Tabela uwag
zgłoszonych w ramach konsultacji publicznych
do projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122)

lp.	Jednostka redakcyjna, do której wnoszone są uwagi	Podmiot wnoszący uwagi	Zgłoszone uwagi	Stanowisko
1.	Art. 1 pkt 1 - dot. art. 1 pkt 9	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga nieuwzględniona** W art. 11a rozporządzenia eIDAS jest mowa o jednoznacznym dopasowywaniu tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej, a nie o dopasowaniu atrybutów tożsamości.
2.	Art. 1 pkt 1 - dot. Art. 1 pkt 10	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga uwzględniona** Przepis zmieniono w celu uwzględnienia uwagi.
3.	Art. 1 pkt 1 - dot. art. 1 pkt 11	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga uwzględniona** Art. 1 pkt 11 zmieniono w celu uwzględnienia uwagi.
4.	Art. 1 pkt 1 - dot. art. 1 pkt 12 oraz 13	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo	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	**Uwaga częściowo uwzględniona** Należy zgodzić się z opinią, że nie wszystkie elektroniczne poświadczenia atrybutów muszą być uznawane w całej UE i co z tym idzie ich schematy powinny być zgłoszone do katalogu Komisji. Taką rolę

		Informatycznego (PTI) Związek Cyfrowa Polska (ZCP	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 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. Zmiana zapisu pkt 12) – ustanawia mechanizmy zapewnienia interoperacyjności dla atrybutów i schematów atrybutów na poziomie krajowym i europejskim	pełnią obecnie z powodzeniem dokumenty mobilne w aplikacji mObywatel i mimo że nie mają transgranicznej skuteczności są przydatne. Liczne podmioty zwracają się do Ministra Cyfryzacji o zapewnienie możliwości uzyskiwania w aplikacji mObywatel wydawania kolejnych dokumentów mobilnych, co tylko potwierdza zapotrzebowanie na krajowe rozwiązania. Projektowana ustawa przewiduje wydawanie przez ministra właściwego do spraw informatyzacji elektronicznych poświadczeń atrybutów ważnych tylko w kraju (na wniosek podmiotu odpowiedzialnego za źródło autentyczne) i nie wyklucza możliwości wydawania takich poświadczeń również bezpośrednio przez te podmioty jako niekwalifikowanej usługi zaufania. Istotnie jednak ustawa powinna nadać minimalne ramy dla takich „zwykłych” elektronicznych poświadczeń atrybutów, które nie są: a) kwalifikowanymi elektronicznymi poświadczeniami atrybutów, b) elektronicznymi poświadczeniami atrybutów wydawanymi przez podmiot sektora publicznego lub w jego imieniu spełniającymi wymagania art. 45f i załącznika VII do rozporządzenia eIDAS, c) elektronicznymi poświadczeniami atrybutów wydawanymi przez ministra właściwego do spraw informatyzacji do zapewnianego przez tego ministra portfela, które nie spełniają wymogów określonych w lit b. W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania zostały wprowadzone zmiany w rozdziale 2. Należy zgodzić się także, że powinno być określone dostępne publicznie miejsce, w którym znajdą się schematy elektronicznych poświadczeń atrybutów uznawanych tylko w kraju, w tym określenie ich struktury, polityki ich wydawania, źródła na jakich się opierają i wskazanie przepisów prawa mających zastosowanie. W związku z tym dodano przepis wprowadzający krajowy katalog schematów

				elektronicznych poświadczeń atrybutów. W art. 2 ustawy nie ma potrzeby umieszczać przepisu, że ustawa ta „ustanawia mechanizmy zapewnienia interoperacyjności dla atrybutów i schematów atrybutów na poziomie krajowym i europejskim”, gdyż interoperacyjność w zakresie europejskim została już ustanowiona rozporządzeniem eIDAS i przepisami wykonawczymi. Nie ma powodu, aby elektroniczne poświadczenia atrybutów wydawane tylko dla potrzeb krajowych opierały się o inne zasady, zwłaszcza, że jeśli okaże się, że niektóre z nich powinny znaleźć się w europejskim katalogu schematów, powinny być gotowe do takiego zgłoszenia.
5.	Art. 1 pkt 2 - dot. art. 4	PWPW S.A.	W ocenie PWPW S.A., dokonując zmian w przepisach prawa dotyczących zasad działania list zaufanych, należy doprecyzować tryb rejestracji zmian we wpisach do rejestrów usług zaufania w zakresie zmian w Politykach. Proponujemy, aby zmiany w przepisach wprowadzały następujący model działania organu nadzoru: jeżeli Polityka usługi zaufania związana jest z dodaniem przez dostawcę zaufanego nowej usługi zaufania nieświadczonej dotychczas przez dostawcę, organ nadzoru wydaje decyzję administracyjną o wpisie. Jednakże jeżeli dostawca w nowej Polityce przewiduje wyłącznie aktualizacje treści polityki w zakresie np.: 1) uwzględnienia np. najnowszych zmiany norm, 2) optymalizacji postanowień lub poprawek językowych, 3) zmian związanych ze strukturą działania dostawcy, organizacji zachowania wymagań dot. bezpieczeństwa, ról zaufanych itp., 4) zmian w zakresie rozszerzenia metod identyfikacji subskrybentów, metod uwierzytelniania, 5) zmian w postaci usprawnienia metod realizacji obowiązków wynikających z norm, 6) zmian technologii, protokołów, zabezpieczeń, jeżeli ich nazwy są wymienione w Polityce itp. - tego rodzaju zmiany, z uwagi na swój uzupełniający lub aktualizacyjny charakter, mogą być akceptowane przez organ nadzoru w postaci czynności materialno-technicznej (obecnie dopuszcza się wprost wskazanie w ustawie na taką czynność) w postaci zaktualizowania wpisu o nową wersję Polityki. W przyjętym modelu proces przedstawiałby się następująco: ¾ zgłoszenie nowej wersji polityki, ¾ analiza polityki przez organ nadzoru, ¾ wpisanie nowej wersji polityki jako czynność materialno-techniczna w terminie	**Uwaga nieuwzględniona** W treści Polityki będą wskazane zasady jej aktualizacji, nie wymaga to wprowadzenia zmian do projektowanej regulacji.

