POLSKIE TOWARZYSTWO INFORMATYCZNE
Zarząd Główny, ul. Solec 38 lok. 103, 00-394 Warszawa, tel.: + 48 22 838 47 05, tel./fax: + 48 22 636 89 87, e-mail: pti@pti.org.pl, www.pti.org.pl

Polskie Towarzystwo Informatyczne
ul. Solec 38 lok. 103 00-394 Warszawa
Kontakt: Beata Ostrowska
e-mail: beata.ostrowska@pti.org.pl
Uwagi opracował zespół w składzie:
Elżbieta Andrukiewicz
Tomasz Cedro
Krzysztof Kuźniak
Mirosław St. Zmyślony

FORMULARZ ZGŁASZANIA UWAG

dotyczący projektu Ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa (UC42)

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
1.	1	Art. 2. p. 2. oraz uzasadnienie do opiniowanego projektu ustawy	Powołany zapis oznacza, iż dla potrzeb stosowania przepisów ustawy obowiązuje polskojęzyczna definicja „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych,	Uzupełnić uzasadnienie do projektu ustawy o ocenę skutków obowiązywania różnych definicji stosowanych pojęć i terminów, w tym pojęcia – terminu „cyberbezpieczeństwo".	W Polsce obowiązują dziś również inne definicje cyberbezpieczeństwa np.: (1) Cyberbezpieczeństwo - odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i niezaprzeczalność przetwarzanych danych lub związanych z

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			użytkowników takich systemów oraz innych osób przed cyberzagrożeniami", zawarta w obowiązującej polskojęzycznej wersji rozporządzenia (UE) 2019/881 oraz definicja „cyberzagrożenie" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób" zawarta tamże Art. 2. p. 8.		nimi usług oferowanych przez te systemy" – Art. 2. p. 4. Ustawy z dnia 5 lipca 2018 r o krajowym systemie bezpieczeństwa Dz. U. 2018 poz. 1560 ze zm. Oznacza to potrzebę ujednolicenia terminologii i definicji po wejściu w życie ustawy.
2.	1	Art. 2 pkt 4) „dokument odzwierciedlający stan wiedzy" i art. 9 ust. 2 pkt 9) oraz art. 12 ust. 2	Definicja nie pochodzi z Rozporządzenia 2019/881 a Rozporządzenia wdrożeniowego Komisji 2024/482 odnoszącego się WYŁĄCZNIE do schematu (programu) EUCC. W tym schemacie wskazano możliwość odstępstwa od zastosowania dokumentu 'state-of-the art' wraz z opisem szczegółowym okoliczności oraz trybu postępowania Jednakże wprowadzenie tego	Prosimy o przywrócenie kontekstu pochodzenia tego pojęcia oraz uwzględnienie ograniczeń wskazanych w rozporządzeniu 2024/482.	Tryb postępowania z wyjątkami stosowania konkretnych dokumentów 'state-of-the-art' w odniesieniu do EUCC jest opisany w art. 15 ust. 2 Rozporządzenia Komisji 2024/482 i tam m.in. wskazuje się konieczność uzyskania opinii ECCG i zastosowania jej w najwyższym możliwym stopniu. Zapis art. 9 ust.2 pkt 9) nie ma jakichkolwiek ograniczeń swobody krajowego organu w określeniu odstąpienia od wymagań określonych w dokumencie 'state-of-the-art.', stąd daje krajowemu organowi

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			mechanizmu do ustawy w ogólności, bez kontekstu EUCC nie jest właściwe.		zbyt duże uprawnienia, które nie były przewidziane w Rozporządzeniu 2019/881.
3.	2	Art. 3 ust. 1 (cel)	„(..)ma na celu wspieranie wytwarzania wysokiej jakości produktów ICT, usług ICT i procesów ICT przez wprowadzenie procedur w zakresie certyfikacji (..)" Samo wprowadzenie procedur nie jest wystarczającym uzasadnieniem celu certyfikacji. Same procedury nie przyczynią się do poprawy jakości wytwarzania czegokolwiek.	Sugeruje się wykorzystanie tekstu wskazanego w uzasadnieniu projektu Ustawy oraz np. motywu (75) rozporządzenia 2019/881: *„Celem europejskich programów certyfikacji cyberbezpieczeństwa powinno być zapewnienie, by produkty ICT, usługi ICT i 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, usług i procesów w trakcie ich całego cyklu życia"* Redakcję przepisu pozostawiamy Autorom projektu	Cel polskiego krajowego systemu certyfikacji cyberbezpieczeństwa nie musi być tożsamy z celem europejskich programów cyberbezpieczeństwa. Powinien jedynie sprzyjać temu celowi i zapewniać optymalne warunki do tworzenia/współtworzenia dobrych krajowych i europejskich programów certyfikacji cyberbezpieczeństwa.
4.	2	Art. 3 ust. 2 lit c)	„(..)prowadzące ocenę produktów ICT, usług ICT lub procesów ICT w zakresie cyberbezpieczeństwa"	Uzupełnić: prowadzące ocenę lub certyfikację (..)	Zgodność z praktyką jednostek oceniających zgodność funkcjonujących na rynku

