoju Gospodarczego. W związku z tym ten rodzaj działalności organów administracji publicznej jest finansowany w całości z budżetu państwa. Równocześnie podmioty

ubiegające się o certyfikat nie muszą wnosić opłat w związku z jego wydaniem.

Cypr

W celu wdrożenia aktu o cyberbezpieczeństwie powołany został nowy organ, który ma pełnić rolę krajowego organu ds. certyfikacji cyberbezpieczeństwa.

Niderlandy

W przyjętym w Niderlandach modelu organy państwa mają jedynie rolę nadzorczą, natomiast sama certyfikacja jest dokonywana przez prywatne podmioty. Ten model funkcjonował jeszcze przed implementacją przepisów rozporządzenia 2019/881, a Niderlandy są jednym z państw wiodących w obszarze certyfikacji cyberbezpieczeństwa. Organem państwa nadzorującym działalność certyfikacyjną jest jeden z ministrów. Jest to model bardzo zbliżony do przyjętego w projektowanej ustawie.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Minister właściwy do spraw informatyzacji	1	Informacja ogólnodostępna	Pozytywne. Minister uzyska uprawnienia kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Będzie też prowadził postępowania administracyjne w sprawach związanych z certyfikacją, np. będzie zatwierdzał certyfikaty odnoszące się do poziomu zaufania „wysoki”.
Przedsiębiorcy z branży IT	131 000	Informacja ogólnodostępna	Pozytywne. Uzyskają dostęp do certyfikatów obowiązujących w całej Unii Europejskiej. Przepisy ułatwią też rozwój własnych kompetencji w obszarze certyfikacji.
Polskie Centrum Akredytacji	1	Informacja ogólnodostępna	Pozytywne. PCA uzyska uprawnienia do prowadzenia akredytacji w nowym obszarze tematycznym.
NASK–PIB	1	Informacja ogólnodostępna	Pozytywne. Proponowane rozwiązania wiążą się z rozwijaniem zdolności certyfikacyjnych w Naukowej i Akademicka Sieć Komputerowej – Państwowym Instytucie Badawczym, dalej „NASK–PIB”, oraz innych usług z tym związanych. Obecnie jest to jedyna jednostka certyfikująca działająca w ramach metodologii Common Criteria.
Państwowe instytuty badawcze	30	Informacje ogólnodostępne	Pozytywne. Będą one realizować zadania związane z certyfikacją cyberbezpieczeństwa. Zadania te będą w wielu wypadkach realizowane odpłatnie lub ze środków ministra.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Projekt zostanie poddany konsultacjom publicznym i opiniowaniu, które będą trwały ok. 30 dni.

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), 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 2022 r. poz. 348), projekt został udostępniony w Biuletynie Informacji Publicznej na stronie

podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

W trybie przepisów ustawy z dnia 23 maja 1991 r. o związkach zawodowych (Dz. U. z 2022 r. poz. 854) oraz ustawy z dnia 23 maja 1991 r. o organizacjach pracodawców (Dz. U. z 2022 r. poz. 97) projekt został skierowany do zaopiniowania przez następujące podmioty:
1) Business Centre Club – Związek Pracodawców;
2) Federacja Przedsiębiorców Polskich;
3) Forum Związków Zawodowych;
4) Konfederacja Lewiatan;
5) Niezależny Samorządny Związek Zawodowy „Solidarność”;
6) Ogólnopolskie Porozumienie Związków Zawodowych;
7) Pracodawcy Rzeczypospolitej Polskiej;
8) Związek Przedsiębiorców i Pracodawców;
9) Związek Rzemiosła Polskiego.