			30 dni od przekazania polityki przez dostawcę. Odmowa wpisania nowej wersji Polityki z uwagi na zbyt szeroki zakres zmian (np. dodanie nowego rodzaju usługi) albo wady merytoryczne Polityki następowałaby w trybie decyzji administracyjnej. Wskazane postępowanie jest oparte o dotychczasową wieloletnią praktykę działania organu nadzoru, odciążyłoby organ nadzoru a jednocześnie nie pozbawiłoby organu nadzoru jego uprawnień. Z punktu widzenia kwalifikowanych dostawców oraz dostawców nowych usług kwalifikowanych poświadczeń atrybutów usprawniłoby to realizację procesu rejestracji Polityki. Propozycja zmian w ustawie w ww. kierunku nie jest także z sprzeczna z przepisami rozporządzenie eIDAS, gdyż samo rozporządzenie w ww. zakresie nie wpływa na przepisy proceduralne dot. wpisywania/aktualizacji wpisów oraz wykreśleń. We wskazanym zakresie obowiązującym prawem są przepisy prawa krajowego, w szczególności art. 4 – 8 ustawy o z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji.	
6.	Art. 1 pkt 2 lit. a - dot. art. 4 ust. 1 pkt 3	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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	**Uwaga wyjaśniona** Zdaniem projektodawcy proponowane brzmienie ma to samo znaczenie. Przepis wskazuje, że do wydawania certyfikatów dostępu strony ufającej portfelowi oraz wydawania certyfikatów rejestracji strony ufającej portfelowi upoważnione są podmioty już świadczące usługi wydawania kwalifikowanych certyfikatów podpisu elektronicznego i kwalifikowanych certyfikatów pieczęci elektronicznej. Właściwa redakcja przepisu zostanie ustalona na późniejszym etapie.
7.	Art. 1 pkt 2 lit. c - dot. art. 4 ust. 6	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Zdaniem projektodawcy proponowane brzmienie ma to samo znaczenie. Właściwa redakcja przepisu zostanie ustalona na późniejszym etapie.
8.	Art. 1 pkt 3 - dot. art. 8	Polska Izba Ubezpieczeń	W kontekście art. 1 ust. 3 mowa jest o konsekwencji odebranie kwalifikowanemu dostawcy usług zaufania uprawnienia do wydawania takich certyfikatów i wykreśleniu go z rejestru dostawców. Przepis nie precyzuje jednak stanu prawnego strony ufającej, legitymizującej się certyfikatem wystawionym przez dostawcę, któremu zostały odebrane uprawnienia w trakcie trwania ważności	**Uwaga wyjaśniona** Wymogi dla walidacji podpisów kwalifikowanych podpisów elektronicznych oraz zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach określają odpowiednio art. 32 i 32a

			wydanego wcześniej certyfikatu. W związku z tym proponujemy po ust. 3 dodanie nowego ust. 3b w brzmieniu: „3b. Minister właściwy do spraw informatyzacji informuje niezwłocznie strony ufające dla których były wystawione certyfikaty przez dostawcę, któremu zostały odebrane uprawnienia do wydawania takich certyfikatów o fakcie wykreślenia takiego dostawcy. Certyfikaty wydane do dnia wydania decyzji o wykreśleniu z rejestru usługi wydawania certyfikatów dostępu strony ufającej portfela i certyfikatów rejestracji uznaje się za ważne do czasu wygaśnięcia ich terminu ich ważności”;	rozporządzenia eIDAS. Z przepisów tych wynika między innymi, że podpisy są ważne, jeżeli kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu. Z uwagi na to, że przyczyny wydania decyzji o wykreśleniu z rejestru kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego kwalifikowanej usługi zaufania mogą być różne, nie można przepisem prawa zdecydować, że co do zasady certyfikaty wydane przed wykreśleniem usługi z rejestru są w każdym przypadku nadal ważne. Ponadto minister nie może informować klientów dostawcy usług zaufania, któremu zostały odebrane uprawnienia do wydawania takich certyfikatów, ponieważ nie ma wiedzy o tych klientach.
9.	Art. 1 pkt 4 - dot. art. 16 pkt 4 i 5	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania zostały wprowadzone zmiany rozdziale 2.

10.	Art. 1 pkt 6 dot. art. 21aa	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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 identyfikacji elektronicznej, umożliwia linkowanie tożsamości, które są zaprzeczeniem reguł ustanawianych rozporządzeniem eIDAS [Sugeruje się] Usunąć pkt 6 wprowadzający art. 21aa w całości.	**Uwaga wyjaśniona** Nie można zgodzić się z przyjętym w uwadze założeniem, że węzeł krajowy identyfikacji elektronicznej będzie pośrednikiem dla środka identyfikacji elektronicznej, jakim jest portfel cyfrowej tożsamości (jak należy się domyślać - chodzi o pośrednictwo w rozumieniu art. 5b ust. 10 rozporządzenia eIDAS, gdzie wprost zakazuje się pośrednikom przechowywania danych na temat treści transakcji. Minister właściwy do spraw informatyzacji zapewnia zgodnie z art. 21a ustawy o usługach zaufania oraz identyfikacji elektronicznej funkcjonowanie węzła krajowego identyfikacji elektronicznej, a co za tym idzie świadczy usługę uwierzytelniania (a nie pośrednictwa w uwierzytelnianiu) użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła krajowego identyfikacji elektronicznej bezpośrednio albo za pośrednictwem węzła transgranicznego. Do węzła krajowego przyłączone są już liczne inne środki identyfikacji elektronicznej, a europejski portfel tożsamości cyfrowej zapewniany w ramach publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa w ust. 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, będzie tylko jednym z nich. Nie ma to zatem mowy o pośrednictwie w rozumieniu art. 5b ust. 10 rozporządzenia eIDAS. Zakłada się, że minister właściwy do spraw informatyzacji zapewniający usługę uwierzytelnienia przez węzeł krajowy identyfikacji elektronicznej nie będzie wpisany do rejestru stron ufających jako pośrednik, o którym mowa w art. 5b ust. 10 rozporządzenia eIDAS oraz w załączniku I pkt 14 i 15 rozporządzenia wykonawczego 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