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			definicja niepełna. CAB[1]-y mogą realizować wyłącznie usługi certyfikacyjne, które są inną działalnością niż „ocena" (ewaluacja) albo realizować, i ewaluację, i certyfikację		
5.	3	Art. 4 ust. 2	Zapis: „2. Produkt ICT, usługa ICT lub proces ICT w ramach oceny zgodności, o której mowa w ust. 1, podlega ocenie zgodności z wymogami bezpieczeństwa, które odpowiadają jednemu z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881." jest mylący. Poziomy uzasadnienia zaufania obejmują i wymagania bezpieczeństwa, i rygor, zakres oraz wnikliwość oceny. Aktualny zapis wskazuje jedynie odpowiedniość poziomu uzasadnienia zaufania do wymogów bezpieczeństwa.	Sugeruje się modyfikację zapisu: „2. Ocena zgodności z wymaganiami bezpieczeństwa produktu ICT, usługi ICT lub procesu ICT ~~w ramach oceny zgodności,~~ o której mowa w ust. 1, ~~podlega ocenie zgodności z wymogami bezpieczeństwa, które odpowiadają~~ odnosi się do jednego z poziomów uzasadnienia zaufania wskazanych w art. 52 rozporządzenia 2019/881	Zgodność z definicją poziomów uzasadnienia zaufania zawartej w Rozporządzeniu 2019/881
6.	3	Art. 6 pkt 1)	W przepisie nie ma związania z odpowiednimi normami referencyjnymi – zob. np. art. 54(1) lit c) rozporządzenia 2019/881,	„wymogi dla produktów ICT, usług ICT lub procesów ICT podlegających ocenie	Odniesienie do norm referencyjnych jest podstawą wiarygodności ocen zgodności - ich porównywalności i powtarzalności

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
				zgodności z odniesieniem do norm, zgodnie z art. 54(1) lit c rozporządzenia 2019/881;	
7.	3	Art. 6 pkt 2)	„szczegółowe metody stosowane w celu wykazania, że produkt ICT, usługa ICT lub proces ICT są zgodne z wymogami, o których mowa w pkt 1" - szczegółowość metody nie jest jej cechą charakterystyczną – kluczowe jest wskazanie metod znormalizowanych	~~szczegółowe~~ znormalizowane metody (..)	Odniesienie do norm referencyjnych jest podstawą wiarygodności ocen zgodności - ich porównywalności i powtarzalności
8.	3	Art. 6 pkt 5)	„5) dokumentację techniczną i sposób jej przechowywania," Zapis jest zbyt ogólny.	Połączyć zapis pkt 7 z pkt 5: 5) dokumentację techniczną oraz inne istotne informacje związane z oceną zgodności, ~~i sposób ich przechowywania,~~ z uwzględnieniem warunków przetwarzania informacji z uwagi na zdefiniowaną wrażliwość informacji oraz okresu jej przechowywania i archiwizowania, a na końcu niszczenia	Doprecyzowanie zapisu, co zostało uwzględnione chociażby w art. 43 rozporządzenia wdrożeniowego 2024/482 dot. EUCC
9.	4	Art. 7	Art. 7. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację w obszarze objętym jednym z europejskich albo krajowych programów certyfikacji	Art. 7. Oceny zgodności dokonuje jednostka oceniająca zgodność posiadająca akredytację o zakresie odnoszącym się do danego ~~w obszarze objętym jednym z~~ europejskiego albo krajowego programu certyfikacji	Powiązanie zakresu działalności CAB z zakresem akredytacji, jaki jednostka oceniająca zgodność faktycznie posiada