W ramach konsultacji publicznych projekt został skierowany do następujących podmiotów:
1) Polskiej Izby Informatyki i Telekomunikacji;
2) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
3) Polskiej Izby Komunikacji Elektronicznej;
4) Krajowej Izby Gospodarczej;
5) Krajowej Izby Komunikacji Ethernetowej;
6) Krajowej Izby Gospodarki Cyfrowej;
7) Fundacji Bezpieczna Cyberprzestrzeń;
8) Polskiego Towarzystwa Informatycznego;
9) Związku Pracodawców Branży Internetowej IAB Polska;
10) Polskiej Rady Biznesu;
11) Naczelnej Organizacji Technicznej;
12) Związku Pracodawców Mediów Elektronicznych i Telekomunikacji Mediakom;
13) Izby Gospodarki Elektronicznej;
14) Internet Society Poland;
15) Związku Importerów i Producentów Sprzętu Elektrycznego i Elektronicznego Branży RTV i IT – ZIPSEE „Cyfrowa Polska”;
16) Polskiego Centrum Badań i Certyfikacji S.A.;
17) Polskiej Organizacji Handlu i Dystrybucji;
18) Naczelnej Rady Zrzeszeń Handlu i Usług;
19) Polskiego Stowarzyszenia Marketingu SMB;
20) Amerykańska Izba Handlowa w Polsce;
21) Krajowej Izby Rozliczeniowej;
22) Fundacja Pułaskiego;
23) Sektorowej Rada ds. Kompetencji – Telekomunikacja i Cyberbezpieczeństwo;
24) Green Rev Institute.

W ramach opiniowania projekt został skierowany do następujących podmiotów:
1) Prezesa Urzędu Komunikacji Elektronicznej;
2) Prezesa Urzędu Ochrony Konkurencji i Konsumentów;
3) Prezesa Urzędu Zamówień Publicznych;
4) Prezesa Urzędu Ochrony Danych Osobowych;
5) Prezesa Głównego Urzędu Statystycznego;
6) Rzecznika Małych i Średnich Przedsiębiorców;
7) Rzecznika Praw Obywatelskich;
8) Krajowej Rady Radiofonii i Telewizji;
9) Polskiego Komitetu Normalizacyjnego;
10) Najwyższej Izby Kontroli;
11) Agencji Bezpieczeństwa Wewnętrznego;
12) Agencji Wywiadu;
13) Biuro Bezpieczeństwa Narodowego;
14) Centralnego Biuro Antykorupcyjne;
15) Służby Kontrwywiadu Wojskowego;
16) Służby Wywiadu Wojskowego;
17) Rządowego Centrum Bezpieczeństwa;
18) Służby Ochrony Państwa;
19) Polskiego Centrum Akredytacji;

20) Naukowej i Akademickiej Sieci Komputerowej – Państwowy Instytut Badawczy;
21) Instytutu Łączności;
22) Rady Dialogu Społecznego;
23) Prezesa Prokuratorii Generalnej Rzeczypospolitej Polskiej.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem	9,715	11,596	11,61	11,627	11,645	11,665	11,685	11,706	11,728	11,751	11,776	126,504
budżet państwa	9,715	11,596	11,61	11,627	11,645	11,665	11,685	11,706	11,728	11,751	11,776	126,504
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-9,715	-11,596	-11,61	-11,627	-11,645	-11,665	-11,685	-11,706	-11,728	-11,751	-11,776	- 126,504
budżet państwa	-9,715	-11,596	-11,61	-11,627	-11,645	-11,665	-11,685	-11,706	-11,728	-11,751	-11,776	- 126,504
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Wydatki będą dokonywane z budżetu państwa w części 27 – Informatyzacja. W związku z nowymi zadaniami koniecznie będzie podwyższenie limitu wydatków z tej części. Jako rok „0” przyjęto 2025 r.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	**Utworzenie wydziału krajowego systemu certyfikacji cyberbezpieczeństwa** W ramach przyjęcia nowych zadań w zakresie certyfikacji cyberbezpieczeństwa przez ministra konieczne jest wzmocnienie urzędu obsługującego ten organ. Pierwszy europejski program certyfikacji (EUCC) będzie stosowany od 31 stycznia 2025 r., co oznacza, że pojawi się konieczność przeprowadzenia czynności administracyjnych przez krajowy organ ds. certyfikacji cyberbezpieczeństwa. Szacuje się, że będzie to jedno postępowanie w 2025 r. Z samego tego programu w 2026 r. i w kolejnych latach będzie prowadzonych około 5 czy 6 postępowań administracyjnych w ciągu roku. Obecnie trwają również prace nad kolejnymi europejskimi programami certyfikacji, z których pierwszym jest europejski program certyfikacji usług chmurowych. Przewiduje się, że wejdzie on w życie w 2026 r., co będzie wiązało się z dodatkowymi postępowaniami administracyjnymi – 1 w 2026 r. oraz 5–6 rocznie w latach kolejnych. Równocześnie od 2026 r. powstanie też konieczność przeprowadzania kontroli wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa. Zgodnie z art. 25 ust. 3 aktu implementującego EUCC[1)], krajowy organ ds. certyfikacji cyberbezpieczeństwa, we współpracy z innymi organami nadzoru rynku, corocznie poddaje kontroli wyrywkowej co najmniej 4% certyfikatów EUCC. W związku z tym wraz ze wzrostem liczby wydanych certyfikatów będzie szybko rosła liczba obowiązkowych kontroli, jakie będzie musiał przeprowadzać ten organ. Szacuje się, że będzie to: – w 2026 r. – 1 kontrola,