				portfela (Dz. U. UE. L. z 2025 r. poz. 848), tylko jako dostawca usługi zapewniającej uwierzytelnienie użytkownika portfela na węźle krajowym identyfikacji elektronicznej. Zostanie to odpowiednio wpisane do rejestru stron ufających zgodnie wymogami pkt 1-12 załącznika I do rozporządzenia 2025/848. Będzie tylko jeden przypadek zamierzonego użycia – przygotowanie asercji SAML zawierającej każdorazowo standardowy zestaw danych przekazywany przez węzeł krajowy identyfikacji elektronicznej (imię, nazwisko, data urodzenia, PESEL). W szczególności minister nie będzie pośrednikiem przekazującym dane identyfikujące osobę w formacie przewidzianym w rozporządzeniu wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). W usłudze nie będzie również możliwe przekazywanie elektronicznego poświadczenia atrybutów, gdyż węzeł krajowy identyfikacji elektronicznej nie jest do tego przeznaczony. Zgodnie z uzasadnieniem do projektu celem tej usługi jest zapewnienie rozwiązania, które pozwoli użytkownikom środków identyfikacji elektronicznej, wydanych w systemach identyfikacji elektronicznej, przyłączonych do węzła krajowego identyfikacji elektronicznej, na uzyskanie podobnej informacji, jaką – zgodnie z art. 5a ust. 4 lit. d rozporządzenia eIDAS – i tak zapewniają europejskie portfele tożsamości cyfrowej w ramach dostępu do rejestru transakcji przeprowadzonych z wykorzystaniem tych portfeli. (…)Takie dane pozwolą użytkownikom podjąć działania zmniejszające dotychczasowe i przyszłe skutki kradzieży tożsamości oraz nieuprawnionego korzystania ze środków identyfikacji elektronicznej przez przestępców. Mając na uwadze, że kradzież tożsamości jest zagrożeniem realnym, jakie może się zdarzyć mimo najlepszych zabezpieczeń i musi być przewidywane

				zgodnie z przepisami rozporządzenia wykonawczego Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2981) - możliwość zapewnienia użytkownikom minimum środków ochrony pomniejszających skutki ewentualnych kradzieży jest zdaniem projektodawcy oczywista. Zdaniem projektodawcy, projekt zapewnia należyte wyważenie pomiędzy zapewnieniem prywatności i bezpieczeństwa. Pozbawienie użytkowników możliwości uzyskania przez nich kluczowych informacji w przypadku kradzieży tożsamości w imię ochrony ich prywatności byłoby błędem.
11.	Art. 1 pkt 9 - dot. art. 22a	IDENTT Sp. z o.o.	Centralizacja architektury a zasady eIDAS 2.0 Zaproponowana architektura opiera się na centralnym węźle krajowym, przez który przechodzą operacje identyfikacji i dopasowywania tożsamości (np. przetwarzanie danych w celu dopasowania do rejestru PESEL). Rozwiązanie to stoi w sprzeczności z architekturą EUDI Wallet zdefiniowaną w art. 5a ust. 4 rozporządzenia eIDAS 2.0, która zakłada, że użytkownik ma pełną kontrolę nad udostępnianiem danych, a wymiana danych ze stroną ufającą odbywa się bez udziału centralnego pośrednika. Logowanie operacji w centralnym węźle budzi poważne wątpliwości w zakresie ochrony prywatności obywateli oraz zasady minimalizacji danych. Propozycja zmiany: Doprecyzowanie w ustawie, że transakcje między portfelem a stroną ufającą odbywają się bez udziału centralnego węzła. Węzeł krajowy powinien być wykorzystywany wyłącznie w precyzyjnie określonych, niezbędnych scenariuszach (np. weryfikacja PESEL przy pierwszym uruchomieniu/użyciu).	**Uwaga nieuwzględniona** Nie można zgodzić się z przyjętym w uwadze założeniem, że węzeł krajowy identyfikacji elektronicznej będzie pośrednikiem dla środka identyfikacji elektronicznej, jakim jest portfel cyfrowej tożsamości (jak należy się domyślać - chodzi o pośrednictwo w rozumieniu art. 5b ust. 10 rozporządzenia eIDAS, gdzie wprost zakazuje się pośrednikom przechowywania danych na temat treści transakcji. Minister właściwy do spraw informatyzacji zapewnia zgodnie z art. 21a ustawy o usługach zaufania oraz identyfikacji elektronicznej funkcjonowanie węzła krajowego identyfikacji elektronicznej, a co za tym idzie świadczy usługę uwierzytelniania (a nie pośrednictwa w uwierzytelnianiu) użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła krajowego identyfikacji elektronicznej bezpośrednio albo za pośrednictwem węzła transgranicznego. Do węzła krajowego identyfikacji elektronicznej przyłączone są już liczne inne środki identyfikacji elektronicznej, a europejski portfel tożsamości cyfrowej

				zapewniany w ramach publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa w ust. 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne będzie tylko jednym z nich. Nie ma to zatem mowy o pośrednictwie w rozumieniu art. 5b ust. 10 rozporządzenia eIDAS. Zakłada się że minister właściwy do spraw informatyzacji zapewniający usługę uwierzytelnienia przez węzeł krajowy identyfikacji elektronicznej nie będzie wpisany do rejestru stron ufających jako pośrednik, o którym mowa w art. 5b ust. 10 rozporządzenia eIDAS oraz w załączniku I pkt 14 i 15 rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848) tylko jako dostawca usługi zapewniającej uwierzytelnienie użytkownika portfela na węźle krajowym identyfikacji elektronicznej. Zostanie to odpowiednio wpisane do rejestru stron ufających zgodnie wymogami pkt 1-12 załącznika I do rozporządzenia 2025/848. Będzie tylko jeden przypadek zamierzonego użycia – przygotowanie asercji SAML zawierającej każdorazowo standardowy zestaw danych przekazywany przez węzeł krajowy identyfikacji elektronicznej (imię, nazwisko, data urodzenia, PESEL). W szczególności minister nie będzie pośrednikiem przekazującym dane identyfikujące osobę w formacie przewidzianym 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). Przedmiotowe rozwiązanie architektoniczne przyjęto zatem z uwagi na wymagania stawiane przez rozporządzenie eIDAS, zapewnienie warunków do jak najpowszechniejszego wykorzystywania portfela do

