Warszawa, dnia 18 marca 2026 roku

Pan Minister
Dariusz Standerski
Sekretarz Stanu
Ministerstwo Cyfryzacji

dot. pisma znak: DP.MC.WLA.0211.35.2025

Szanowny Panie Ministrze,

W imieniu Polskiej Izby Informatyki i Telekomunikacji (PIIT), Polskiego Towarzystwa Informatycznego (PTI) oraz Związku Cyfrowa Polska (ZCP) dziękujemy za możliwość udziału w konsultacjach projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw. Kierunek zmian należy ocenić jako istotny z punktu widzenia dalszego rozwoju polskiej informatyzacji, wdrożenia europejskiego portfela tożsamości cyfrowej oraz budowy nowoczesnego ekosystemu usług zaufania w Polsce.

Odnosząc się do ewentualnych wątpliwości w zakresie potrzeby dokonania zmian w przepisach sektorowych, które w sposób szczególny dopuszczałyby stosowanie europejskiego portfela tożsamości cyfrowej, przyjęto założenie, że nie ma potrzeby wprowadzania takich przepisów. Należy bowiem wskazać, że każdy europejski portfel tożsamości cyfrowej (w tym także ten, który będzie wydawany w Polsce), musi być zgodnie z art. 5f rozporządzenia eIDAS akceptowany w każdej usłudze online, świadczonej przez podmiot sektora publicznego i w części usług niektórych podmiotów prywatnych.

Pragniemy zauważyć, iż na gruncie rozporządzenia PE i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (dalej „rozporządzenia eIDAS 2.0") poleganie przez strony ufające na EPTC jest co do zasady dobrowolne. Zgodnie bowiem z art. 5b ust. 1 rozporządzenia eIDAS 2.0. rejestracja w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej jest wymagana wyłącznie w przypadku, gdy strona ufająca zamierza polegać na EPTC. *Per analogiam*, jeżeli dana strona ufająca nie zamierza korzystać z EPTC, nie dokonuje powyższej rejestracji.

Obowiązek akceptacji EPTC, a tym samym rejestracja w rejestrze stron ufających EPTC powstaje jednak w sytuacji, o której mowa w art. 5f ust. 2 rozporządzenia eIDAS 2.0.

Zgodnie z tym przepisem:

W przypadku gdy prywatne strony ufające, które świadczą usługi (…) zobowiązane są na podstawie prawa Unii lub prawa krajowego do stosowania silnego uwierzytelnienia użytkownika do celów identyfikacji elektronicznej lub w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego, w tym w obszarach (…) telekomunikacji, te prywatne strony ufające (…) również akceptują europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem.

W naszej ocenie obowiązek akceptacji EPTC powstaje tylko w określonych sytuacjach, tj. tylko wtedy, kiedy prywatne strony ufające – przy świadczeniu swoich usług – spełniają dwa warunki:

2) stosują silne uwierzytelnianie użytkownika (SCA) do celów identyfikacji elektronicznej,

2) do stosowania SCA do celów identyfikacji elektronicznej, zobowiązane są na podstawie prawa UE, prawa krajowego lub zobowiązania umownego.

Rozporządzenie eIDAS w art. 5f ust. 2 zawiera też przykładowy katalog branż, które mogłyby akceptować EPTC: transport, energia, bankowość, usługi finansowe, zabezpieczenie społeczne, zdrowie, woda pitna, usługi pocztowe, infrastruktura cyfrowa, edukacja lub telekomunikacja. Jak widać, jest to bardzo szeroki katalog, który dotyczy wielu branż, w których obowiązków SCA nie przewidywało dotychczas prawo unijne – nie sposób byłoby czytać tej listy jako próby wprowadzenia obowiązku stosowania SCA do bliżej nieokreślonych procesów w każdej z tych branż. O przykładowym charakterze wskazania szerokiej listy branż świadczy też treść motywu 56 rozporządzenia – w którym przed listą branż użyte jest określenie „na przykład".

Obowiązek akceptacji EPTC powstaje zatem wyłącznie w odniesieniu do tych usług, których świadczenie przez danego przedsiębiorcę oparte jest na silnym uwierzytelnianiu użytkownika (na podstawie przepisu prawa lub zobowiązania umownego) i jest ono stosowane do celów identyfikacji elektronicznej, i jednocześnie nie dotyczy on innych usług, świadczonych przez tego samego przedsiębiorcę, których świadczenie nie wymaga SCA na podstawie prawa ani zobowiązań umownych.

W przypadku przedsiębiorców telekomunikacyjnych ani prawo unijne, ani krajowe nie narzuca obowiązku stosowania SCA. Zatem jeśli przedsiębiorca sam nie zobowiązał się do stosowania SCA wobec klientów w warunkach umowy, akceptacja EPTC w usługach online, w szczególności przy potwierdzeniu tożsamości podczas zawierania umów o świadczenie usług komunikacji elektronicznej, powinna być rozpatrywana wyłącznie jako fakultatywna - podobnie jak obecnie odbywa się potwierdzanie danych abonenta drogą elektroniczną z wykorzystaniem danych potwierdzonych za pomocą certyfikatu użytkownika aplikacji mObywatel, jeżeli użytkownik wyraził zgodę na tę formę podania danych.

Wobec powyższego dostrzegamy jednak konieczność nowelizacji przepisów sektorowych w ramach niniejszego Projektu poprzez zmianę ustawy – Prawo komunikacji elektronicznej i dopuszczenie, jako kolejnej możliwości, potwierdzania danych abonentów z wykorzystaniem danych potwierdzanych za pomocą certyfikatów udostępnionych w ramach nowej aplikacji mObywatel z warstwą europejską (mObywatel Europa), czy też w ramach osobnego rozwiązania (np. osobnej aplikacji) – w zależności od finalnych rozstrzygnięć Projektodawcy.

Jednocześnie po analizie projektu oraz zestawieniu szczegółowych uwag przekazanych w załączniku, pragniemy wyrazić istotny niepokój co do kilku rozwiązań systemowych, które w naszej ocenie mogą ograniczyć skuteczność ustawy, osłabić rozwój rynku oraz utrudnić budowę interoperacyjnego, bezpiecznego i opartego na wielu niezależnych dostawcach modelu usług cyfrowych.

Najważniejsze obszary wymagające ponownego rozważenia

- **Konflikt interesów między funkcją nadzorczą a funkcją dostawcy usług.** Projekt w obecnym kształcie łączy w jednej strukturze kompetencje regulacyjne i nadzorcze z kompetencjami operacyjnymi związanymi z portfelem, rejestrem i poświadczeniami. Taka konstrukcja nie daje gwarancji rzeczywiście niezależnego nadzoru i rodzi poważne ryzyka systemowe, ustrojowe oraz praktyczne.
- **Centralizacja wydawania poświadczeń atrybutów.** Przyjęty model prowadzi do nadmiernej koncentracji kompetencji po stronie ministra właściwego do spraw informatyzacji i w praktyce może zablokować możliwość skutecznego wdrażania poświadczeń atrybutów przez inne sektory oraz podmioty odpowiedzialne za autentyczne źródła. Uderza to zarówno w tempo cyfryzacji, jak i w sektorową użyteczność nowych rozwiązań.
- **Ryzyko monopolizacji infrastruktury państwowej.** Projekt wzmacnia model jednego dominującego operatora dla kluczowych elementów ekosystemu. Doświadczenia z innych obszarów pokazują, że taki model prowadzi do powstawania wąskich gardeł, ograniczenia konkurencji wpływającej na spadek poziomu innowacji i osłabienie presji jakościowej, a także wzrostu ryzyk cybersec i spadku elastyczności wdrożeń.

- **Brak współpracy z kwalifikowanymi dostawcami usług zaufania w zakresie dostarczenia poświadczeń atrybutów.** Szybka adopcja rynku wymaga ustanowienia mechanizmów pozwalających na szeroką możliwość budowania poświadczeń atrybutów przez rynek kwalifikowanych dostawców, zarówno w obszarze realizacji poświadczeń bazujących na danych pochodzących z publicznych jaki i prywatnych źródeł. Brak tej współpracy i osadzenie całości poświadczeń na usługach świadczonych przez ministra ds. informatyzacji będzie ograniczeniem możliwości szybkiego wykorzystania potencjału portfela.
- **Brak realnych mechanizmów rozwoju rynku i interoperacyjności.** W projekcie brakuje wystarczająco silnych instrumentów wspierających dialog z rynkiem, standaryzację, interoperacyjność i rozwój modelu opartego na wielu dostawcach usług zaufania. Nadzór nie powinien ograniczać się do funkcji formalnych i sprawozdawczych, lecz powinien aktywnie wspierać rozwój bezpiecznego ekosystemu tożsamości cyfrowej.
- **Model pośrednika jako potencjalna centralna brama do portfela.** Rozwiązania dotyczące pośrednictwa i rejestru stron ufających wymagają doprecyzowania. Ustawa powinna zapewniać możliwość bezpośredniego korzystania z portfela przez strony ufające, a pośrednictwo powinno stanowić model opcjonalny, a nie faktyczny warunek wejścia do ekosystemu.
- **Potrzeba jasnych zasad odpowiedzialności i równych reguł dla rynku usług zaufania.** Współpraca z kwalifikowanymi dostawcami usług zaufania powinna wzmacniać rynek polskich przedsiębiorstw, pozwalać na wykorzystanie ich potencjału, zamiast budować rządowe usługi, których wykorzystanie ogranicza się tylko do administracji publicznej. W tym zakresie konieczne jest wdrożenie jasnych zasad, odpowiedzialności, audytowalności i przejrzystego dostępu do infrastruktury a także brak uprzywilejowanego traktowania niektórych podmiotów świadczących usługi dla sektora publicznego.
- **Projektowane rozszerzenie profilu zaufanego** o profil zaufany podmiotu publicznego oraz profil zaufany osoby reprezentującej podmiot publiczny budzi zasadnicze wątpliwości systemowe. Proponowane rozwiązanie odchodzi od założeń wskazanych rozporządzeniem eIDAS2 i Europejskimi Ramami Tożsamości Cyfrowej, ponieważ próbuje budować nowe, krajowe rozwiązania, w technologiach centralnych baz danych identyfikacyjne tam, gdzie właściwym mechanizmem powinny być elektroniczne poświadczenia atrybutów potwierdzające status podmiotu publicznego oraz wskazanie powiązania osób fizycznych z podmiotami publicznymi.
- **Projektowane zmiany w ustawie o doręczeniach elektronicznych** budzą poważne wątpliwości systemowe, ponieważ mogą prowadzić do dalszej centralizacji i monopolizacji rynku doręczeń elektronicznych przez jeden podmiot kosztem konkurencyjności, elastyczności wdrożeń i prawa wyboru po stronie podmiotów realizujących zadania publiczne. W szczególności zastrzeżenia budzi zarówno wprowadzenie definicji podmiotu niepublicznego realizującego zadania publiczne, jak i powiązanie nowego Katalogu Podmiotów Publicznych z mechanizmami obowiązkowego funkcjonowania w modelu publicznej usługi doręczeń elektronicznych. W ocenie PIIT, PTI, ZCP rozwiązania te mogą w praktyce ograniczyć możliwość korzystania przez podmioty niepubliczne z usług innych dostawców, wzmacniać zależność od jednego operatora oraz przenosić do ustawy o doręczeniach elektronicznych materię, która ze względu na swój charakter ewidencyjny i architektoniczny powinna być regulowana raczej w ustawie o informatyzacji lub innym horyzontalnym akcie dotyczącym infrastruktury państwa. Taki kierunek zmian grozi utrwaleniem modelu, w którym rozwój rynku doręczeń elektronicznych będzie podporządkowany centralnej strukturze organizacyjnej, zamiast opierać się na nadzorowanym, interoperacyjnym i opartym na wielu dostawcach ekosystemie usług zaufania.
- **Równoległe procedowanie niezależnej nowelizacji ustawy o doręczeniach** w ramach której prowadzone są również konsultacje projektu ustawy o zmianie ustawy o zmianie ustawy o doręczeniach elektronicznych oraz niektórych innych ustaw (UD236), które w dużej mierze zawierają już zmiany wprowadzane niniejszym Projektem. Podobną uwagę przedstawiono w stanowisku do konsultacji publicznych projektu UD236. Postulujemy taką organizację procesu legislacyjnego, aby te same zmiany wprowadzane były wyłącznie w ramach nowelizacji jednego aktu prawnego. Dlatego też rekomendowanym rozwiązaniem byłoby uspójnienie tych zmian poprzez wykreślenie z Projektu UC 122 zmian do ustawy o doręczeniach elektronicznych w całości i przeniesienie ich do projektu UD236 w zakresie nieobjętym zmianami