Lp.	Str.	Jednostka redak-cyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			cyberbezpieczeństwa". Zapis zbyt szeroki – mógłby prowadzić do błędnej interpretacji, że jak – przykładowo – CAB ma akredytacje na badania i testy zgodnie z Common Criteria, to mógłby również świadczyć usługi w programie dot. certyfikacji cyberbezpieczeństwa rozwiązań w chmurze.	cyberbezpieczeństwa	
10.	5	Art. 8 ust. 2	„2. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854)." Dokumenty odzwierciedlające stan wiedzy mogą mieć zastosowanie do akredytacji – tak jest w przypadku EUCC (zob. rozporządzenie wdrożeniowe 2024/482	„2. Do akredytacji stosuje się przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2022 r. poz. 1854), z uwzględnieniem wskazanych dokumentów odzwierciedlających stan techniki, jeśli mają zastosowanie"	Specyfika cyberbezpieczeństwa wymaga uszczegółowienia lub rozszerzenia wymagań ogólnych dot. akredytacji CAB, zawartych w normach zharmonizowanych, jak to uczyniono już w wypadku EUCC.
11.	5	Art. 10 ust 1 pkt 3)	„3.przeprowadzania badań produktów ICT;" zakres tego przepisu jest zbyt wąski. Dlaczego tylko produktów ICT? I dlaczego tylko badań?	przeprowadzania badań **lub testów** produktów ICT, usług ICT lub procesów ICT"	Pokrycie możliwych potrzeb ministra właściwego do spraw informatyzacji w pełnym zakresie przedmiotu Ustawy

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
12.	5	Art. 10 ust. 1 pkt 4)	„4.publikację specyfikacji technicznych, norm i standardów" Instytutu badawcze nie są uprawnione do publikowania norm – to wyłączne prawo krajowej jednostki normalizacyjnej w tym zakresie wynika z ustawy o normalizacji; dodatkowo, nie wiadomo, co w kontekście Ustawy oznacza termin „standard"	Sugeruje się wykreślić przepis z projektu Ustawy	Zakres stosowalności norm lub specyfikacji technicznych oraz sposobu ich używania określa rozporządzenie UE o normalizacji 2012/1025 i ono jest wystarczające; Ew. odniesienie do norm lub innych specyfikacji technicznych jest w zakresie uprawnienia ministra właściwego do spraw informatyzacji i już jest zawarte w przepisach art. 6 projektu Ustawy
13.	6	Art. 10 ust. 1 pkt 6)	„6. opracowanie i walidację procedur badawczych" – nie wiadomo, co Autor miał na myśli. Do „walidacji procedur" można odnieść działania wskazane w normie ISO 9001 (np. walidacja procesu) i definicję tam stosowaną. Z kolei, norma PN-EN 17025, która jest normą służącą do akredytacji laboratoriów badawczych i wzorcujących stosuje pojęcie „walidacji" w odniesieniu do metod badawczych (mówi się też o procedurze walidacji); jeśli Autor miał na myśli to drugie znaczenie, to mieści się ona w zapisie punktu 7)	Sugeruje się skreślenie pkt 6)	Unikanie pojęć niezdefiniowanych „walidacja procedury badawczej", co może wprowadzić w błąd osoby wdrażające lub stosujące przepisy Ustawy