				uwierzytelniania w usługach online oraz w celu ułatwienia dopasowania tożsamości użytkownika. Jednocześnie warto zauważyć, że projektowana ustawa umożliwia podmiotom zainteresowanym wykorzystywanie portfela do uwierzytelniania bezpośrednio po zarejestrowaniu w rejestrze stron ufających.
12.	Art. 1 pkt 6 - dot. art. 21aa	Krajowa Izba Rozliczeniowa	Zmiany dotyczące weryfikacji historii użycia środków identyfikacji elektronicznej w węźle krajowym (WK) Projekt – w dodawanym do ustawy art. 21aa – zakłada udostępnienie usług weryfikacji historii użycia środków identyfikacji elektronicznej w WK. Proponowana regulacja wzbudza poniższe wątpliwości: Ważne jest ustalenie interpretacji art. 21aa ust. 2 pkt 2. Nie jest jasne, jak należy rozumieć pojęcie „danych identyfikujących środek identyfikacji elektronicznej”. Środek identyfikacji elektronicznej nie ma żadnego identyfikatora. Nie wymaga tego żaden przepis, w tym w szczególności na poziomie europejskim. Używanie środka i uwalnianie danych również nie wymaga podawania żadnego jego identyfikatora. Proponujemy usunięcie tego punktu lub ewentualnie nadanie mu brzmienia: „wskazanie systemu identyfikacji elektronicznej przyłączonego do węzła krajowego, w którym został wydany środek identyfikacji elektronicznej, z którego skorzystał użytkownik”. Proponujemy, aby wymóg użycia środka identyfikacji elektronicznej na wysokim poziomie bezpieczeństwa w celu skorzystania z usługi weryfikacji historii użycia środka w WK nie dotyczył historii użycia środków identyfikacji elektronicznej na innym poziomie. Proponujemy, aby za wystarczający został uznany środek, którego historię użycia chce poznać użytkownik. W przeciwnym wypadku w celu poznania historii PZ nie wystarczy PZ, lecz w każdym przypadku będzie wymagany, np. EPTC. Oznaczałoby to przy okazji, że posiadacz EPTC mógłby skorzystać z tej usługi, a ten, który go nie posiada, nie poznałby historii, mimo częstego korzystania z WK na podstawie PZ.	**Ad. 1 – uwaga uwzględniona** Celem przepisu nie było wskazywanie identyfikatora środka identyfikacji elektronicznej tylko danych które jednoznacznie określą ten środek. Mogłaby to być pełna nazwa lub akronim. W związku z tym, że przepis wzbudza wątpliwości, art. 21aa ust. 1 otrzymał nowe brzmienie. **Ad. 2 – uwaga nieuwzględniona** Z uwagi na potrzebę zmniejszenia skutków potencjalnego skutecznego ataku na środek identyfikacji elektronicznej na średnim poziomie bezpieczeństwa, w celu uniemożliwienia atakującemu ustalenia w jakich systemach/usługach zaatakowany ma konta, przyjęto założenie, że historia użycia środków identyfikacji elektronicznej będzie dostępna tylko po uwierzytelnieniu na wysokim poziomie bezpieczeństwa. W Polsce będzie zapewniony dostęp do dwóch nieodpłatnych środków identyfikacji na wysokim poziomie bezpieczeństwa (profilu osobistego i europejskiego portfela tożsamości cyfrowej).
13.	Art. 1 pkt 6 - dot. art. 21aa ust. 2 pkt 2	PWPW S.A.	Projektowane brzmienie art. 21aa ust. 2 pkt 2 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej wymaga doprecyzowania o określenie, czy użytkownikowi przysługuje prawo do wglądu do informacji o środku identyfikacji elektronicznej udostępnionego w systemie identyfikacji elektronicznej (w tym wypadku krajowego systemu identyfikacji elektronicznej udostępnionego za pomocą Węzła Krajowego), czy też dowolnego środka, z którego użytkownik skorzystał za pomocą Węzła Krajowego.	**Uwaga wyjaśniona** Użytkownikowi przysługuje prawo do wglądu do informacji w zakresie dowolnego środka, z którego skorzystał użytkownik za pomocą węzła krajowego identyfikacji elektronicznej.
14.	Art. 1 pkt 9 - dot. art. 22a	Związek Przedsiębiorstw	W naszej ocenie Projekt ustawy powinien zostać uzupełniony w taki sposób, aby zapewniał możliwość pozyskiwania również tych danych, które są w praktyce	**Uwaga wyjaśniona** Należy zaznaczyć, że „dopasowywanie tożsamości”

	ustawy o usługach zaufania Art. 1 pkt 9 - dot. art. 22a ust. 4-5 ustawy o usługach zaufania Art. 6 pkt 2 - dot. art. 14a ust. 2-5 ustawy o aplikacji mObywatel	Finansowych w Polsce	niezbędne do realizacji obowiązków AML/KYC. Ewentualnie postulujemy o wprowadzenie możliwości uzyskiwania przez strony ufające, w ściśle określonych przypadkach i na podstawie przepisów szczególnych, dodatkowych danych niezbędnych do realizacji obowiązków ustawowych. Z tych względów postulujemy uzupełnienie Projektu ustawy o rozwiązania, które pozwolą stronom ufającym – w granicach i na podstawie przepisów prawa – wymagać przekazania kompletnego pakietu danych koniecznych do realizacji obowiązków ustawowych, tak aby wykluczyć ryzyko technicznego przesyłania niepełnych zestawów danych w usługach objętych podwyższonym reżimem regulacyjnym.	zgodnie z art. 3 pkt 55 rozporządzenia eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Powyższe oznacza, że celem przepisów nie jest ustalenie tożsamości celem wypełnienia obowiązków (AML/KYC) wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ale tylko dopasowanie tożsamości zweryfikowanej za pomocą środka identyfikacji elektronicznej wydanego w innym kraju UE do tożsamości już wcześniej zweryfikowanej. Należy podkreślić, że zakresy danych wskazane w projekcie ustawy wskazują na dane identyfikujące osobę, jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846). Tamże wskazuje się, że odpowiednio należy polegać na danych, o których mowa w rozporządzeniu wykonawczym (UE) 2024/2977 wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi lub zestawie danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. W związku z tym, jeżeli dopasowanie jest dokładne i jednoznaczne na podstawie ww. danych wraz zaproponowaną procedurą uzupełniającą dopasowanie uważa się za skuteczne. System dopasowywanie tożsamości co do zasady zgodnie z art. 2 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/846 dotyczy usług online