wprowadzanymi w projekcie UD236. Ewentualnie wykreślenie z Projektu UC122 tylko tych zmian do ustawy o doręczeniach elektronicznych, które dublują się ze zmianami wprowadzonymi do Projektu UD236, przy czym to alternatywne rozwiązanie zdaje się mieć istotną wadę z punktu widzenia wejścia w życie obu regulacji. Wprawdzie oba projekty przewidują wejście w życie tych konkretnych zmian po upływie 12 miesięcy od ogłoszenia, jednak z uwagi na prawdopodobne różne terminy ogłoszenia obu tych aktów prawnych w Dzienniku Ustaw, różne będą też terminy wejścia w życie tychże przepisów.

- **Projektowane zmiany w ustawie o aplikacji mObywatel** wymagają ponownego uporządkowania na poziomie systemowym, ponieważ w obecnym kształcie mieszają funkcję krajowej aplikacji publicznej z funkcją europejskiego portfela tożsamości cyfrowej, nie zapewniając dostatecznej jasności co do relacji między tożsamością osoby fizycznej, danymi podmiotu oraz podstawą prawną reprezentacji. Z przedstawionych uwag wynika, że projekt może prowadzić do niejednoznaczności co do możliwości łączenia w jednym portfelu danych osoby fizycznej i danych związanych z osobą prawną lub działalnością gospodarczą, nie rozstrzyga w sposób wystarczający podstawy i skutków prawnych takiego powiązania, a dodatkowo tworzy ryzyko nieuzasadnionego wykluczenia części użytkowników, w szczególności osób nieposiadających numeru PESEL. W naszej ocenie kierunek zmian powinien zmierzać do wyraźnego rozdzielenia warstwy identyfikacji osoby, warstwy atrybutów i warstwy umocowania do działania w imieniu innych podmiotów, tak aby rozwiązanie było zgodne z architekturą eIDAS2 (separacja domen związanych z osobą fizyczną i osobą prawną), interoperacyjne, inkluzywne i czytelne w skutkach prawnych zarówno dla obywatela, jak i dla administracji oraz rynku.

Rekomendowany kierunek zmian

W naszej ocenie ustawa powinna zostać uzupełniona przede wszystkim o rzeczywisty rozdział funkcji nadzoru i świadczenia usług, odejście od centralnego modelu wydawania poświadczeń atrybutów jako rozwiązania domyślnego, wprowadzenie mechanizmów wspierających interoperacyjność i dialog z rynkiem, a także o jasne ramy odpowiedzialności dla pośredników oraz mierzalne standardy jakości działania całego ekosystemu.

Przekazujemy szczegółowe uwagi i propozycje zmian w załączonym zestawieniu. Liczymy, że dalsze prace legislacyjne pozwolą wypracować model zgodny z celami Europejskiej Cyfrowej Tożsamości eIDAS2, zasadami państwa prawa oraz potrzebami administracji, obywateli i rynku. Deklarujemy gotowość do dalszego udziału w dialogu oraz pracach nad dopracowaniem rozwiązań ustawowych.

Z wyrazami Szacunku,

w imieniu Polskiej Izby Informatyki i Telekomunikacji
Andrzej Dulka

Digitally signed by Andrzej Dulka
Date: 2026.03.18 10:33:03 +01'00'

w imieniu Polskiego Towarzystwa Informatycznego
Wiesław Paluszyński

Signature Not Verified
Dokument podpisany przez Wiesław Paluszyński
Data: 2026.03.18 08:30:26 CET

w imieniu Związku Cyfrowa Polska
Michał Kanownik

Michał Kanownik

Tabela uwag PIIT, PTI, ZCP do Uzasadnienia i Oceny Skutków regulacji Projektu z dnia 18 lutego 2026 r. Ustawa o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122).

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
1	Uzasadnienie str. 6 Następująca treść Będzie to proces rozciągnięty w czasie, wymagający okresu przejściowego, w trakcie, którego będzie konieczne utrzymywanie obu rozwiązań (aplikacji) ze stopniowym przenoszeniem się użytkowników aplikacji mObywatel do aplikacji europejskiego portfela tożsamości cyfrowej. Należy podkreślić, że to użytkownicy sami zdecydują o tym, czy chcą korzystać z europejskiego portfela tożsamości cyfrowej, ponieważ nie będzie to narzędzie obowiązkowe. Odnotowania wymaga, że mimo udostępnienia europejskiego portfela tożsamości cyfrowej dostęp do usług publicznych i prywatnych nadal będzie musiał być możliwy z wykorzystaniem innych, istniejących środków identyfikacji i uwierzytelniania	Należy wskazać mechanizm - np. regulacja ustawowa wskazująca na możliwość wydania komunikatu np. "Minister właściwy do spraw informatyzacji, mając na uwadze uwarunkowania techniczne i organizacyjne niezbędne do … ogłasza w Dzienniku Ustaw Rzeczypospolitej Polskiej komunikat określający termin wygaszania (lub konsolidacji) aplikacji mObywatel ..." Utrzymywanie dwóch rozwiązań jest ekonomicznie, technicznie i logicznie nieuzasadnione. Brak takiego przepisu spowoduje, że nawet przy chęci realizacji konieczna będzie nowelizacja ustawy.
2	Uzasadnienie str. 11 Następująca treść Oznacza to, że sami użytkownicy portfela będą mieli możliwość zweryfikowania, czy żąda się od nich nadmiarowych danych i będą mogli poinformować o takim ewentualnym przypadku organ ochrony danych osobowych za pomocą usługi udostępnionej w każdym portfelu.	Proponujemy rozważyć upublicznienie rekordów rejestru z danymi jakie strony ufające chcą pobierać od użytkowników portfela, np. w celu kontroli przez organizacje dbające o ochronę konsumentów.
3	Uzasadnienie str. 14 Następująca treść Z uwagi na to, że nie istnieje obecnie żadna krajowa platforma umożliwiająca weryfikację tak rozległego zakresu danych, zakłada się, że co do zasady możliwość weryfikacji danych drogą elektroniczną będą realizowały podmioty publiczne, które są odpowiedzialne na poziomie krajowym za poszczególne źródła autentyczne – każdy podmiot we własnym zakresie. Nie wyznacza się pośredników, którzy mogliby, zamiast podmiotów odpowiedzialnych za źródła autentyczne, weryfikować atrybuty,	Dwie kwestie, które są ze sobą sprzeczne. Brak narzucenia terminu lub jednego punktu weryfikacji danych i/lub dostępu do autentycznego źródła może mieć znaczące negatywne konsekwencje. 1. Obywatele mogą nie otrzymywać poświadczeń atrybutów w podobnym tempie jak w innych krajach UE. 2. Brak wyznaczenia pośrednika, lub możliwości wyznaczenia pośrednika nie daje nawet opcji zbudowania takiego pośrednika i wsparcia podmiotów publicznych. Zalecamy dodanie możliwości tworzenia pośredników i wydawania atestacji w imieniu podmiotów odpowiedzialnych za źródła autentyczne. Podejście takie umożliwi szybsze i sprawniejsze tworzenie