Lp.	Str.	Jednostka redak-cyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
14.	6	Art. 10 ust 4 pkt 1)	„1) utrzymanie stałej sprawności operacyjnej w zakresie opracowywania i walidacji procedur badawczych, metod i technik oceny oraz wytwarzania materiałów odniesienia;" – zapis kompletnie niezrozumiały oraz zbyt wąski. Niezrozumiałe jest, w jaki sposób państwowy instytut badawczy miałby tworzyć „materiał odniesienia"? Może Autor miał na myśli ew. organizację porównań międzylaboratoryjnych lub badaniach biegłości oraz – w wypadku jednostek certyfikujących – wzajemne oceny (peer assessment) (zob. PN-EN ISO/IEC 17025 oraz Art.54(1) lit u) rozporządzenia 2019/881, odpowiednio.	Z uwagi na niepewność co do intencji Autora projektu, sugeruje się uogólnienie zapisu w następujący sposób: „utrzymanie stałej sprawności operacyjnej w zakresie realizacji zadań wskazanych w ust. 3" Można rozważyć dodanie w ust. 3 nowego punktu: x) organizację porównań międzylaboratoryjnych lub badań biegłości lub wzajemnej oceny, w europejskim albo krajowym programie certyfikacji cyberbezpieczeństwa"	Zapewnienie zgodności między ust. 3 a 4, co do „operacyjnej gotowości"
15.	6	Art. 10 ust. 5	Błąd gramatyczny. W ust. 1 i 3 jest mowa o „państwowe instytuty badawcze" (liczba mnoga) a w ust. 5 jest mowa o „podmiocie" (liczba pojedyncza)	Poprawić na liczbę mnogą („inne niż podmioty wskazane")	Poprawka gramatyczna

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
16.	7	Art. 11	Brakuje przepisu określającego relację „zezwolenia" do „akredytacji". Akredytacja jest warunkiem koniecznym posiadania zezwolenia Brakuje okresu ważności zezwolenia lub warunków, w których status zezwolenia zmienia się (zależność od akredytacji)	Dodać nowe ustępy: „x) warunkiem koniecznym wydania lub wznowienia zezwolenia jest przedstawienie przez jednostkę oceniającą zgodność ważnego certyfikatu akredytacji o zakresie pokrywającym zakres europejskiego albo krajowego programu certyfikacji cyberbezpieczeństwa" y) zezwolenie jest ograniczane, zawieszane lub cofane w wypadku analogicznych zmian w certyfikacie akredytacji lub na wniosek danej jednostki oceniającej zgodność"	Uzyskanie zgodności z przepisami określonymi w rozporządzeniu 2019/881.
17.	8	Art. 12 ust. 2	Jak wskazano w rozporządzeniu wdrożeniowym Komisji 2024/482 (art. 15 ust. 2), uchylenie wymagań jest poparte uzyskaniem opinii ECCG oraz jej uwzględnieniem w jak największym stopniu	„2. Minister właściwy do spraw informatyzacji zezwala, w drodze decyzji, na zrezygnowanie z zastosowania odpowiedniego dokumentu odzwierciedlającego stan wiedzy w przypadku, gdy takie odstępstwo jest uzasadnione charakterem danego produktu ICT, usługi ICT lub procesu ICT oraz było poprzedzone zasięgnięciem opinii Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa i jej uwzględnieniem w jak największym stopniu"	Zachowanie zasady oceny w odniesieniu do takich samych lub co najmniej równoważnych wymagań, co pozwala korzystać z przywileju automatycznego uznawania certyfikatu wydanego w danym Kraju Członkowskim we wszystkich pozostałych Krajach UE oraz EOG. Odstępstwo może skutkować brakiem możliwości uznania certyfikatu jako zgodnego z danym europejskim programem certyfikacji cyberbezpieczeństwa.

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
18.	8	Art. 14	Art. 14 określa model certyfikacji w wypadku zastosowania poziomu uzasadnienia zaufania „wysoki" w którym KAŻDY certyfikat jest zatwierdzany przez krajowy organ ds. certyfikacji cyberbezpieczeństwa. Rozporządzenie 2019/881 w art. 56 ust. 6 przewiduje drugi model w postaci stałej delegacji „na podstawie ogólnego powierzenia przez krajowy organ ds. certyfikacji cyberbezpieczeństwa zadania polegającego na wydawaniu takich europejskich certyfikatów cyberbezpieczeństwa jednostce oceniającej zgodność."	Szczegółowe zapisy są w tej chwili niemożliwe do zaproponowania, ponieważ sugerujemy najpierw zastanowić się nad modelem, w którym krajowy organ przekazuje stałe powierzenie zarządzania certyfikatami wskazanej - akredytowanej i posiadającej zezwolenie do wydawania certyfikatów ocenianych na poziomie uzasadnienia zaufania „wysoki - jednostce certyfikującej.	Model stałego powierzenia jest wariantem bardziej korzystnym w wypadku krajowych organów, które się dopiero tworzą - przypadek Polski. Należy wskazać, że zarządzanie certyfikatami to nie tylko wydawanie i cofanie certyfikatu, ale też zawieszanie, odnawianie, zmiana zakresu certyfikatu. Jeśli jeszcze założyć, że programów europejskich będzie więcej niż jeden, jak dziś (EUCC), to obciążenie administracyjne krajowego organu związane jedynie z zarządzaniem certyfikatami będzie przekraczało założoną wielkość komórki organizacyjnej w MC dedykowanej do roli krajowego organu.
19.	9	Art. 16 ust. 1 pkt 2)	Skarga – na jednostkę oceniającą zgodność; Uprawnienie to jest przypisane każdemu, bez jakiegokolwiek uwarunkowania. Może to doprowadzić do działań wrogich, skierowanych na zakłócenie działalności CAB-a, np. przez konkurencyjny podmiot	„2.na jednostkę oceniającą zgodność, w wypadku uzasadnienia interesu skarżącego"	Zapewnienie bezpieczeństwa prawnego jednostkom oceniającym zgodność