				oferowanych przez podmiot sektora publicznego lub w jego imieniu. W przypadku gdy prywatna strona ufająca jest zobowiązana na podstawie art. 5f ust. 2 rozporządzenia eIDAS do akceptacji europejskich portfeli tożsamości cyfrowej i jednocześnie zobowiązana do stosowania przepisów wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, to w zależności od tego czy akceptacja portfela dotyczy już istniejącego konta użytkownika (dla którego już stwierdzono komplet wymaganych danych) czy też nowego – procedury powinny być inne. W przypadku konieczności uzyskania dodatkowych danych wykraczających poza zakres danych identyfikujących osobę przewidziany w rozporządzeniu wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977) odpowiednio zakres tych dany powinien zostać wpisany przez taki podmiot do rejestru stron ufających. Kwestią wykraczającą poza możliwości krajowych regulacji jest zgłoszenie przez inne państwa członkowskie atrybutów potwierdzających dodatkowe dane. W zakresie danych nieobjętych (niewymienionych) załącznikiem VI do rozporządzenia eIDAS, nie występuje obowiązek ich zgłaszania. Przy wypełnianiu obowiązków AML/KYC znaczenie może mieć proces uwierzytelniania lub przekazywania atrybutów stronom ufającym przy pomocy portfela i w tym zakresie znaczenie mogą mieć przepisy o stronach ufających. Zgodnie z przepisami dotyczącymi rejestracji w rejestrze stron ufających, w tym wskazywania zakresu danych dla każdej usługi, jak również propozycji polegania na certyfikatach rejestracji strony ufającej, portfele tożsamości cyfrowej automatycznie rozpoznają zakres danych, jaki jest wymagany dla określonej usługi i po stronie użytkownika pozostaje wybór, czy z danej

				usługi skorzystać. Z drugiej strony w przypadku otrzymania żądania ujawnienia danych, które użytkownikowi wydaje się nadmiarowe lub podejrzane, będzie miał on możliwość zgłoszenia tego faktu organowi ochrony danych osobowych.
15.	Art. 1 pkt 9 - dot. art. 22a ust. 1	PWPW S.A.	W ocenie PWPW S.A. procedura krajowa poświadczania atrybutów elektronicznych powinna zostać powiązana z procesem opracowywania wzorów dokumentów publicznych, wytwarzania dokumentów publicznych, procesem ich indywidualizacji i personalizacji, która została uregulowana w przepisach ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669, z późn. zm.). Obecnie projekt ustawy wprowadza bowiem odrębną od uregulowanej przepisami ww. ustawy procedurę dotyczącą elektronicznego poświadczania atrybutów. Projekt nie uwzględnia bowiem w żadnym zakresie uczestnictwa podmiotów biorących udział w procesie kształtowania polityki bezpieczeństwa dokumentów publicznych na gruncie przepisów ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych w procesie poświadczania elektronicznych atrybutów. W szczególności projekt ustawy pomija: 1) Ministra Spraw Wewnętrznych i Administracji („MSWiA") jako organu kształtującego obecnie politykę bezpieczeństwa dokumentów publicznych i sprawującego nadzór nad systemem bezpieczeństwa dokumentów publicznych; 2) Ministra Infrastruktury i innych emitentów dokumentów publicznych – jako organów odpowiedzialnych za opracowywanie wzorów dokumentów publicznych i biorących udział w cyklu życia dokumentu publicznego; 3) Komisję do spraw dokumentów publicznych – jako organu pomocniczego MSWiA, do zadań którego należy w szczególności uczestniczenie w procesie opracowywania wzoru dokumentu publicznego, inicjowanie zabezpieczeń dokumentu publicznego oraz kontrola wytwórców blankietów dokumentów publicznych; 4) wytwórcę wyłącznego – jako podmiotu, któremu przysługuje prawo wyłączne w zakresie wytwarzania, indywidualizacji i personalizacji niektórych dokumentów publicznych, w tym dokumentów z warstwą elektroniczną (dowody osobiste). Projekt ustawy zakłada, że minister właściwy do spraw informatyzacji będzie w praktyce głównym podmiotem odpowiedzialnym za wydawanie elektronicznych poświadczeń atrybutów (tj. cyfrowych odpowiedników danych z dokumentów publicznych). Powoduje to konsolidację w ramach jednego organu (Ministra Cyfryzacji) wykonywanie zarówno funkcji nadzorczych (w zakresie usług zaufania oraz europejskiego portfela tożsamości), jak również czynności wykonawczych związanych z europejskim portfelem tożsamości, a także świadczenie samych usług w ramach tego portfela. Zapewnienie przejrzystości, jednoznacznej odpowiedzialności i uniknięcie konfliktu interesów wymaga rozdzielenia tych	**Uwaga wyjaśniona** Dokumenty publiczne nie są i nie były również wcześniej przedmiotem 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 (rozporządzenia eIDAS). Ostatnie zmiany wprowadzone do rozporządzenia eIDAS rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ustanowiły między innymi europejski portfel tożsamości cyfrowej i nową usługę zaufania, jaką jest wydawanie elektronicznych poświadczeń atrybutów. Zarówno europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów, zostały nie tylko zdefiniowane w rozporządzeniu eIDAS, aktach wykonawczych do tego rozporządzenia, ale również precyzyjnie opisano wymagania organizacyjne i techniczne wobec tych narzędzi wskazując na właściwe normy Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI). Z pewnością zatem europejski portfel tożsamości cyfrowej, jak również elektroniczne poświadczenia atrybutów, nie są dokumentami publicznymi w rozumieniu ustawy o dokumentach publicznych, jak również należą do odrębnego niezależnego reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim. Nie można zgodzić się zatem z tezą, że ww. przepisy europejskie wyłączające do odrębnego reżimu prawnego określone dokumenty w postaci elektronicznej będą miały jakikolwiek negatywny wpływ na jednolitość polityki bezpieczeństwa dokumentów publicznych, jak i szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub

			funkcji. Zaproponowane przez Ministra Cyfryzacji rozwiązanie – w przypadku wejścia w życie projektu ustawy w aktualnym brzmieniu – będzie skutkowało powstaniem dualizmu w zakresie systemu dokumentów publicznych, ponieważ w odniesieniu do dokumentów w postaci papierowej podmiotami odpowiedzialnymi będą nadal podmioty wskazane w przepisach ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych, w szczególności zaś Minister Spraw Wewnętrznych i Administracji, zaś w odniesieniu do dokumentów publicznych w formie cyfrowej wyłącznie właściwy będzie Minister Cyfryzacji („MC"). W ocenie PWPW proces elektronicznego poświadczania atrybutów powinien być spójny z tworzonymi dokumentami publicznymi, a w przypadku gdy atrybuty opierają się na treści dokumentu publicznego – ważność elektronicznego poświadczenia atrybutów powinna być powiązana z ważnością (fizycznego) dokumentu publicznego. Uwzględniając powyższe stanowisko PWPW S.A. proponuje w przedstawionym projekcie ustawy przynajmniej sformułować odpowiednie przepisy: 1) nakładające obowiązek współpracy między MSWiA a MC w zakresie zasad tworzenia atrybutów powiązanych z dokumentami publicznymi; 2) uzupełniające skład osobowy Komisji do spraw dokumentów o ekspertów posiadających wiedzę w zakresie identyfikacji elektronicznej. Propozycja brzmienia przepisu: 1) w projektowanym brzmieniu art. 22a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725) jako nowy ust. 1 dodać przepis w brzmieniu: „1. Minister właściwy do spraw informatyzacji współpracuje z ministrem właściwym do spraw wewnętrznych w zakresie działań obejmujących identyfikację elektroniczną oraz tworzenie schematów i wydawanie elektronicznych poświadczeń atrybutów, w zakresie w jakim dane wykorzystywane w procesie identyfikacji elektronicznej lub tworzenia elektronicznych poświadczeń atrybutów są związane z danymi zawartymi w dokumentach publicznych w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. 1669, z późn. zm.)."; 2) po art. 4 należy dodać przepis nowelizujący ustawę z dnia 22 listopada 2018 r. o dokumentach publicznych w brzmieniu: „Art. 5. W ustawie z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881) wprowadza się następujące zmiany: 1) w art. 1 dodaje się ust. 4 w brzmieniu:	potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami. Wprost przeciwnie, europejskie portfele tożsamości cyfrowej i elektroniczne poświadczenia atrybutów mogą i powinny stać się ważnym uzupełnieniem dokumentów publicznych w rozumieniu ustawy o dokumentach publicznych i skutecznie zastępować je w usługach online i stosownych przypadkach również w trybie offline (zob. art. 3 pkt 2, art. 5a ust. 4 lit. a oraz ust. 5 lit. a ppkt III rozporządzenia eIDAS). W tym miejscu warto podkreślić, że z uwagi na kryptograficzne zabezpieczenia europejskiego portfela tożsamości cyfrowej i elektronicznych poświadczeń atrybutów ich weryfikacja przez strony ufające nie będzie wymagała znajomości zabezpieczeń, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 1 lipca 2022 r. w sprawie wykazu minimalnych zabezpieczeń dokumentów publicznych przed fałszerstwem (Dz. U. poz. 1456), a jedynie posiadania oprogramowania do weryfikacji ważności elektronicznego poświadczenia atrybutów lub zestawu danych identyfikujących osobę. Co do zasady z przepisów europejskich już wynika, że państwa członkowskie są zobowiązane do zapewnienia co najmniej jednego europejskiego portfela tożsamości cyfrowej (który może być zapewniony bezpośrednio przez państwo członkowskie, na podstawie upoważnienia od państwa członkowskiego lub niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie). Zakładając, że zgłoszona uwaga nie podważa założenia, że europejski portfel tożsamości cyfrowej będzie wydawany przez ministra właściwego do spraw informatyzacji pozostaje wyjaśnienie sposobu zapewniania i zasad uznawania elektronicznych poświadczeń atrybutów. Rozporządzenie eIDAS wprost w art. 5f ust. 1 i 2 oraz art. 6 ustanawia obowiązek transgranicznego uznawania środków identyfikacji elektronicznej, w tym europejskich portfeli tożsamości cyfrowej w usługach publicznych i w części usług prywatnych. Ponadto 45b ust. 2 stanowi, że

			„4. Minister, kształtując politykę bezpieczeństwa dokumentów publicznych, współpracuje z ministrem właściwym do spraw informatyzacji w prowadzeniu działań związanych z identyfikacją elektroniczną opartą na danych związanych z dokumentami publicznymi, w zakresie tworzenia schematów i elektronicznych poświadczeń atrybutów, oraz w prowadzeniu działań związanych z funkcjonowaniem scentralizowanego rejestru, o którym mowa w art. 21a ust. 1 lit. c ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725), umożliwiającego dopasowywanie tożsamości, o którym w art. 11a 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, z późn. zm.).”; 2) w art. 49 w ust. 3 pkt 3 otrzymuje brzmienie: „3) do pięciu członków powołanych spośród ekspertów innych podmiotów zajmujących się dokumentami publicznymi, w szczególności posiadających udokumentowane doświadczenie w działalności eksperckiej w zakresie identyfikacji elektronicznej.”.	kwalifikowane elektroniczne poświadczenie atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ma taki sam skutek prawny jak poświadczenia wydane zgodnie z prawem w postaci papierowej. Celem tych przepisów jest niewątpliwie zapewnienie w całej UE wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w UE, co wynika z wprost motywów 1 i 2 preambuły. Mając na uwadze, że przepisy rozporządzenia eIDAS stosuje się wprost, oznacza to, że zarówno kwalifikowani dostawcy usług zaufania, jak i krajowe podmioty odpowiedzialne za źródła autentyczne mogą wydawać elektroniczne poświadczenia atrybutów ważne w całej UE pod warunkiem, że spełnią stosowne wymagania wynikające z przepisów rozporządzenia eIDAS i aktów wykonawczych. Dodatkowo rozporządzenie eIDAS umożliwia wyznaczenie przez państwa członkowskie podmiotu sektora publicznego, upoważnionego do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne. Istotne jest również że przepisy rozporządzenia eIDAS nie przewidują wyznaczenia do takiej roli podmiotu innego niż publiczny. Wydaje się to oczywiste z uwagi na to, że państwa członkowskie co do zasady zgodnie z art. 45e zapewniają środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację atrybutów polegających na źródłach autentycznych w sektorze publicznym drogą elektroniczną, na żądanie użytkownika. Propozycja, aby podmiotem, który ma możliwość wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne był minister