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
		nowych rynków, procesów biznesowych i usług wykorzystujących poświadczenia atrybutów co może się znacząco przyczynić do lepszego odbioru nowego portfela.
4	Uzasadnienie str. 14 Następująca treść Wspomniane wyżej podmioty publiczne celowo nie są wymieniane wprost w projektowanych przepisach, z uwagi na to, że stale postępująca informatyzacja zadań publicznych powoduje tworzenie kolejnych publicznych źródeł autentycznych, które wcześniej nie istniały. Zakłada się, że odpowiednie podmioty publiczne udostępnią kwalifikowanym dostawcom usług zaufania zarządzane przez siebie źródła autentyczne – do weryfikacji danych na podstawie przepisów eIDAS – stąd też nie ma potrzeby dodawania takiego wymogu w przepisach sektorowych.	Uwaga jak do poprzednich zapisów dotyczących 'braku motywacji' podmiotów odpowiedzialnych za źródła autentyczne do wydawania poświadczeń atrybutów.
5	Uzasadnienie str. 15 Następująca treść W związku z powyższym, w proponowanych przepisach zakłada się, że minister właściwy do spraw informatyzacji będzie mógł wydawać elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia eIDAS, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, a w szczególności będzie mógł wydawać je do zapewnianego przez siebie europejskiego portfela	Może dla szybszego i sprawniejszego zasilenia nowego portfela poświadczeniami atrybutów, powinna powstać możliwość, aby niektóre atrybuty był wydawane przez kwalifikowane Czy? Art. 9 Rozporządzenia 2025/1569 nie przesądza jednoznacznie 'monopolu' krajów UE na wydawanie poświadczeń atrybutów do portfela, wręcz odwrotnie, zachęca, aby udział w tym procesie brały CUZy.
6	Uzasadnienie str. 21 Następująca treść Jeżeli chodzi o zapewnienie możliwości wydawania profilu zaufanego podmiotu publicznego oraz profilu zaufanego osoby fizycznej reprezentującej podmiot publiczny, to pierwsze z tych narzędzi będzie środkiem identyfikacji elektronicznej osoby prawnej, w rozumieniu rozporządzenia eIDAS, a drugie środkiem identyfikacji elektronicznej osoby fizycznej reprezentującej osobę prawną. Celem wydawania takich środków jest zapewnienie narzędzi, które następnie umożliwią osobom prawnym, jakimi są podmioty publiczne, i ich pracownikom, na zidentyfikowanie się w systemach teleinformatycznych jako takie właśnie osoby, bez potrzeby dodatkowego informowania strony ufającej o tym, że ma ona do czynienia z podmiotem publicznym lub jego przedstawicielem.	Czy na pewno słuszne jest budowanie rozwiązań bazujących na identyfikacji osoby prawnej, jeśli jak słusznie zauważono w uzasadnieniu obecnie nie funkcjonują systemy przygotowane do użycia takich rozwiązań. Rekomendujemy wykorzystanie w pierwszej kolejności poświadczeń atrybutów oraz mechanizmów wynikających z portfela biznesowego zanim powstaną nowe usługi. W dzisiejszym kształcie portfel, jego funkcjonalności i przepisy powinny być wystarczające do ochrony PESEL każdego obywatela w kontaktach ze stronami ufającymi.
7	Uzasadnienie str. 22 Następująca treść W ramach projektowanych przepisów określono sposób potwierdzania tożsamości przed rejestracją użytkownika europejskiego portfela tożsamości cyfrowej, zapewnianego przez	Przepis powinien dopuścić stosowanie metody profil mObywatel + certyfikat obecności, przetestowanej i ocenionej przez audytorów przy pilotażu podpisu kwalifikowanego nie powinien stanowić 4 metody weryfikacji, skoro jest już wykorzystywana w ekosystemie?

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
	ministra właściwego do spraw informatyzacji. Przewidziano trzy podstawowe sposoby potwierdzania tożsamości.	
8	Uzasadnienie str. 24 Następująca treść Często podnoszony w odniesieniu do usług online argument, że nie każda taka usługa online oraz nie każdy system teleinformatyczny wymaga identyfikacji osoby fizycznej przy użyciu numeru PESEL, a w wielu przypadkach cele przetwarzania mogą być realizowane z wykorzystaniem innych identyfikatorów lub mechanizmów uwierzytelniania, nie jest w tym przypadku wystarczający. Należy bowiem wskazać, że europejski portfel tożsamości cyfrowej bez możliwości przekazania przez użytkownika numeru PESEL w procesie uwierzytelniania stałby się narzędziem bezużytecznym dla większości użytkowników. Wobec znaczących nakładów finansowych, jakich wymaga zapewnienie obywatelom takiego portfela, opisana wyżej sytuacja nie tylko byłaby rażącą niegospodarnością, ale byłaby także niezgodna z ogólnymi celami rozporządzenia eIDAS (ułatwienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania). Niemożliwe byłoby również uzyskiwanie elektronicznych poświadczeń atrybutów w oparciu o źródła autentyczne, w których cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej powiązano z numerem PESEL. Użytkownik portfela będzie za każdym razem informowany komu i jakie dane przekazuje i będzie mógł zablokować wysłanie takich danych oraz w wygodny sposób powiadomić organ ochrony danych o każdym nieuzasadnionym żądaniu danych, co będzie prowadziło do samoregulującego się systemu (tj. dane nadmiarowe nie będą żądane przez strony ufające z uwagi na możliwość interwencji powiadomionego, przez użytkownika portfela, organu ochrony danych).	Argumenty podnoszone w cytowanym paragrafie wyraźnie bronią długu architektonicznego (architektura danych) jaki został zaciągany przez lata w systemach administracji publicznej. Autor proponuje jego utrzymanie poprzez wprowadzenie do PID suplementu w postaci personal_administrative_number. Proponujemy rozważyć stopniową spłatę długu poprzez wprowadzenie w publicznych systemach informatycznych albo złożonego klucza składającego się z kolekcji atrybutów jednoznacznie identyfikujących osobę fizyczną, niezawierającego numeru PESEL, albo klucza będącego jednoznacznym odwzorowaniem atrybutów tworzących klucz złożony np. skrótu z kolekcji atrybutów. Zgadzamy się z uzasadnieniem, że w zestawie atrybutów jednoznacznie identyfikujących osobę fizyczną powinniśmy unikać atrybutów, których zmiana może być częsta i realizowana swobodnie przez obywatela (np. Adres email, nr telefonu). Polemizujemy z kosztownością przebudowy systemów publicznych. Systemy te muszą być okresowo aktualizowane i modyfikowane ze względu na dług technologiczny. Rozsądnym biznesowo wydaje się zatem wpasowanie zmian dotyczących rozszerzenia jednoznacznych identyfikatorów o nowe (przy utrzymaniu nr PESEL przez pewien czas) w horyzoncie np. 5 lat (średni okres amortyzacji księgowej i technologicznej systemu IT). Mechanizm samoregulacji może nie zadziałać o ile organowi ochrony danych przedstawiana będzie przez właścicieli usług publicznych argumentacja uzasadniająca konieczność pozostawienia numeru PESEL przedstawiona w niniejszym opracowaniu.
9	Uzasadnienie Str. 26 Następująca treść Wizerunek twarzy użytkownika portfela jako element krajowego zestawu danych identyfikujących osobę, jest niezbędny z uwagi na potrzebę zwiększenia bezpieczeństwa procesu identyfikacji podczas obecności fizycznej. Chodzi o to, aby użytkownik europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji, podobnie jak obecnie użytkownik dokumentu mObywatel, mógł potwierdzić swoją tożsamość, okazując, oprócz zestawu danych określających jego tożsamość, także fotografię. Zakłada się, że potwierdzenie danych podczas obecności fizycznej wymaga okazania również fotografii tak, aby	Pomysł ciekawy, ale może doprowadzić do tworzenia procesów, które będą zawsze wymagały wizerunku. Co w sytuacji, kiedy do procesu przystąpi osoba bez zdjęcia w portfelu? Czy lokalny, polski, przepis będzie wystarczający, aby odmówić jej możliwości realizacji procesu na podstawie braku zdjęcia? Przepisy eIDAS wskazują jasno o wzajemnym uznawaniu minimalnego zestawu danych zgodnie z przyjętą praktyką. Zalecamy stosowanie zdjęcia tylko w wyjątkowych sytuacjach jako dodatkowy element zabezpieczający, a nie artefakt, który zawsze będzie elementem zestawu danych przechowywanym w portfelu.

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
	strona weryfikująca tożsamość miała pewność, że dokumentem tym posługuje się ta osoba fizyczna, której dane zawiera okazywany dokument. Dzięki temu wyeliminowane zostanie niebezpieczeństwo posługiwania się europejskim portfelem tożsamości cyfrowej, zapewnianym przez ministra właściwego do spraw informatyzacji, podczas obecności fizycznej, przez osoby trzecie działające bez zgody lub wiedzy użytkownika tego portfela.	
10	Uzasadnienie str. 31 Następująca treść Zakłada się, że dane identyfikujące osobę prawną, i co z tym idzie portfel osoby prawnej, będą wydawane wyłącznie zarejestrowanym już użytkownikom europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji. Przewiduje się możliwość samodzielnego uzyskania takiego portfela, przez osobę fizyczną uwierzytelnioną łącznie za pomocą swojego europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji oraz kwalifikowanego elektronicznego poświadczenia atrybutów, które będzie poświadczało pełnomocnictwo tej osoby do posługiwania się europejskim portfela tożsamości cyfrowej reprezentowanej osoby prawnej.	Czy ten przepis jest zgodny z projektem Rozporządzenia o portfelu osoby prawnej? Dlaczego przepisy mają ograniczyć pozyskanie portfela osoby prawnej tylko przy użyciu polskiego portfela osoby fizycznej, a ograniczyć stosowanie w tym celu innych portfeli z krajów UE? W wielu sytuacjach możliwy jest onboarding do usług przy użyciu portfela, ale również i przy użyciu środka identyfikacji na poziomie wysokim. Nie rozumiemy, dlaczego nagle narzucane są w tym kontekście tak znaczące ograniczenia.
11	Uzasadnienie str. 32 Następująca treść przepisy rozporządzenia eIDAS nie wymagają, aby rozwiązania architektoniczne oraz techniczno-organizacyjne dla europejskiego portfela tożsamości cyfrowej, wydanego osobie prawnej, były inne niż dla europejskiego portfela tożsamości cyfrowej, wydanego osobie fizycznej – są one takie same, - portfel osoby prawnej różni się tylko zestawem danych identyfikujących osobę i co za tym idzie sposobem ich uzyskania, - z uwagi na istotę narzędzia, jakim jest środek identyfikacji elektronicznej osoby prawnej, należy zabezpieczyć taki środek przed nieuprawnionym przejęciem przez osoby nieupoważnione, jednocześnie możliwość używania tego środka przez osobę upoważnioną, wykorzystującą w tym celu tę samą instancję portfela , która posłużyła mu do potwierdzenia swojej tożsamości celem uzyskania danych identyfikujących osobę prawną, którą reprezentuje, jest rozwiązaniem, które zapewni spełnienie powyższego wymagania.	Wydaje się, że w kontekście przygotowania Rozporządzenia o portfelu osoby prawnej, jest zbyt wcześnie, aby przyjmować tak daleko idące założenia. Model funkcjonowania portfela osoby prawnej dopiero powstaje i na jego podstawie będą dopiero tworzone procesy biznesowe onboarding, wykorzystania i zakresu działania takiego rozwiązania. Sugerujemy na tym etapie prac nie łączyć tych wątków, a w szczególności nie determinować funkcjonalności nowego portfela na podstawie niedookreślonych zapisów portfela biznesowego. Podejmowanie decyzji biznesowych i architektonicznych dotyczących obsługi osób prawnych w tej samej aplikacji, która służy do obsługi osób fizycznych rodzi uzasadnione obawy o ryzykowne alokowanie środków publicznych na tworzenie rozwiązań informatycznych w dynamicznie zmieniającym się otoczeniu prawnym (prawo EU). Przy artykułowanej wielokrotnie intencji Komisji Europejskiej by Europejskie Portfele Biznesowe były w pierwszej kolejności dostarczane przez podmioty biznesowe, a w przypadku braku zainteresowania rynku tą usługą, rolę dostawcy przejmowały jednostki publiczne lub instytucje unijne. Promowanie funkcjonalności portfela biznesowego w ramach tworzonego obecnie portfela rodzi uzasadnione obawy o intencjonalne naruszanie pryncypium równych zasad zapewniających konkurencyjność dostawców oraz potencjalne osłabianie polskich przedsiębiorców zamierzających w przyszłości dostarczać rozwiązania portfela biznesowego.