[1)] Rozporządzenie Wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC).

– w 2027 r. – 4 kontrole,

– od 2028 r. – 8 kontroli rocznie.

Wraz z wejściem w życie każdego kolejnego programu certyfikacji cyberbezpieczeństwa będzie pojawiała się konieczność prowadzenia dodatkowych kontroli, co będzie stanowiło znaczne obciążenie dla pracy krajowego organ ds. certyfikacji cyberbezpieczeństwa.

W związku z tym, w celu sprawnego wykonywania nowych zadań konieczne będzie utworzenie nowego wydziału i zatrudnienie pracowników od 2026 r. Pracownicy tworzonego wydziału będą zajmować się przede wszystkim prowadzeniem postępowań administracyjnych, analizą rynku i przeprowadzaniem postępowań kontrolnych. Konieczne jest wyasygnowanie środków na stanowiska naczelnika wydziału oraz 2 głównych specjalistów. Do zadań tych osób będzie również należało uczestniczenie w posiedzenia Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa oraz w grupach roboczych związanych z certyfikacją, współpraca z podmiotami międzynarodowymi i krajowymi funkcjonującymi w tym obszarze oraz udział w pracach nad kolejnymi europejskimi programami certyfikacji cyberbezpieczeństwa. Należy podkreślić, że zadania te będą wiązały się z koniecznością posiadania kompetencji nie tylko w obszarze postępowań administracyjnych i kontrolnych, ale również z zakresu cyberbezpieczeństwa. Ze względu na międzynarodowy charakter systemu certyfikacji niezbędna będzie też bardzo dobra znajomość języka angielskiego. Zadania te nie mogą być wykonane przy wykorzystaniu obecnych pracowników urzędu obsługującego ministra.

Należy zauważyć, że po wyodrębnieniu Ministerstwa Cyfryzacji, jako odrębnego urzędu, niemożliwe było pokrycie zobowiązań wynikających z potencjalnych dodatkowych 110 umów o pracę przy środkach, jakie zostały wyodrębnione z budżetu Kancelarii Prezesa Rady Ministrów. W związku z powyższym w Ministerstwie Cyfryzacji w I kwartale 2024 r. została dokonana analiza potrzeb etatowych urzędu, w wyniku której do Ministra Finansów został złożony wniosek o uruchomienie środków na wynagrodzenia z rezerwy celowej budżetu państwa z poz. 56, nie obejmuje on jednak przedmiotowych etatów. Z tego względu nałożenie na Ministra Cyfryzacji dodatkowych zadań powoduje konieczność zabezpieczenia dodatkowych środków na wynagrodzenia osobowe wraz z pochodnymi.

Koszty wynagrodzeń wyniosą od 2026 r. – 0,432 mln zł w tym pochodne[2)] w wysokości 0,07 mln zł.

Od 2027 r. będzie również wypłacane dodatkowe wynagrodzenie roczne w kwocie 33,22 tys. zł. W związku z tym całkowita kwota na rok wzrośnie do 0,432 mln zł.

Przy wyliczeniach przyjęto mnożnik kwoty bazowej w wysokości:

- 3,2 dla głównych specjalistów,
- 4,0 dla naczelnika wydziału.

Koszty wynagrodzeń 3 stanowisk w mln zł

2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0	0,399	0,432	0,432	0,432	0,432	0,432	0,432	0,432	0,432	0,432

Koszty organizacji stanowisk pracy

Koszty organizacji stanowisk pracy dla wskazanych wyżej 3 osób wyniosą w 2026 r. łącznie 36 tys. zł. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja.