Lp.	Str.	Jednostka redak-cyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
20.		Uwaga ogólna	Wydaje się celowe uzupełnienie opiniowanego projektu o przepis nakazujący przeprowadzanie okresowych przeglądów oraz dokonywanie okresowych kompleksowych ocen funkcjonowania krajowego systemu certyfikacji cyberbezpieczeństwa przez ministra właściwego do spraw informatyzacji (na wzór przepisów Art 67 rozporządzenia 2019/881) i przedkładania wyników Radzie Ministrów RP		Krajowy System Certyfikacji Cyberbezpieczeństwa jest nowym rozwiązaniem systemowym w polskim systemie prawnym i powinien podlegać „tuning'owi"
21.		Uwaga ogólna	W projekcie ustanowiono mechanizm planowania generowania przychodów z kar - kto, dlaczego i na jakich zasadach może być ukarany - czy karane mają być nieupoważnione/nieakredytowane jednostki oceniające zgodność, jednostki oceniające zgodność wydające certyfikaty klientom niespełniającym wymagań lub jeśli same nie spełniają wymagań, klienci łamiący wymagania stawiane przez krajowy/europejski program certyfikacji cyberbezpieczeństwa po	Sugeruje się znaczące zmniejszenie wysokości kar.	Uniknięcie efektu odstraszania i promocja certyfikacji (pozytywne bodźce), która jest jednym z oczywistych celów Ustawy.

Lp.	Str.	Jednostka redakcyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			otrzymaniu certyfikatu i w czasie obowiązywania. Krajowy system certyfikacji cyberbezpieczeństwa jest w Polsce konstrukcją nową i rozbudowany system kar będzie po prostu odstraszający. Wydaje się, że lepiej jest pomagać i dawać dobry przykład niż karać.		
22.	1	OSR, pkt. 1	„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." Teza ta jest nietrafna. Samo wprowadzenie krajowych programów certyfikacji cyberbezpieczeństwa nie może być aktem woli krajowego organu, ponieważ rozporządzenie 2019/881 zakazuje tworzenia krajowych programów, jeśli zakres przedmiotowy pokrywa eu-	Sugeruje się skreślenie wskazanego akapitu z OSR.	Przepisy Art.57 ust. 2 rozporządzenia 2019/881 stanowią cyt. „Państwa członkowskie nie mogą wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT i procesów ICT, które są już objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa.". Co więcej, tamże (ust. 4) stanowi: „Z myślą o unikaniu rozdrobnienia rynku wewnętrznego, państwa członkowskie informują Komisję i ECCG o wszelkich zamiarach dotyczących opracowania nowych krajowych programów certyfikacji cyberbezpieczeństwa.". Wskazany akapit (przedostatni) p. 1-go OSR – co najmniej niejednoznaczny - może wprowadzać w błąd

Lp.	Str.	Jednostka redak-cyjna/wiersz	Treść uwagi	Propozycja zapisu	Uzasadnienie
			ropejski program certyfikacji cyberbezpieczeństwa. Stąd Minister ma tu bardzo ograniczone pole do działania		Ustawodawcę w trakcie procedowania opiniowanego projektu ustawy w Parlamencie

[1] Skrót od Conformity Assessment Body – jednostka oceny zgodności

17.06.2024 r.

PREZES
Polskiego Towarzystwa Informatycznego
Wiesław Paluszyński