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
		W powyższym kontekście zgadzamy się ze stwierdzeniem: *"W tym miejscu należy ponownie podkreślić, że wspomniany powyżej projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia Europejskich Portfeli Biznesowych w przypadku uchwalenia takich przepisów może w ogóle podważyć konieczność, a za co za tym idzie i sens wydawania europejskiego portfela tożsamości cyfrowej dla osoby prawnej – dlatego też planowanie odrębnych rozwiązań technicznych jest przedwczesne."*
12	Uzasadnienie, str. 33 Następująca treść Z powyższych powodów, aby domyślnie i nieodpłatnie zapewnić wszystkim osobom fizycznym możliwość składania kwalifikowanych podpisów elektronicznych, należałoby wydawać taki podpis w ramach specjalnej usługi publicznej albo zlecić zapewnienie takiego podpisu, za stosowną rekompensatą, kwalifikowanym dostawcom usług zaufania, którzy już obecnie świadczą takie usługi,	Przy okazji wprowadzenia podpisu kwalifikowanego w Portfelu nasuwa się pytanie po co Skarb Państwa ma utrzymywać 3 równoległe rozwiązania podpisu elektronicznego w Polsce? Warto nadmienić w tym miejscu projekt Strategii Cyfryzacji Państwa (cel 2.4.2), gdzie wskazana jest „kompleksowa inwentaryzacja istniejących mechanizmów" która wg nas pozwoli na pokazanie realnej mnogości sektorowych „narzędzi podpisowych" w Polsce. Obywatel nie powinien w ogóle zastanawiać się jaki rodzaj podpisu elektronicznego wybierze, ponieważ mechanizmy podpisu powinny być zaszyte w procesach udostępnianych obywatelowi. Wraz z obligatoryjnym wprowadzeniem Europejskiego Portfela Tożsamości Cyfrowej z możliwością składania kwalifikowanego podpisu elektronicznego należy rozważyć docelowe wycofanie się Państwa z wykorzystywania innych rodzajów podpisów elektronicznych które posiadają ograniczenia formalnoprawne. Powinno to jasno wynikać co najmniej z uzasadnienia do Ustawy
13	OSR (str. 8) Następująca treść 3. Wskazanie, że używanie przez osoby fizyczne kwalifikowanych podpisów elektronicznych, jakie mają być nieodpłatnie dostępne dla posiadaczy europejskiego portfela tożsamości cyfrowej, ogranicza się tylko do celów innych niż profesjonalne. Został zdefiniowany także cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny oraz określenie ograniczeń w posługiwaniu się przez osoby fizyczne kwalifikowanym podpisem elektronicznym tylko do celów innych niż profesjonalne. Przepisy wskazują, że na wniosek kwalifikowanego dostawcy usług zaufania, po spełnieniu określonych wymagań przez tego dostawcę, minister właściwy do spraw informatyzacji wyraża zgodę, w drodze decyzji przyznającą możliwość świadczenia nieodpłatnej usługi kwalifikowanego podpisu elektronicznego dla posiadaczy europejskich portfeli tożsamości cyfrowej wydanych w Polsce, do celów innych niż profesjonalne. W związku z tym, że pojęcie „cel inny niż profesjonalny" nie zostało zdefiniowane w rozporządzeniu 910/2014, przepisy wskażą, że przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny rozumie się składanie tego podpisu w celu oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w celu	Proponujemy utrzymanie znanej już definicji z pilota :*Przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny rozumie się składanie podpisu celem oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w celu załatwienia sprawy prywatnej, niezwiązanej z zawieraniem umów konsumenckich, wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenie reprezentuje lub w jakiej funkcjonowaniu uczestniczy.*

Lp.	Artykuł, punkt, litera, akapit, teść zapisu.	Opis uwagi
	załatwienia sprawy prywatnej, niezwiązanej z wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenia reprezentuje	

Tabela zgłaszania uwag do Projektu z dnia 18 lutego 2026 r. Ustawa o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw[1)]

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
1.	Art. 1 pkt 1. 9)	Ustawa nie określa dopasowywania tożsamości, a ustanawia zasady dopasowania atrybutów tożsamości w zakresie identyfikacji osób fizycznych	Zmiana zapisu pkt 9) - Określa zasady dopasowania atrybutów tożsamości osób fizycznych w zakresie identyfikacji elektronicznej.
2.	Art. 1 pkt 1. 10)	Ustawa powinna ustalać zasady a nie skupiać się na opisywaniu architektury rozwiązań IT wspierających te zasady. Wpisanie literalne w zakresie przedmiotowym ustawy, że weryfikacja atrybutów następuje za pomocą punktu weryfikacji ogranicza możliwość zastosowania innych rozwiązań. Jednocześnie ustawa nie powinna tworzyć centralnego punktu dla źródeł autentycznych innych niż będące w posiadaniu rejestrów państwowych lub podmiotów prywatnych.	Zmiana zapisu pkt 10) - Określa zasady weryfikacji atrybutów względem źródeł autentycznych podmiotów publicznych
3.	Art. 1 pkt 1. 11)	Ustawa powinna określać zasady funkcjonowania wydawców usługi wydawania poświadczeń atrybutów w imieniu podmiotu publicznego. Ustawa nie powinna tworzyć architektury jednego rozwiązania a ustanawiać zasady, na bazie których może funkcjonować realizacja usług publicznych w tym wydawania atrybutów w imieniu podmiotów publicznych.	Zmiana zapisu pkt 11) – Określa zasady wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za autentyczne źródła
4.	Art. 1 pkt 1 12) oraz 13)	Celem rozporządzenia eIDAS jest zapewnienie funkcjonowania poświadczeń atrybutów w sposób pozwalający na ich rozpoznawanie zarówno na poziomie lokalnym, krajowym i europejskim. Ograniczenie ustawy tylko do poświadczeń atrybutów zgłaszanych i ustanowionych na poziomie katalogu usług ogłaszanych przez Komisję Europejską ma za zadanie wprowadzić poświadczenia atrybutów mające zastosowania na poziomie całej UE, ograniczenie się tylko do poświadczeń paneuropejskich stanowi pozbawienie możliwości stosowania poświadczeń atrybutów ustanawianych lokalnie, na potrzeby gmin, powiatów, grup zawodowych, które mają znacznie dla rozwoju polskiej gospodarki. Celem ustawy	Zmiana zapisu pkt 12) – ustanawia mechanizmy zapewnienia interoperacyjności dla atrybutów i schematów atrybutów na poziomie krajowym i europejskim

[1)] Niniejsza ustawa służy stosowaniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, Dz. Urz. UE L 333 z 27.12.2022, str. 80 oraz Dz. Urz. UE L 2024/1183 z 30.04.2024).

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		powinno być wspieranie procesów zapewniających rozpoznawanie poświadczeń atrybutów na poziomie lokalnym, krajowym i europejskim, w tym tworzenie krajowego katalogu poświadczeń atrybutów, wspieranie procesu interoperacyjności tych poświadczeń a także przekazywanie na poziom Komisji tych atrybutów co do których kraj członkowski jest zobowiązany do udostępnienia.	
5.	Brak w projekcie	Dotyczy art. 2 pkt. 2 obowiązującej ustawy: 2) zaufaną listę Rozporządzenie eIDAS wprowadza możliwość świadczenia wielu zaufanych list, co ma znaczenie w związku z znaczącym wzrostem informacji dotyczących zaufanych podmiotów. Z tego powodu może być konieczne prowadzenie	Dodać nowy artykuł w art. 1 zmieniającym UoUZoIE Zmiana art. 2 pkt 2 zaufane listy
6.	Brak w projekcie	Dotyczy art. 2 pkt. 2 obowiązującej ustawy: Minister cyfryzacji będzie pośredniczył i rejestrował podmioty wpisywane na listy zaufanych podmiotów utrzymywane przez komisję europejską. W szczególności uwzględnia to dostawców portfela, PID, certyfikatów stron ufających.	Dodać nowy artykuł w art. 1 zmieniającym UoUZoIE Dodanie art. 2 pkt 4 - rejestr podmiotów polskich wpisanych na listy zaufanych podmiotów utrzymywane przez komisję europejską.
7.	Brak w projekcie	Dotyczy art. 2 pkt. 2 obowiązującej ustawy: Infrastruktura zaufania będzie także dotyczyła możliwości rejestracji atrybutów oraz schematów atrybutów które mają znaczenie krajowe a mogłyby się przyczynić do wzrostu użyteczności portfela	Dodać nowy artykuł w art. 1 zmieniającym UoUZoIE Dodanie art. 2 pkt 5 - ewidencję atrybutów i schematów atrybutów ustanowionych na poziomie krajowym
8.	Brak w projekcie	Konieczna aktualizacja w związku z wymaganiem normalizacyjnym zaufanych list., aktualna ustawa pomija dane niezbędne do prawidłowego funkcjonowania systemu list zaufania (TSL). Zgodnie z normą ETSI TS 119 612 (klauzule 5.3.5.2 oraz 5.4.3.2), każda pozycja na liście zaufania musi obligatoryjnie zawierać adres poczty elektronicznej oraz adres strony internetowej dostawcy, służące do obsługi zapytań i reklamacji. Ponadto, najnowsza wersja normy (V2.4.1) przewiduje możliwość podawania numeru telefonu dostawcy w sformalizowanym formacie URI. Brak tych danych w ustawowym rejestrze, z którego zasilana jest krajowa lista TSL, spowoduje niezgodność techniczną polskiej listy z unijnymi specyfikacjami i utrudni jej automatyczne przetwarzanie przez systemy w innych państwach członkowskich.	Proponowane brzmienie Art. 3 ust. 4 (poprzez dodanie/zmianę punktów): „4. Wpisowi do rejestru podlegają następujące dane dostawcy usług zaufania: (...) x) adres poczty elektronicznej służący do kontaktu w sprawach związanych ze świadczonymi usługami zaufania; y) adres strony internetowej dostawcy; z) numer telefonu do kontaktów z użytkownikami i organem nadzoru (opcjonalnie).”