				właściwy do spraw informatyzacji nie wyklucza możliwości wydawania elektronicznych poświadczeń atrybutów przez podmioty w swoim imieniu. W związku z niepewnością w tym zakresie proponuje się zmianę w proponowanym art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej. Warto również wskazać na projektowany przepisy ustawy o usługach zaufania oraz identyfikacji elektronicznej, z których wynika, że minister właściwy do spraw informatyzacji wydaje elektroniczne poświadczenia atrybutów na wniosek podmiotów zainteresowanych zawierający w szczególności odniesienie do przepisów, norm lub wytycznych, jeżeli mają zastosowanie. Podsumowując, nie ma wątpliwości że w związku z proponowanymi przepisami nie ucierpi szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami.
16.	Art. 1 pkt 9 w zakresie art. 22a ust. 2 pkt 2	Konfederacja Lewiatan	Niewystarczający zakres „minimalnego zestawu danych” dla procesów AML/KYC Zgodnie z projektowanym art. 22a ust. 2 pkt 2) ustawy o usługach zaufania oraz identyfikacji elektronicznej system scentralizowany zapewnia w szczególności możliwość żądania przez stronę ufającą od osoby fizycznej podania dodatkowych danych, o których mowa w ust. 4 pkt 3, i przekazania tych danych przez osobę fizyczną celem jednoznacznego dopasowania tożsamości w przypadku, gdy dopasowanie tożsamości jest niejednoznaczne. Pragniemy zaznaczyć, że wskazany ust. 4 pkt 3 (rozumiemy, że chodzi o ust. 4 pkt. 3 z art. 22a) nie istnieje. Zgodnie z projektowanym art. 22a ust. 3 (pkt 1) ustawy o usługach zaufania oraz identyfikacji elektronicznej, w systemie scentralizowanym przetwarzane są dane osobowe obejmujące dane identyfikacyjne osoby, o którym mowa w załączniku do rozporządzenia wykonawczego 2015/1501 - w przypadku osoby fizycznej posługującej się notyfikowanym środkiem identyfikacji elektronicznej. Przepis ten odnosi się do załącznika do rozporządzenia wykonawczego 2015/1501 gdzie określono minimalny zestaw danych dotyczących osoby fizycznej - obowiązkowych (imię, nazwisko, data urodzenia, PESEL) oraz zestaw danych dodatkowych (imię oraz nazwisko rodowe, miejsce urodzenia, aktualny adres, płeć). Zakres ten jest zdecydowanie niewystarczający do wypełnienia obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (AML). W katalogu brakuje kluczowych obligatoryjnych danych, takich jak: seria i numer dokumentu tożsamości, data ważności dokumentu, miejsce (miasto) i kraj	**Uwaga wyjaśniona** Celem systemu scentralizowanego jest jednoznaczne dopasowanie tożsamości w rozumieniu art. 3 pkt 55 oraz art. 11a rozporządzenie eIDAS, jak również przepisów rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846. Należy zaznaczyć, że "dopasowywanie tożsamości" zgodnie z art. 3 pkt 55 rozporządzenia eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Powyższe oznacza, że celem przepisów nie jest ustalenie tożsamości celem wypełnienia obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ale tylko dopasowanie tożsamości zweryfikowanej za

			urodzenia. W związku z czym, instytucje obowiązane (w tym instytucje pożyczkowe) nie będą mogły polegać wyłącznie na Portfelu tożsamości cyfrowej przy onboardingu klienta lub zawieraniu umów/procesowaniu transakcji, co zmusi je do dublowania procesów weryfikacji danych.	pomocą środka identyfikacji elektronicznej wydanego w innym kraju UE do tożsamości już wcześniej zweryfikowanej. Należy podkreślić, że zakresy danych wskazane w projekcie ustawy wskazują na dane identyfikujące osobę jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846). Tamże wskazuje się, że odpowiednio należy polegać na danych, o których mowa w rozporządzeniu wykonawczym (UE) 2024/2977 wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi lub zestawie danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. W związku z tym, jeżeli dopasowanie jest dokładne i jednoznaczne na podstawie ww. danych wraz zaproponowaną procedurą uzupełniającą dopasowanie uważa się za skuteczne. Podsumowując – celem scentralizowanego systemu dopasowania tożsamości jest: a) wstępne ustalenie, czy osoba fizyczna używająca zagranicznego środka identyfikacji elektronicznej (czyli jednoznacznie zidentyfikowana, czego gwarantem jest państwo członkowskie UE) miała nadany nr PESEL i jaki to numer, co pozwoli na jednoznaczną jej identyfikacją w Polsce bez potrzeby weryfikacji dokumentów tożsamości, b) przesłanie danych (za zgodą tej osoby) do końcowej strony ufającej z ustalonym nr PESEL lub w przypadku niedopasowania do rejestru PESEL – danych identyfikujących osobę przekazywanych transgranicznie.

				Celem tych przepisów nie jest weryfikacja w każdym przypadku serii i numeru dokumentu tożsamości, daty ważności dokumentu oraz miejsca i kraju urodzenia. System dopasowywania tożsamości co do zasady zgodnie z art. 2 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/846 dotyczy usług online oferowanych przez podmiot sektora publicznego lub w jego imieniu. W przypadku gdy prywatna strona ufająca jest zobowiązana na podstawie art. 5f ust. 2 rozporządzenia eIDAS do akceptacji europejskich portfeli tożsamości cyfrowej i jednocześnie zobowiązana do stosowania przepisów wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, to w obszarze AML/KYC zaproponowano rozwiązanie tego problemu przez zmianę w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu w zakresie art. 36 ust. 1 pkt 1 lit d. W art. 22a ust. 2 pkt 2 poprawiono odwołanie.
17.	Art. 1 pkt 9 – dot. art. 22a ust. 2 pkt 2	Związek Przedsiębiorców i Pracodawców (ZPP)	Projekt wymaga korekty w zakresie błędnego odesłania legislacyjnego W uwagach trafnie wskazano również problem stricte legislacyjny, który nie powinien zostać pominięty. Projektowany art. 22a ust. 2 pkt 2 odwołuje się do ust. 4 pkt 3, który, jak wynika z treści projektu, nie istnieje. Tego rodzaju błąd redakcyjny może prowadzić do niejasności interpretacyjnych i powinien zostać usunięty na etapie dalszych prac legislacyjnych. ZPP postuluje zatem techniczno-legislacyjne skorygowanie tego przepisu, tak aby odesłanie było precyzyjne i nie budziło wątpliwości co do zakresu danych, których może żądać strona ufająca w przypadku niejednoznacznego dopasowania tożsamości	**Uwaga uwzględniona** W art. 22a ust. 2 pkt 2 poprawiono odwołanie.
18.	Art. 1 pkt 9 - dot. art. 22a ust. 2 pkt 2	Izba Gospodarki Elektronicznej	Zakres danych dla AML/KYC i mechanizm udostępniania Projektowany art. 22a ust. 2 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej przewiduje, że system scentralizowany zapewnia w szczególności możliwość żądania przez stronę ufającą od osoby fizycznej podania dodatkowych danych, o których mowa w ust. 4 pkt 3, i przekazania tych danych przez osobę fizyczną celem jednoznacznego dopasowania tożsamości w przypadku, gdy dopasowanie tożsamości jest niejednoznaczne. Z kolei art. 22a ust. 3 pkt 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej stanowi, że w systemie scentralizowanym przetwarzane są dane osobowe obejmujące dane identyfikacyjne osoby, o których mowa w załączniku do rozporządzenia wykonawczego 2015/1501, w przypadku osoby fizycznej posługującej się notyfikowanym środkiem identyfikacji elektronicznej. Przepis odnosi się do	**Uwaga wyjaśniona** Należy zaznaczyć że „dopasowywanie tożsamości" zgodnie z art. 3 pkt 55 rozporządzenia eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Powyższe oznacza, że celem przepisów nie jest ustalenie tożsamości celem wypełnienia obowiązków (AML/KYC) wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ale tylko dopasowanie tożsamości zweryfikowanej za