Koszty organizacji stanowisk pracy

2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035

[2)] Pod pojęciem pochodne rozumie się:

- składki na ubezpieczenie emerytalne, ubezpieczenie rentowe, ubezpieczenie wypadkowe, Fundusz Pracy, Fundusz Solidarnościowy;
- a także wpłatę na Pracownicze Plany Kapitałowe.

0	0,036	0	0	0	0	0	0	0	0	0

Koszt badań

Jednym z obowiązków ministra będzie przeprowadzanie badań produktów, które otrzymały certyfikaty cyberbezpieczeństwa. Będzie się to wiązało z koniecznością zakupu usług zewnętrznych, w szczególności usług wyspecjalizowanych laboratoriów. Zgodnie z art. 25 ust. 3 aktu implementującego EUCC krajowy organ ds. certyfikacji cyberbezpieczeństwa, we współpracy z innymi organami nadzoru rynku, corocznie poddaje kontroli wyrywkowej co najmniej 4% certyfikatów EUCC. Należy spodziewać się, że kolejne programy będą zawierały analogiczne postanowienia. Przewiduje się, że koszty takich badań wyniosą 300 tys. zł w 2025 r., a w kolejnych latach kwota będzie zwiększać się o 5% w każdym kolejnym roku. Przy określaniu założonych środków przyjęto, że koszt badań będzie wynosił ok. 1/4 kosztu przeprowadzenia oceny zgodności danego produktu. W przypadku Common Criteria taki średni koszt wynosi ok. 300 tys. złotych. W związku z tym przyjęta kwota umożliwi przeprowadzenie badań czterech produktów. W przypadku poziomu zaufania wysoki taka kwota wystarczy na 1 albo 2 badania. Łącznie w latach 2025–2035 koszty wyniosą ok 4,481 mln zł. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja. Badania te będą prowadzone w ramach kontroli prowadzonych przez ministra u podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

Koszty badań produktów ICT										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,315	0,331	0,348	0,365	0,383	0,403	0,423	0,444	0,466	0,489	0,514

Przygotowanie opinii na potrzeby realizacji zadań krajowego organu ds. certyfikacji cyberbezpieczeństwa

W celu wsparcia ministra w zakresie nadzoru nad krajowym systemem certyfikacji cyberbezpieczeństwa planuje się zlecanie przygotowania opinii zewnętrznych. Koszty opinii wyniosą 30 tys. zł rocznie. Koszty te zostaną poniesione w ramach budżetu państwa z części 27 – Informatyzacja.

Przygotowanie opinii										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,03

Wpływy z kar

Przewiduje się wpływy do Funduszu Cyberbezpieczeństwa z tytułu kar płaconych przez członków krajowego systemu certyfikacji cyberbezpieczeństwa.

Zgodnie z powyższym szacuje się, że dochody z kar pojawią się w 2025 r. w wysokości 147 543 zł. W związku ze wzrostem liczby wydawanych certyfikatów przewiduje się, że kwota ta będzie wzrastać o około 5% w każdym kolejnym roku. Ponadto w następnych latach powinny zostać przyjęte kolejne europejskie programy certyfikacyjne, co przełoży się na znaczny wzrost certyfikatów. W związki z tym w 2028 r. przyjęto dwukrotny wzrost wpływów z kar. Należy w tym miejscu zaznaczyć, że dane dotyczące kar pieniężnych to szacunki, a nie cele. Podkreślenia wymaga, że kary będą nakładane w drodze decyzji administracyjnej w następstwie naruszenia prawa, zgodnie z przepisami ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2024 r. poz. 572).