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
9.	Art. 1 pkt 2. litera a) dot. art. 4 ust. 1 pkt 3.	Zapis punktu 3 jest nieczytelny i może rodzić wątpliwości zakresu świadczonej usługi.	Zmienić teść punktu na: 3) usługi świadczonej przez kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektronicznej, wydawania certyfikatów dostępu strony ufającej portfelowi oraz wydawania certyfikatów rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających europejskiego portfela tożsamości cyfrowej (Dz. Urz. UE L z 2025 r. poz. 848), zwanym dalej „rozporządzeniem 2025/848
10.	Art. 1 punkt 2 litera b. punkt 2 dot. art. 4 ust. 4	Zapis dotyczy wpisu usług a nie pojedynczej usługi. Każda usługa może mieć osobną politykę, wobec czego przepis prawa powinien umożliwiać dołączenie do wniosku polityk (liczba mnoga) świadczenia usług. Dodatkowo adres elektroniczny zgodnie z ustawą Dz. U. 2002 Nr 144 poz. 1204 jest rozumiany jako adres email. W aktach wykonawczych do eIDAS2 stosuje się zapis ujednolicony adres URL	Zmiana treści punktu: 2) polityki świadczenia usług objętych wnioskiem, zgodnie z którą mają być świadczone usługi zaufania, oraz ujednolicone adresy URL, pod którymi umieszczone są wskazane polityki;
11.	Brak w projekcie	Wydawanie kwalifikowanych poświadczeń atrybutów jest realizowane w oparciu o kwalifikowaną pieczęć elektroniczną zgodnie z zał. V rozporządzenia eIDAS. W związku z tym zamiast generacji danych powinno być dołączenie wygenerowanego wcześniej kwalifikowanego certyfikatu. To samo powinno dotyczyć opcjonalnie innych usług, które wykorzystują kwalifikowaną pieczęć elektroniczną: doręczeń elektronicznych, walidacji podpisów elektronicznych. Jednocześnie istnieją kwalifikowane usługi zaufania, które nie są powiązane z certyfikatem – np. usługa zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do składania pieczęci elektronicznej na odległość.	Dodanie w Art. 1 punkt 2 litera b. pkt 4 otrzymuje brzmienie: dane niezbędne do wystawienia certyfikatu, o którym mowa w art. 10 ust. 1 lub kwalifikowany certyfikat dostawcy usługi zaufania.
12.	Art. 1 punkt 2 litera c dot. Art. 4 ust 6	Zapis jest niezrozumiały i może budzić wątpliwości dotyczące zakresu usługi.	Zmiana treści punktu: 3) usługi wydawania certyfikatów dostępu strony ufającej portfelowi oraz wydawania certyfikatów rejestracji strony ufającej portfelowi, świadczonej przez kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektroniczne.
13.	Brak w projekcie	Zmiana art. 5 UoUZoIE w zakresie umożliwienia prowadzenia zaufanych list. 2. Minister właściwy do spraw informatyzacji prowadzi zaufaną listę. Wynika to z faktu rozszerzenia zakresu o usługi wydawania certyfikatów dostępu oraz rejestracji przez kwalifikowanych dostawców usług zaufania.	2. Minister właściwy do spraw informatyzacji prowadzi zaufane listy zgodnie z art. 22 rozporządzenia 910/2014.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
14.	Brak w projekcie	Artykuł 5 definiuje prowadzenie dokonanie wpisu w zaufanych listach tylko kwalifikowanych usług. Aktualny zapis uniemożliwia wpisanie na zaufaną listę niekwalifikowanych usług zaufania w sytuacjach, gdy te usługi prowadzą interakcje z kwalifikowanymi usługami zaufania oraz stanowią znaczenie dla ekosystemu usług zaufania. W kontekście usług świadczonych dla portfela cyfrowej tożsamości będzie miał to znaczenie dla następujących usług: ➔ Wydawania poświadczeń atrybutów niekwalifikowanych do portfela ➔ Świadczenia usług doręczenia elektronicznego w ramach krajowego systemu doręczeń elektronicznych Katalog usług wpisywanych na zaufane listy został określony w normie technicznej ETSI TS 119 612, która definiuje katalog usług kwalifikowanych, niekwalifikowanych oraz zdefiniowanych na poziomie krajowym. W szczególności aktualny zapis w rzeczywistości jest sprzeczny z praktyką, w której umieszczono zaufanej liście Narodowy Bank Polski.	Dodanie art. 5 ust. 3 Minister może wpisać na zaufaną listę niekwalifikowaną usługę zaufania o ile jest ona świadczona przez podmiot wpisany do rejestru zgodnie z art. 6 lub kwalifikowanego dostawcę usług zaufania, oraz spełnia wymagania art. 19a rozporządzenia 910/2014 oraz świadczenie usługi ma znaczenie dla funkcjonowania portfela cyfrowej tożsamości lub innych kwalifikowanych usług zaufania.
15.	Brak w projekcie	Art. 19a eIDAS oraz rozporządzenie CIR 2025/2160 ustanowiły wymagania dla świadczenia niekwalifikowanych usług zaufania. Wpis do rejestru powinien być skorelowany z wymaganiami ww. przepisów. W szczególności ujęcie we wpisie wymagań posiadania przez dostawcę niekwalifikowanej usługi zaufania: (i) procedur rejestracji i wdrażania w odniesieniu do usługi zaufania; (ii) kontrolami proceduralnymi lub administracyjnymi niezbędnymi do świadczenia usługi zaufania: (iii) zarządzaniem usługami zaufania i ich wdrażaniem;	Wymaga zmian art. 6 odpowiedniego sformułowania prawnego i odniesienia do art. 19a rozporządzenia i wymagań aktów implementujących.
16.	Brak w projekcie	Projekt pominął rejestrację w rejestrze następującej nowej usługi zaufania: Wydawanie elektronicznego poświadczenia atrybutów wydawanego przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu. Jeżeli wpis takiej usługi wymaga osobnej procedury prawnej, to odpowiednie zapisy ustawy także należy poprawić. Konieczność ww. wynika z tego, że dostawcy usługi wydawania elektronicznego poświadczenia atrybutów przez podmiot publiczny odpowiedzialny za źródło	W art. 6 UoUZoIE dodanie punktu 3) Usługi wydawania elektronicznego poświadczenia atrybutów przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		autentyczne lub w jego imieniu stanowią część infrastruktury zaufania określonej w art. 2 ustawy UZoIE	
17.	Art. 1 pkt 4 dotyczący art. 16 UoUZoIE	Projekt pominął fakt, że zaawansowanym lub kwalifikowanym podpisem elektronicznym są opatrywane także produkty i dowody innych usług zaufania określonych znowelizowanym rozporządzeniem eIDAS, w szczególności usługi doręczeń elektronicznych, raporty walidacji, poświadczenia atrybutów, poświadczenia z usługi archiwum i rejestru cyfrowego, w związku z powyższym należy przebudować jeszcze raz brzmienie całego art. 16, tak aby odpowiadało ono stanowi faktycznemu. Jednocześnie należy wyraźnie wskazać, że cześć kwalifikowanych usług zaufania będzie się posługiwała kwalifikowanym certyfikatem.	Art. 1 ust 4: Art. 16 uzyskuje brzmienie. Zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna weryfikowane za pomocą certyfikatu dostawcy usług zaufania lub kwalifikowanego certyfikatu dostawcy usług zaufania służą do opatrywania podpisem elektronicznym lub pieczęcią elektroniczną: 1) certyfikatów kwalifikowanych, o których mowa w załączniku I lit. g, załączniku III lit. g oraz załączniku IV lit. h do rozporządzenia 910/2014; 2) informacji o statusie certyfikatów kwalifikowanych, w tym listy zawieszonych lub unieważnionych certyfikatów; 3) innych certyfikatów związanych ze świadczeniem kwalifikowanych usług zaufania; 4) dowodów i poświadczeń z innych kwalifikowanych usług zaufania; 5) certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi; 6) informacji o statusie certyfikatów, o których mowa w pkt 4.
18.	Brak w projekcie	Rozporządzenie CIR 2025/2160 nakłada szczególne wymagania związane ze świadczeniem niekwalifikowanych usług zaufania. Ze względu na realizację tych wymagań ustawa w art. 19 powinna wskazać obowiązek potwierdzenia przez niekwalifikowanych dostawców wpisanych do rejestru spełnienia wymagań ww. rozporządzenia. Wynika to z faktu braku regularnych audytów.	W art. 19 UoUZoIE dodanie ust 5. Niekwalifikowany dostawca usług zaufania potwierdza przynajmniej raz na 2 lata spełnienie wymagań rozporządzenia 2025/2160 składając raport z wewnętrznego przeglądu zgodności z normami określonymi ww. rozporządzeniem.
19.	Art. 1 pkt 6 dot. art. 21aa	Dodany art. 21aa jest sprzeczny z wymaganiami art. 5b ust. 10 rozporządzenia 910/2014, gdzie pośrednicy nie mogą przechowywać danych transakcyjnych, czyli logów. Należy wskazać, że węzeł krajowy będzie pośrednikiem dla środka identyfikacji jakim są portfele cyfrowej tożsamości – w tym zakresie niedopuszczalne jest rozporządzeniem eIDAS przechowywanie danych transakcyjnych w usłudze pośrednika. Przechowywanie takich danych może być elementem świadczenia usługi identyfikacji elektronicznej lub portfela cyfrowej tożsamości, natomiast niezgodne z prawem i ochroną danych osobowych jest tworzenie centralnych lub zbiorczych systemów przetwarzających informacje o transakcjach z wykorzystaniem środków identyfikacji elektronicznej. Mimo wskazania, że dane będą tylko dostępne dla samego użytkownika wprowadzenie artykułu stanowi znaczące naruszenie bezpieczeństwa obywatela w zakresie poufności zbierania danych na temat użycia przez niego środków	Usunąć pkt 6 wprowadzający art. 21aa w całości.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		identyfikacji elektronicznej, umożliwia linkowanie tożsamości, które są zaprzeczeniem reguł ustanawianych rozporządzeniem eIDAS.	
20.	Art. 1 pkt 9 dotyczący art. 22b ust 3 pkt 1) b)	Nie można przyjąć założenia, że identyfikacja realizowana przez osobę prawną za pomocą środka identyfikacji elektronicznej lub za pomocą pieczęci elektronicznej stanowi poświadczenie chęci złożenia lub modyfikacji wniosku o wpis do rejestru stron ufających. Pieczęć ta nie dostarcza informacji o rodzaju uprawnienia, a pieczęci są stosowane aktualnie do wielu czynności związanych z fakturowaniem. Przyjęcie takiego założenia może narazić stronę ufającą na nieznane skutki bez jednoznacznej możliwości wskazania osoby w rzeczywistości dokonującej wpisu. Wobec powyższego jako minimum należy przyjąć konieczność dodatkowej identyfikacji osoby fizycznej wykonującej faktycznej czynności. Jednocześnie wątpliwości interpretacyjne może budzić zapis wskazujący zaawansowaną pieczęć elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu, czy ta definicja obejmuje kwalifikowaną pieczęć, z tego powodu sugerujemy jednoznaczne wskazanie w przepisie, że kwalifikowana pieczęć elektroniczna także jest ujęta w tym zapisie.	W art. 22b ust. 3 pkt 1 litera b) b) w przypadku osób prawnych stosowane łączenie z identyfikacją osoby faktycznie wykonującej czynność wpisu zgodnie z wymaganiami określonymi w punkcie a): – środka identyfikacji elektronicznej osoby prawnej zapewniającego wysoki poziom bezpieczeństwa lub – kwalifikowanej lub zaawansowanej lub pieczęci elektronicznej weryfikowanej za pomocą kwalifikowanego certyfikatu;
21.	Art. 1 pkt 9 dotyczący art. 22b ust 8.	Sprawdzenie upoważnienia pośrednika jest czynnością zbędną, ponieważ certyfikat rejestracji przypisany do certyfikatu dostępu pośrednika nie mogą działać bez aktywnej roli pośrednika. Wobec czego stosowanie tego przepisu jest zbędną czynnością, za którą poniesie koszt skarb państwa. W takim wypadku wpis pośrednika powinien zapewniać poinformowanie pośrednika o wykonanym wpisie. Przepisy europejskie zakładają odwrotną możliwość złożenia wniosku za pomocą pośrednika i wtedy występuje konieczność udowodnienia, że pośrednik ma prawo występować w imieniu finalnej strony ufającej.	Zmiana treści ust. 8 8. W przypadku, gdy wniosek zawiera wskazanie pośrednika, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, wpisanego do rejestru, o którym mowa w ust. 1. Na adres do doręczeń elektronicznych wskazanego pośrednika przekazywana jest informacja o wykonanym wpisie oraz ew. zmianach statusu wpisu. 8a. W przypadku gdy wniosek jest składany za pośrednictwem kwalifikowanego dostawcy usług w sposób, o którym mowa w ust. 3 pkt 2, kwalifikowany dostawca usług zaufania zapewnia poinformowanie pośrednika o wykonanym wpisie oraz ew. zmianach statusu wpisu.
22.	Art. 1 pkt 9 dotyczący art. 22b ust 8.	Ustęp 13. Wskazuje, że certyfikaty rejestracji strony ufającej portfelowi dla podmiotów publicznych mogą być wydawane przez ministra właściwego do spraw informatyzacji. Natomiast jest to niezgodne z wcześniejszymi zapisami krajowej infrastruktury zaufania, która wskazuje, że tylko kwalifikowani dostawcy usług zaufania wpisywani są do rejestru określonego w art. 4. Stosowanie różnych zasad będzie problematyczne dla osiągnięcia interoperacyjności rozwiązania, wobec czego, jeżeli minister świadczy usługę wydawania certyfikatów to powinien	13.Certyfikaty rejestracji strony ufającej portfelowi dla podmiotów publicznych mogą być wydawane przez kwalifikowanych dostawców usług zaufania oraz przez podmiot prowadzący rejestr stron ufających.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		dokonać wpisu dostawcy takiej usługi do rejestru. W dodatku należy określić warunki stosowania i nadzoru wskazanej usługi. Jednocześnie należy wskazać, czy wskazana rejestracja stron ufających będzie realizowana ze wskazaniem pośrednika. Jednocześnie niniejszy zapis może być interpretowany w kontekście przepisów prawa administracyjnego, że certyfikaty rejestracji mogą być wydawane tylko przez ministra właściwego do spraw informatyzacji.	
23.	Art. 1 pkt 9 dotyczący art. 22b ust 14. Pkt 1)	Uwierzytelnienie do rejestru stron ufających nie może być realizowane za pomocą certyfikatu dostępu strony ufającej portfelowi. Certyfikat ten ma zastosowanie do uwierzytelniania się do portfela cyfrowej tożsamości i jest wydawany dla czynników (instancji) strony ufającej. Tych certyfikatów może być wiele i ich użycie powinno ze względów bezpieczeństwa być ograniczone tylko i wyłącznie do interakcji z portfelem. Przykładowo certyfikat wydany dostawcy usług zaufania pozwala na osadzanie w portfelu poświadczeń atrybutów lub inicjowanie funkcji podpisu elektronicznego. Stosowanie tego certyfikatu do logowania do systemów pozwalać może na ataki typu phishing do stron ufających, ponieważ użycie tego certyfikatu będzie realizowane w interakcji z portfelami.	Wykreślić w pkt. 1) części: „oraz za pomocą certyfikatu dostępu strony ufającej portfelowi”;
24.	Art. 1 pkt 9 dotyczący art. 22b ust 14. Pkt 4) lit b)	Przepis lit b) może wskazywać, że informowanie następuje jedynie w przypadku realizacji nowego wpisu, dla jasności należy wskazać, że dotyczy też zmiany wpisu.	Zmiana litery b) dokonaniu wpisu do rejestru lub zmiany wpisu w rejestrze na wniosek, o którym mowa w ust. 3 pkt 2, złożony za ich pośrednictwem
25.	Art. 1 pkt 9 dotyczący art. 22b ust 15	Należy dodać pkt. 4 wprowadzający założenia z projektu Strategii Cyfryzacji Pastwa w szczególności wskazanej w niej *Politykę tworzenia, akceptacji i weryfikacji podpisów elektronicznych* w celu unormowania po latach aspektu podpisywania i weryfikacji podpisu elektronicznego w Polsce w szczególności, że pojawi się nowe zagadnienie tj. akceptacji podpisu kwalifikowanego do celów innych niż profesjonalne. Do dogłębnego rozważenia pozostaje aspekt wykorzystania usług kwalifikowanej walidacji, która jako jedyna usługa transgraniczna pozwala wydać “werdykt prawny” w zakresie poprawności złożonych podpisów lub pieczęci. Zgodnie z założeniami projektu Strategii Cyfryzacji Państwa czytamy: *„Rozwój narzędzi do podpisywania i weryfikowania dokumentów podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym.* ***Opracowanie, we współpracy z rynkiem, krajowej polityki tworzenia, akceptacji***	Proponujemy wprowadzenie delegacji ustawowej dla ministra ds. informatyzacji do wprowadzenia rozporządzeniem polityki tworzenia, weryfikacji i akceptacji podpisów i pieczęci elektronicznych w usługach publicznych.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		i weryfikacji podpisów elektronicznych, poprzedzonej kompleksową inwentaryzacją istniejących mechanizmów”.	
26.	Art. 1 pkt 9 dotyczący art. 22d	Przepisy art. 22d wprowadzają różne tryby zgłaszania atrybutów i schematów atrybutów na poziom unijny. O ile ten zakres jest przydatny, natomiast pomija on możliwość powstawania i koordynowania budowania katalogu atrybutów oraz schematów atrybutów na poziomie krajowym, który usprawni działanie krajowych jednostek, pozwoli na funkcjonowanie poświadczeń atrybutów mających znaczenie lokalne oraz pozwoli na zbudowanie krajowych rozwiązań wykorzystujących potencjał poświadczeń atrybutów. Ograniczenie się jedynie do katalogu paneuropejskiego może skutkować niską adopcją rozwiązań na polskim rynku, ślepym podążaniem tylko drogą schematów i atrybutów ustanowionych na poziomie europejskim. Jednocześnie w projekcie ustawy nie zawarto przepisów pozwalających na prowadzenie interakcji między podmiotami w celu uzgodnienia krajowych schematów, list utrzymywanych atrybutów i sposobów ich wykorzystania. Prowadzić to będzie do marginalizacji użyteczności elektronicznych poświadczeń atrybutów stosowanych krajowo.	Wprowadzenie przepisów zapewniających utworzenie krajowego repozytorium atrybutów i schematów atrybutów o znaczeniu krajowym. Koordynacja działań realizowanych przez ministra w zakresie ww. interoperacyjności atrybutów i schematów o znaczeniu krajowym.
27.	Art. 1 pkt 9 dotyczący art. 22f	Przepis we wskazanym brzmieniu ogranicza możliwość wydawania elektronicznych poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, tylko i wyłącznie do MINISTRA ds. INFORAMATYZACJI. Stosowny przepis uniemożliwia w rzeczywistości świadczenie usług przez inne ministerstwa, gminy lub powiaty i może stanowić naruszenie niezależności ww. samorządu. Jednocześnie ograniczenie tej możliwości stanowi zagrożenie sprawności państwa, gdzie możliwość wydawania poświadczeń atrybutów w imieniu podmiotów publicznych będzie zależne tylko od ministra właściwego ds. informatyzacji i uniemożliwi sprawne wykorzystanie potencjału portfela cyfrowej tożsamości przez inne podmioty publiczne. Minister cyfryzacji powinien zapewnić rejestrowanie podmiotów wydających poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014. Jednocześnie powinien zapewnić ich nadzór i zgłaszanie na do rejestru.	Zmiana treści art. Art. 22f. Minister właściwy do spraw informatyzacji rejestruje i upoważnia podmioty do wydawania elektronicznych poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, w imieniu podmiotów odpowiedzialnych za źródła autentyczne po spełnieniu przez nich wymagań określonych załącznikiem VII rozporządzenia.
28.	Art. 1 pkt 9 dotyczący art. 22g	Jak wyżej przepis ogranicza możliwość wydawania zwykłych poświadczeń atrybutów tylko do ministra ds. informatyzacji. Ogranicza to możliwość świadczenia tych poświadczeń przez inne podmioty publiczne. W rzeczywistości przepis powinien upoważnić podmioty publiczne do wystąpienia do ministra o	Zmiana zapisu na: Art. 22g ust. 1 Minister na zasadach określonych w art. 6 i art. 7 rejestruje niekwalifikowane usługi zaufania wydawania elektronicznych poświadczeń atrybutów w rozumieniu art. 3 pkt 44 rozporządzenia 910/2014:

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		możliwość świadczenia usługi wydawania zwykłych poświadczeń atrybutów na zasadach niekwalifikowanych usług zaufania. Jednocześnie należy wskazać, że certyfikat pozwalający na wydawanie ww. poświadczeń atrybutów powinien znaleźć się krajowej liście zaufania. Tylko w taki sposób można zapewnić interoperacyjność i rozpoznawalność wydawania poświadczeń atrybutów. Stosowanie zabiegu w art. 22g w rzeczywistości jest zastosowanie mechanizmu profilu zaufanego na poziomie portfela z pominięciem zasad eIDAS, świadczenia niekwalifikowanych usług zaufania i nadzoru nad tymi usługami. Jednocześnie przepis w aktualnym brzmieniu umożliwia ministrowi ds. informatyzacji konkurowanie, z rynkiem którego jest nadzorcą, w szczególności wydawanie poświadczeń na podstawie niepublicznych źródeł autentycznych.	1) w formacie danych określonym w rozporządzeniu wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2979); 2) opatrzone zaawansowaną pieczęcią elektroniczną weryfikowaną kwalifikowanym certyfikatem wpisaną na zaufaną listę zgodnie z art. 11. 3) zawierające dane i informacje, o których mowa w art. 22h ust. 2 pkt 2. 2. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej schematy elektronicznych poświadczeń atrybutów, o których mowa w ust. 1. Usunięcie art. 22h.
29.	Art. 1 pkt 9 dotyczący art. 22j	Przepis określony w art. 22j zauważa konflikt interesu jakim jest nadzorowanie rynku usług zaufania i świadczenie usług zaufania przez ministra właściwego ds. informatyzacji.	Zmiana zapisu art. 22j: Minister ds. informatyzacji nie może świadczyć usług zaufania określonych art. 22d i 22g ze względu na realizację roli nadzoru nad rynkiem usług zaufania.
30.	Art. 1 pkt 11 dotyczący art. 23	Artykuł ustanawia szereg działań nadzorczych ministra nad funkcjonowaniem eIDAS – wobec powyższego Minister ds. informatyzacji nie może pełnić roli dostawcy usług zaufania, ponieważ nie jest możliwe rozdzielenie funkcji dostawcy usługi i nadzoru usług. Co może naruszać zarówno bezpieczeństwo świadczenia usług, monopolizację, zależność od ministra możliwości świadczenia usług przez inne podmioty i jednostki. Jeżeli celem ustawy jest świadczenie bezpośrednio usług przez ministra ds. informatyzacji należy nadzór przenieść do innego podmiotu kompetentnego do realizacji nadzoru.	Konieczność podjęcia decyzji o przeniesieniu ww. nadzoru do kompetentnej jednostki lub zmiana innych zapisów upoważniających ministra ds. informatyzacji do realizacji usług zaufania i dostarczenia portfela cyfrowej tożsamości.
31.	Art. 1 pkt 12 dotyczący art. 23a	Art. 23 a jest iluzoryczny i w rzeczywistości nie wykazuje prawidłowej konstrukcji nadzoru oraz realizacji usług. W rzeczywistości dwie komórki organizacyjne w tym samym ministerstwie nie zapewniają niezależności nadzoru nad realizacją usług zaufania, które sam minister świadczy.	Konieczność podjęcia decyzji o przeniesieniu ww. nadzoru do kompetentnej jednostki niezależnej od ministra ds. informatyzacji lub zmiana innych zapisów upoważniających ministra ds. informatyzacji do realizacji usług zaufania i dostarczenia portfela cyfrowej tożsamości
32.	Brak przepisu Konieczna zmiana w artykule 27.	Stosowanie niektórych usług zaufania wymaga opublikowania certyfikatu kwalifikowanego, którego wydawcą nie jest minister ds. informatyzacji, ponieważ nie świadczy kwalifikowanych usług zaufania. W szczególności dotyczyć to będzie kwalifikowanych certyfikatów do weryfikacji poświadczeń atrybutów.	Dodanie pkt 2a) publikuje kwalifikowane certyfikaty służące do świadczenia usług zaufania.
33.	Brak przepisu Konieczność uzupełnienia	Przepisy karne nie uwzględniają kar wynikających ze świadczenia innych usług zaufania niż wydawanie certyfikatów. W szczególności nie ujęto tam kar za wydawanie fałszywych dowodów doręczenia elektronicznego, nieprawdziwych	Wskazanie odpowiednich przepisów karnych w zakresie nowych usług zaufania.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
	rozdziału 6 przepisy karne	poświadczeń atrybutów, fałszywych innych poświadczeń wydawanych przez dostawców usług zaufania.	
34.	Brak przepisu Dodanie do Art. 1 przepisu dotyczącego art. 27 ust. 2 UoUZoIE	Proponowana poprawka jest logiczną konsekwencją i zapewnia na poziomie państwa członkowskiego mechanizm realizacji przepisu art. 15 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (wersja skonsolidowana)	W UoUZoIE art. 27 ust. 2: 1. dodaje się pkt 7 w brzmieniu: "7. bada zgodność z europejskimi normami zharmonizowanymi dostępności dla osób z niepełnosprawnościami usług zaufania;" 2. obecne punkty 7, 8, 9 otrzymują odpowiednio numery 8, 9 i 10.
35.	Art. 4. Pkt.1 Dot. Art. 3 pkt 14 lit b)	Utworzenie profilu zaufanego podmiotu publicznego idzie w poprzek założeniom Europejskich Ram Tożsamości Cyfrowej. Konstrukcja każdego środka identyfikacji wymaga określenia wymagań utworzenia środka, zarządzania nim oraz jego użycia. Rozwiązanie wskazane w ustawie nie jest środkiem identyfikacji elektronicznej, ponieważ nie przypisano do niego mechanizmu uwierzytelnienia, w rzeczywistości nie pozwala na realizację procesu identyfikacji podmiotu publicznego. Tworzenie środka, którego jedynym celem jest powielenie zakresu KPP (Katalogu Podmiotów Publicznych) nie ma sensu ani technicznego, ani użytkowego. Zamiast tego, w zgodzie z eIDAS2 należy rozważyć możliwość wydawania elektronicznego poświadczenia atrybutów zawierającego dane KPP.	Wykreślenie zmiany art. 3 pkt. 14 lit b) oraz wszystkich kolejnych zmian wynikających z powyższej.
36.	Art. 4. Pkt.1 Dot. Art. 3 pkt 14 lit c)	Utworzenie profilu zaufanego osoby reprezentującej podmiot publiczny idzie w poprzek założeniom Europejskich Ram Tożsamości Cyfrowej. Profil zaufany jest środkiem identyfikacji skonstruowanym w 2008 roku i opiera się na założeniach operacyjnych bazodanowego systemu identyfikacji elektronicznej z luźnym przypisaniem środków uwierzytelniających, które są źródłem wielu ryzyk. Możliwość reprezentacji podmiotu publicznego w ramach systemu identyfikacji powinna być realizowana za pomocą kwalifikowanego poświadczenia atrybutu. Źródłem takiego atrybutu jest decyzja osób dających upoważnienie do reprezentacji. W rzeczywistości docelowo mechanizm powinien być realizowany przez portfel biznesowy podmiotu publicznego. Utworzenie profilu zaufanego opartego na zasadach określonych w proponowanej zmianie do ustawy o informatyzacji będzie bardzo drogim rozwiązaniem w zakresie budowy i utrzymania procesowego, a także powielaniem błędów z projektów które w minionych latach skończyły się fiaskiem ministerstwie ds. informatyzacji – tj. rejestru upoważnień.	Wykreślenie zmiany art. 3 pkt. 14 lit c) oraz wszystkich kolejnych zmian wynikających z powyższej.