Utworzenie zdolności do certyfikacji w ramach kolejnych europejskich programów certyfikacji

Koszty rozwoju zdolności do certyfikacji										
2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
9,4	10,8	10,8	10,8	10,8	10,8	10,8	10,8	10,8	10,8	10,8

	Aby w pełni wykorzystać szanse jakie daje europejski system certyfikacji cyberbezpieczeństwa oraz zapewnić polskim konsumentom dostęp do certyfikowanych usług w tym obszarze, konieczne będzie zapewnienie możliwości przeprowadzenia certyfikacji w podmiotach publicznych, takich jak NASK–PIB. Należy podkreślić, że NASK–PIB prowadzi już działalność certyfikacyjną w ramach metodologii Common Criteria (projekt KSO3C), jednej z najstarszych i najbardziej skomplikowanych metodologii oceny bezpieczeństwa produktów ICT. W związku z powyższym te zdolności powinny być dalej rozwijane tak, aby przedsiębiorcy chcący certyfikować swoje produkty zawsze mieli możliwość dokonania tego w Polsce. Koszty na ten cel przewidziane zostały na podstawie doświadczeń z projektu KSO3C i uwzględniają m.in. koszt roboczogodzin związanych z dostosowaniem NASK–PIB do wymagań, nowego programu, zatrudnienie niezbędnych ekspertów oraz utrzymanie sprzętu niezbędnego do prowadzenia badań. Cały projekt KSO3C kosztował w sumie ok. 24 mln złotych. W związku z tym za podstawę do dostosowania się jednostki certyfikującej i laboratoriów do nowych programów przewidziana została ok. 1/3 tej kwoty. W związku z tym w 2024 r. przewidziano na ten cel dodatkowe środki w wysokości 9,4 mln zł. związane z wejściem w życie pierwszego europejskiego programu certyfikacji EUCC. W następnych latach przewiduje się wejście w życie kolejnych programów certyfikacyjnych, co będzie wiązało się z koniecznością rozwijania zdolności certyfikacyjnej w nowych obszarach, w związku z tym przewiduje się na ten cel wydatki w wysokości 10,8 mln zł. Wydatki te będą związane każdorazowo z przygotowaniem odpowiedniego programu certyfikacji, uzyskaniem akredytacji PCA, pozyskaniem ekspertów posiadających wiedzę niezbędną do realizacji tych zadań, a także pozyskanie sprzętu potrzebnego do przeprowadzenia badań. Na razie żaden kolejny europejski program certyfikacji cyberbezpieczeństwa nie został przyjęty w związku z czym trudno jest precyzyjnie ocenić jak wiele przygotowań będzie koniecznych do jego wprowadzenia. Dlatego podstawą dla przyjętej kwoty są doświadczenia z programu KSO3C. Jeśli prace te nie zostaną wykonane spowoduje to, że certyfikacja w ramach europejskich programów nie będzie możliwa w Polsce. Oznacza to, że polscy przedsiębiorcy chcący certyfikować swoje produkty będą musieli zwracać się do jednostek certyfikujących z innych krajów. W ramach tych kosztów wzmocnione zostaną wszystkie państwowe instytuty badawcze, których kompetencje są niezbędne dla zapewnienia efektywnego działania krajowego systemu cyberbezpieczeństwa. W szczególności wzmocnione zostaną NASK–PIB oraz Instytut Łączności, które obecnie już wykonują zadania w obszarze certyfikacji cyberbezpieczeństwa. Równocześnie nie wyklucza się rozwijania tych zdolności również w innych instytutach. Nie jest wiadome, jakich jeszcze obszarów będą dotykały kolejne europejskie programy certyfikacji, w związku z czym nie można wykluczyć, że pojawi się program dotykający obszaru, w których specjalizuje się inny instytut. W takim wypadku zasadnym będzie rozwijanie tego instytutu, a nie budowanie zdolności od początku w jednym z już wymienionych podmiotów. W szczególności środki te posłużą do wzmocnienia kadr w instytutach badawczych tak, aby stale dysponowały one ekspertami potrzebnymi do prowadzenia certyfikacji w tym obszarze. Należy zauważyć, że dotyczy to jednego z najbardziej konkurencyjnych obszarów gospodarki pod kątem płac. Zarobki konsultanta ds. cyberbezpieczeństwa mieszczą się w przedziale od 18 do 26 tys. zł.[3)], a w przypadku certyfikacji konieczne jest pozyskanie osób mających szczególnie duże kompetencje i wiedzę. Do przeprowadzenia procesu certyfikacji potrzebni są specjaliści, którzy dysponują znaczną wiedzą techniczną, ale również wiedzą w zakresie metodologii badań oraz procesów certyfikacyjnych. Ich kompetencje są unikalne, w związku z czym pozyskanie i utrzymanie takich osób musi wiązać się z zapewnieniem im zarobków podobnych do rynkowych. W przeciwnym wypadku nie zostaną zrealizowane cele ustawy. Budowa tych zdolności jest niezbędna dla realizacji celu ustawy, jakim jest stworzenie w pełni działającego systemu certyfikacji cyberbezpieczeństwa w Polsce. Znacząco utrudni to dostęp do certyfikowanych produktów i jednostek certyfikujących dla polskich przedsiębiorców. Ponadto środki te posłużą również na przygotowanie krajowych programów certyfikacji cyberbezpieczeństwa.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

	Skutki						
Czas w latach od wejścia w życie zmian	0	1	2	3	5	10	*Łącznie (0-10)*

[3)] https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-pensje-w-branzy-cyberbezpieczenstwa-ile-zarabiaja-specjalisci

W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							
	(dodaj/usuń)							

W ujęciu niepieniężnym	duże przedsiębiorstwa	Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Certyfikaty będą ważne na obszarze całej Unii Europejskiej, w związku z czym ich posiadanie ułatwi wejście na rynki innych państw europejskich. Ponadto certyfikaty będą brane pod uwagę przy zamówieniach publicznych zarówno dla poszczególnych państw członkowskich, jak i realizowanych przez samą Komisję Europejską. Przedsiębiorstwa posiadające certyfikaty uzyskają dodatkowo przewagę nad konkurencją. Obecnie coraz większa waga przykładana jest do cyberbezpieczeństwa produktów i usług. Szacuje się, że cyberataki kosztowały świat 8 bilionów USD w 2023 r.[4]. W związku z tym coraz więcej firm będzie szukało dla siebie rozwiązań sprawdzonych, które zagwarantują bezpieczeństwo ich danych.
	sektor mikro-, małych i średnich przedsiębiorstw	Przedsiębiorstwa z branży certyfikacyjnej uzyskają lepszy dostęp do rynku w innych krajach. Mogą również skorzystać z większego zapotrzebowania na certyfikowane, bezpieczne produkty. Inne przedsiębiorstwa otrzymają lepszy dostęp do certyfikowanych produktów. Certyfikaty będą ważne na obszarze całej Unii Europejskiej, w związku z czym ich posiadanie ułatwi wejście na rynki innych państw europejskich. Ponadto certyfikaty będą brane pod uwagę przy zamówieniach publicznych zarówno dla poszczególnych państw członkowskich jak i realizowanych przez samą Komisję Europejską. Przedsiębiorstwa posiadające certyfikaty uzyskają dodatkowo przewagę nad konkurencją. Obecnie coraz większa waga przykładana jest do cyberbezpieczeństwa produktów i usług. Szacuje się, że cyberataki kosztowały świat 8 bilionów USD w 2023 r.[5]. W związku z tym coraz więcej firm będzie szukało dla siebie rozwiązań sprawdzonych, które zagwarantują bezpieczeństwo ich danych.
	rodzina, obywatele oraz gospodarstwa domowe	Wprowadzone przepisy zapewnią większą dostępność rozwiązań technicznych zapewniających bezpieczeństwo indywidualnym użytkownikom. Widoczne certyfikaty cyberbezpieczeństwa będą również stanowić istotną pomoc dla konsumentów przy wyborze bezpiecznych produktów i usług.
	(dodaj/usuń)	
Niemierzalne	(dodaj/usuń)	
	(dodaj/usuń)	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Ze względu na przyjęcie dobrowolnego modelu certyfikacji procedowane przepisy nie spowodują zakłóceń konkurencyjności. Czas i koszt przeprowadzenia procesu certyfikacji zależą od przyjętego poziomu ewaluacji i dla: – 2 poziomu ewaluacji trwa 4–6 miesięcy i kosztuje ok. 200 tys. zł., – 3 poziomu ewaluacji trwa 6–9 miesięcy i kosztuje ok. 600 tys. zł., – 4 poziomu ewaluacji trwa 7–12 miesięcy i kosztuje ok. 900 tys. zł..