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
37.	Art. 4. Pkt.6	Mechanizm tworzenia profili zaufanych podmiotów publicznych oraz profili zaufanych osób reprezentujących podmiot publiczny nie ma sensu, ponieważ nie zawiera ani zakresu reprezentacji, okresu używania, jego zakładanie nie wynika z prawa do reprezentacji podmiotu publicznego oraz wskazany mechanizm nie daje możliwości osobie udzielającej prawa do reprezentacji zarządzanie tym prawem. Należy rozważyć możliwość wprowadzenia przepisów umożliwiających utworzenia na upoważnienia podpisanego przez osobę kierującą podmiotem publicznym odpowiedniego poświadczenia atrybutów	Opracowanie zamiast koncepcji nowego profilu zaufanego przepisów pozwalających na tworzenie i zarządzanie kwalifikowanymi poświadczeniami atrybutów potwierdzającymi prawo do reprezentacji podmiotu publicznego, lub powiązanie z podmiotem publicznym. Pozwoli to na stosowanie poświadczeń atrybutu wraz z uznanymi krajowo środkami identyfikacji elektronicznej.
38.	Art. 5 pkt. 1 Dot. Art. 2 pkt 6a	Tworzenie definicji podmiotu niepublicznego realizującego zadania publiczne ma na celu dalszą monopolizację rynku doręczeń elektronicznych przez Pocztę Polską, uniemożliwiając tym podmiotom wybór usługi pozwalającej na obsługę doręczeń elektronicznych. Należy zwrócić uwagę, że w tym momencie na rynku polskim występuje 5 kwalifikowanych dostawców usług zaufania, którzy mogą te funkcje realizować, podlegają nadzorowi. Działania ministra ds. informatyzacji powinny iść w kierunku nadzoru rynku i stworzenia przestrzeni jego rozwoju a nie dalszej jego monopolizacji. Co więcej zaproponowane zmiany, ponieważ naruszają konkurencyjność rynku podmiotów świadczących usługi drogą elektroniczną zazwyczaj za opłatą będzie wymagać przeprowadzenia procedury notyfikacji.	Wykreślenie proponowanej zmiany i wszystkich odniesień w ustawie.
39.	Art. 5 pkt. 2	O ile nie kwestionujemy pomysłu utworzenia katalogu podmiotów publicznych, to jego tworzenie w ustawie o doręczeniach elektronicznych jest niezgodne z zakresem przedmiotowym wskazanej ustawy. Katalog ten powinien być elementem ustawy o informatyzacji lub innej ustawy w ww. zakresie.	Przeniesienie zakresu do innej ustawy.
40.	Art. 5 pkt 2 dot. Zmian w art. 11	Takie powiązanie katalogu podmiotów publicznych i włączenie w niego podmiotów niepublicznych uniemożliwia podmiotom niepublicznym realizującym zadania publiczne wybór dostawcy usług doręczeń, rezygnacje ze struktury skrzynki doręczeń elektronicznych która jest powiązana tylko z publiczną usługą doręczeń elektronicznych. W efekcie stanowi zwiększenie monopolizacji usług doręczeń elektronicznych i uzależnienie kolejnych pomiotów od Poczty Polskiej.	Usunięcie zmiany.
41.	Art. 6 pkt 2 dot. Art. 14a ust. 2	Wskazany zapis może uniemożliwiać jednej osobie posiadać w ramach portfela zarówno dane identyfikujące jego jak i dane identyfikujące osobę prawną. W tym zakresie intencja ustawodawcy jest niejasna.	Zmiana: Zestaw danych identyfikujących osobę fizyczną, umieszczanych w Europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, obejmuje.
42.	Art. 6 pkt 2 dot. Art. 14a ust. 2. Pkt. 5)	Projektowana ustawa uniemożliwia wydanie europejskiego portfela cyfrowej tożsamości osobom nie posiadającym numeru PESEL. Uniemożliwia to wydanie	Zmiana Art. 14a ust. 2. Pkt 5) numer PESEL lub inny numer jednoznacznie identyfikujący osobę fizyczną;