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy

[4] https://www.expressvpn.com/pl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

[5] https://www.expressvpn.com/pl/blog/the-true-cost-of-cyber-attacks-in-2024-and-beyond/

☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☐ nie dotyczy

Komentarz: Dobrowolny charakter certyfikacji sprawia, że nie dojdzie do zmiany obciążeń regulacyjnych spoczywających na przedsiębiorcach. Uczestnicy krajowego systemu certyfikacji cyberbezpieczeństwa będą musieli stosować przepisy niniejszej ustawy związane z kontrolą zarówno ze strony PCA, jak i ministra. PCA będzie przygotowywać programy akredytacji dla podmiotów zainteresowanych prowadzeniem oceny zgodności w ramach europejskich programów certyfikacji cyberbezpieczeństwa, a następnie będzie prowadzić proces akredytacji i nadzór nad akredytowanymi podmiotami. Uzyskanie akredytacji będzie miało charakter odpłatny i będzie odbywać się na warunkach rynkowych.
Minister będzie prowadził szereg postępowań administracyjnych, m.in. zezwalał na prowadzenie oceny zgodności w określonych przypadkach, zatwierdzał certyfikaty odwołujące się do poziomu uzasadnienia zaufania „wysoki" oraz nakładał kary administracyjne. Ponadto będzie również prowadził postępowania kontrolne wobec podmiotów krajowego systemu certyfikacji cyberbezpieczeństwa.

9. Wpływ na rynek pracy

Sektor cyberbezpieczeństwa jest jednym z najbardziej dynamicznych sektorów gospodarki. Cyberprzestępstwa wskazywane są jako jedne z pięciu najistotniejszych zagrożeń dla firm obok m.in. katastrof naturalnych. Na tak szybko zmieniającym się rynku rola certyfikatów stanowiących dowód na odpowiedni poziom cyberbezpieczeństwa produktów będzie rosła. W związku z tym powstaną nowe miejsca pracy m.in. w jednostkach certyfikujących czy laboratoriach badających te produkty i usługi.
Jeśli osiągnięte zostaną cele projektowanej ustawy w zakresie rozwoju rynku prawdopodobne jest również powstanie nowych etatów w tym sektorze gospodarki.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☒ sądy powszechne, administracyjne lub wojskowe	☐ demografia ☐ mienie państwowe ☐ inne:	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Rozwiązania przyjęte w projektowanej ustawie powinny zapewnić impuls do rozwoju technologii w zakresie cyberbezpieczeństwa. Przyjęcie schematów certyfikacyjnych powinno przyczynić się do dalszego ujednolicenia standardów cyberbezpieczeństwa zarówno w sektorze prywatnym, jak i publicznym. Wejście w życie ustawy i zwiększenie poziomu cyberbezpieczeństwa w sektorze przedsiębiorstw może przyczynić się do zmniejszenia strat wynikających z działań cyberprzestępców. Ponadto wprowadzenie systemu certyfikacji cyberbezpieczeństwa może przyczynić się do zwiększenia dostępności tego typu usług dla sektora małych i średnich przedsiębiorstw. Przyjęte przepisy mogą stanowić również ważny bodziec do rozwoju technologii związanych z bezpieczeństwem w cyberprzestrzeni. Uznawalność certyfikatów na obszarze całej Unii Europejskiej będzie stanowiło zachętę do rozwoju rynku usług certyfikacyjnych w kraju. Certyfikaty będą również przydatne dla administracji publicznej przy dokonywaniu zakupów. Będą one mogły zostać wykorzystane w ramach oceny ofert pod kątem bezpieczeństwa w ramach zamówień publicznych.

11. Planowane wykonanie przepisów aktu prawnego

Pierwszym krokiem jest stworzenie jednolitych procedur akredytacji i certyfikacji na potrzeby cyberbezpieczeństwa. Równocześnie utworzony zostanie organ nadzoru, który będzie monitorował rozwój rynku certyfikacji. Odpowiednie działania zostaną podjęte w Ministerstwie Cyfryzacji. Zatrudnione zostaną dodatkowe osoby, które będą prowadziły postępowania administracyjne oraz przeprowadzały kontrole, zgodnie z przepisami projektowanej ustawy. Działania te zostaną rozpoczęte w 2025 r.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zastosowane zostaną następujące mierniki:
1) liczba akredytowanych jednostek oceniających zgodność;

2) liczba wydanych certyfikatów i wystawionych deklaracji zgodności.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
Nie dotyczy