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		portfela osobom, które czasowo przebywają w Polsce w związku z realizowaną pracą. Uniemożliwi też posiadanie portfela osobom posiadającym Kartę Polaka.	
43.	Art. 6 pkt 2 dot. Art. 14a ust. 3	Wskazany zapis może uniemożliwiać jednej osobie posiadać w ramach portfela zarówno dane identyfikujące jego jak i dane identyfikujące osobę prawną. W tym zakresie intencja ustawodawcy jest niejasna.	Zmiana: Zestaw danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą, umieszczanych w Europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, obejmuje.
44.	Art. 6 pkt 2 dot. Art. 14a ust. 3	Nie jest jasne, w jaki sposób dane dotyczące osoby prawnej są powiązane z danymi osoby fizycznej i co stanowi podstawę tego powiązania. W efekcie prezentacja danych dotyczących osoby prawnej będzie miała nieokreślone skutki prawne.	Uzupełnienie zestawu danych o relację pomiędzy osobą fizyczną w której portfelu umieszczono zestaw danych identyfikujących osobę prawną.
45.	Art. 6 pkt 2 dot. Art. 14a ust. 5	Zaproponowany przepis nie spełnia wymagań art. 3 rozporządzenia 2024/2977, które wymaga w procesie nie tylko potwierdzenia tożsamości, ale także spełnienia warunków bezpieczeństwa, powiązania kryptograficznego, oraz uruchomienia procesu zarządzania danymi. W związku z tym zamiast opisania automatycznej procedury w ustawie, pozostawić tylko zapisy dotyczące pochodzenia danych w ww. zestawie. Jednocześnie przepis uniemożliwia wydawanie portfela osobie nieposiadającej numeru PESEL, np. posiadających Kartę Polaka.	5. Dane, o których mowa, w ust. 2: 1) pkt 1 - 8 – pochodzą z rejestru PESEL, 2) pkt 9 – pochodzą z Rejestru Dowodów Osobistych lub jeżeli nie jest to możliwe z dokumentu potwierdzającego tożsamość spełniającego zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, zwanej dalej „ICAO", określone w dokumencie - Doc 9303 Machine Readable Travel Documents część 10, 11 i 12 Uzupełnienie przepisu o możliwość wydania portfela osobie nieposiadającej numeru PESEL.
46.	Art. 6 pkt 2 dot. Art. 14a ust. 6 pkt 1)	Wskazany zapis może być mylący. Chodzi o przetwarzanie danych przez 20 lat od unieważnienia instancji portfela zawierającej ten zestaw danych.	20 lat od dnia unieważnienia europejskiego portfela tożsamości cyfrowej, zawierającego dane, o których mowa w art. 14 ust. 2 lub art. 14 ust. 2 rozporządzenia 910/2014– w przypadku danych …
47.	Art. 6 pkt 2 dot. Art. 14a ust. 7	Uznanie rejestru transakcji za dane podlegające odtworzeniu wymaga ich przetwarzania przez ministra ds. informatyzacji poza kontrolą użytkownika. Stanowić to może podejrzenie używania portfela do inwigilacji i kontroli używania portfela.	Usunięcie rejestru transakcji z zakresu określonego ust. 7 pkt 1) Jednocześnie wskazanie, że portfel będzie umożliwiał wskazanie przez użytkownika miejsca zbierania rejestru transakcji poza obszarem, który może kontrolować minister ds. informatyzacji. Np. na prywatnym dysku lub w usłudze podmiotu trzeciego.
48.	Art. 6 pkt 2 dot. Art. 14b	Artykuł nie zawiera i nie odnosi się do wymagań rozporządzenia 2024/2977 w zakresie wydawania PID, warunków uwierzytelnienia i weryfikacji wszystkich komponentów portfela cyfrowej tożsamości. Należy uzupełnić wskazany przepis o ww. warunki.	Wskazanie, że art. 14b dotyczy warunków wydania danych identyfikujących osobę do portfela cyfrowej tożsamości i oparcie ich na wymagania CIR 2024/2977

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
49.	Art. 6 pkt 2 dot Art. 14c ust 1.	Przepis powinien jednoznacznie określić zakres powiązania osoby fizycznej i osoby prawnej w zakresie posługiwania się portfelem osoby prawnej. Napisanie w przepisie kto może zostać nie daje podstawy do jednoznacznej interpretacji tego powiązania w momencie prezentacji danych z portfela osoby prawnej.	Przepis powinien konstruować najpierw znaczenie prawne powiazania osoby prawnej z osobą fizyczną na której portfelu umieszczono dane identyfikujące osobę prawną. Dopiero później powinien definiować, że tylko te osoby mogą w swoim portfelu osoby fizycznej posiadać odpowiednie dane osoby prawnej.
50.	Art. 6 pkt 2 dot Art. 14c ust 4.	Przepis może budzić wątpliwości czy unieważnienie portfela osoby prawnej umieszczonego w portfelu osoby fizycznej unieważnia także portfel osoby fizycznej. Kłopot polega na tym, że od samego początku dane identyfikujące osobę prawną są mylone w tej ustawie z portfelem osoby prawnej. A tak naprawdę konstrukcja prawna powinna dotyczyć możliwości umieszczenia danych identyfikujących osobę prawną w portfelu osoby fizycznej.	Wskazać, że unieważnienie portfela osoby prawnej nie musi oznaczać unieważnienia portfela osoby fizycznej.
51	Art. 6 pkt 2 dot Art. 14e ust 9.	W przypadku gdy parametr LUP służący do wyliczenia rekompensaty wynosi więcej niż 10 milionów, do wyliczenia przyjmuje się liczbę 10 milionów. Wszystkim stronom powinno zależeć aby użytkowników Portfela było więcej niż obecnie posiada mObywatel. Podobnie wszystkim powinno zależeć, aby upowszechnił się jeden podstawowy sposób elektronicznego podpisywania dokumentów z wykorzystaniem podpisu kwalifikowane. Stawka wymieniona z projekcie ustawy za użytkownika (nie za złożony podpis) jest symboliczna. Dlatego też uważamy, że ograniczanie wyliczeń na poziomie 10 mln użytkowników jest przejawem braku wiary w napełnienie systemu Portfela większą liczbą obywateli korzystających z uniwersalnego rozwiązania podpisu kwalifikowane.	Wykreślenie Art. 14e ust 9.
52	Art. 6 pkt 2 dot Art. 14f ust. 1.	Przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny, o którym mowa w art. 22e ust. 1, rozumie się składanie tego podpisu w celu oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w celu załatwienia sprawy prywatnej, niezwiązanej z wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenia reprezentuje	Nowe brzmienie art. Art. 14f. 1. *Przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny,* o którym mowa w art. 22e ust. 1, *rozumie się składanie podpisu celem oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w celu załatwienia sprawy prywatnej, niezwiązanej z zawieraniem umów konsumenckich, wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenie reprezentuje lub w jakiej funkcjonowaniu uczestniczy.*
53	Art. 6 pkt 2 dot Art. 14g ust 1 pkt 2)	Zapis ogranicza możliwość dostarczenia odpowiedniego poświadczenia tylko do ministra ds. informatyzacji. Poświadczenie powinno móc być wydane przez publiczną lub kwalifikowaną usługę w postaci elektronicznego poświadczenia atrybutów. Wydawanie wszystkich poświadczeń atrybutów powinno być realizowane przez usługę zaufania wydawania poświadczeń atrybutów w imieniu podmiotu	uzyskanie elektronicznego poświadczenia atrybutów elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu; albo uzyskanie kwalifikowanego poświadczenia atrybutu, zawierającego dane, o których mowa w pkt 1;

Lp.	Artykuł, punkt, litera, akapit…	Opis uwagi	Propozycja zmiany
		publicznego, kwalifikowaną usługę wydawania poświadczeń atrybutów lub niekwalifikowaną usługę wydawania poświadczeń atrybutów. Proponowany zapis uniemożliwia stosowanie kwalifikowanych poświadczeń w tym celu.	
54	Art. 6 pkt 2 dot Art. 14g ust 1 pkt 2)	W sytuacji, gdy portfel ma umożliwiać składanie kwalifikowanych podpisów elektronicznych tworzenie w ramach portfela funkcjonalności o znacznie mniejszym poziomie uznania i wiarygodności podpisu elektronicznego stoi w sprzeczności z założeniami rozporządzenia eIDAS którego celem jest zapewnienie podpisywania pism i dokumentów kwalifikowanymi podpisami elektronicznym. Dodatkowo należy wskazać, że żaden inny podpis niż kwalifikowany nie jest uznawany transgranicznie co może dodatkowo spowodować niezrozumienie dla obywateli, jeśli podpis zaufany lub podpis osobisty zostanie użyty w transakcji.	7) kwalifikowanym podpisem elektronicznym, 8) zapewnia weryfikacje dokumentów opatrzonych podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym.
55	Art. 6 pkt 2 dot Art. 14g ust 2	Na bazie przepisu umożliwia się w portfelu udostępnianie funkcjonalności dowolnego systemu teleinformatycznego. W rzeczywistości przepis nie daje wymagań zwianych z rzeczywistą zasadnością utworzenia takiej funkcjonalności oraz zapewnieniem bezpieczeństwa takiego rozwiązania. Jednocześnie udostępnienie danych z rejestrów niepublicznych może stanowić konkurencję dla prywatnych kwalifikowanych i niekwalifikowanych usług wydawania poświadczeń atrybutów.	Ograniczenie przepisu tyko do usług, które mają znaczenie dla funkcjonowania portfela, nie naruszają konkurencyjności usług.
56	Art. 6 pkt 2 dot Art. 16	j.w.	j.w.