			załącznika, który przewiduje minimalny zestaw danych osoby fizycznej— obowiązkowych (imię, nazwisko, data urodzenia, PESEL) oraz dodatkowych (imię i nazwisko rodowe, miejsce urodzenia, aktualny adres, płeć). Taki zakres pozostaje jednak niewystarczający dla realizacji obowiązków wynikających z ustawy AML: brak co najmniej serii i numeru dokumentu tożsamości, daty jego ważności oraz miejsca (miasta) i kraju urodzenia. W konsekwencji instytucje obowiązane, w tym instytucje pożyczkowe, nie będą mogły oprzeć onboardingu klientów oraz zawierania umów/procesowania transakcji wyłącznie na danych z portfela tożsamości cyfrowej, co wymusi równoległe, dublujące się procedury weryfikacyjne. Zwracamy także uwagę na błąd redakcyjny w projektowanym art. 22a w zakresie odesłania do „ust. 4 pkt 3”, wymagający korekty, aby nie rodził wątpliwości interpretacyjnych przy dopasowywaniu tożsamości. Ponadto mechanizm selektywnego udostępniania, choć słusznie wzmacnia kontrolę klienta nad prywatnością, w praktyce może prowadzić do przekazywania instytucjom finansowym niekompletnych zestawów informacji, co utrudnia realizację procesów regulowanych. Postulujemy, aby strona ufająca miała uprawnienie do określenia obowiązkowego profilu danych niezbędnych do zawarcia umowy bądź przeprowadzenia transakcji. Użytkownik powinien mieć jasny wybór: albo udostępnia pełen pakiet wymagany przepisami, albo rezygnuje z usługi. Należy wykluczyć możliwość przesyłania częściowo wypełnionych formularzy lub ograniczania zgód w sposób skutkujący niepełnością danych wymaganych prawem.	pomocą środka identyfikacji elektronicznej wydanego w innym kraju UE do tożsamości już wcześniej zweryfikowanej. Należy podkreślić, że zakresy danych wskazane w projekcie ustawy wskazują na dane identyfikujące osobę jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846). Tamże wskazuje się, że odpowiednio należy polegać na danych, o których mowa w rozporządzeniu wykonawczym (UE) 2024/2977 wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi lub zestawie danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. W związku z tym jeżeli dopasowanie jest dokładne i jednoznaczne na podstawie ww. danych wraz zaproponowaną procedurą uzupełniającą dopasowanie uważa się za skuteczne. System dopasowywanie tożsamości co do zasady zgodnie z art. 2 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/846 dotyczy usług online oferowanych przez podmiot sektora publicznego lub w jego imieniu. W przypadku gdy prywatna strona ufająca jest zobowiązana na podstawie art. 5f ust. 2 rozporządzenia eIDAS do akceptacji europejskich portfeli tożsamości cyfrowej i jednocześnie zobowiązana do stosowania przepisów wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, to w zależności od tego czy akceptacja portfela dotyczy już istniejącego konta użytkownika (dla

				którego już stwierdzono komplet wymaganych danych) czy też nowego – procedury powinny być inne. W przypadku konieczności uzyskania dodatkowych danych wykraczających poza zakres danych identyfikujących osobę przewidziany w rozporządzeniu wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977) odpowiednio zakres tych dany powinien zostać wpisany przez taki podmiot do rejestru stron ufających. Kwestią wykraczającą poza możliwości krajowych regulacji jest zgłoszenie przez inne państwa członkowskie atrybutów potwierdzających dodatkowe dane. W zakresie danych nieobjętych (niewymienionych) załącznikiem VI do rozporządzenia eIDAS, nie występuje obowiązek ich zgłaszania. W związku z przepisami dotyczącymi rejestracji w rejestrze stron ufających, w tym wskazywania zakresu danych dla każdej usługi, jak również propozycji polegania na certyfikatach rejestracji strony ufającej portfele tożsamości cyfrowej automatycznie rozpoznają zakres danych jaki jest wymagany dla określonej usługi wskazane zagrożenie nie wydaje się istotne. Użytkownicy z pewności szybko się nauczą możliwości jakie daje im portfel. W art. 22a odesłanie zostało poprawione.
19.	Art. 1 pkt 9 - dot. art. 22b ust. 3 pkt 1 lit. b	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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	**Uwaga wyjaśniona** W odniesieniu do kwestii, czy kwalifikowana pieczęć elektroniczna jest zaawansowaną pieczęcią elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu, to wątpliwości w tej sprawie można wyjaśnić wprost na podstawie definicji art. 3 pkt 27 rozporządzenia eIDAS: „27) "kwalifikowana pieczęć elektroniczna" oznacza zaawansowaną pieczęć elektroniczną, która została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na

			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;	kwalifikowanym certyfikacie pieczęci elektronicznej". Na podstawie tej definicji należy potwierdzić, że każda kwalifikowana pieczęć elektroniczna jest jednocześnie zaawansowaną pieczęcią elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu. Sugerowane dopisanie w ustawie, że przez zaawansowaną pieczęć elektroniczną weryfikowaną kwalifikowanym certyfikatem należy rozumieć również kwalifikowaną pieczęć elektroniczną mogłoby spowodować pojawianie się interpretacji, że gdziekolwiek w innych przepisach mówi się o zaawansowanej pieczęci elektronicznej /zaawansowanym podpisie elektronicznym, a nie zostało tam dopisane, że wymagania takie spełniają również pieczęci/podpisy kwalifikowane, to nie można ich stosować. Jeżeli chodzi o sugerowany dodatkowy wymóg identyfikacji osoby fizycznej dokonującej wpisu, to jego wprowadzenie mogłoby wymusić po stronie rejestratora (ministra właściwego do spraw informatyzacji) konieczność weryfikacji uprawnień tej konkretnej osoby do dokonania wpisu i ostatecznie mogłoby wynikowo wymagać dodatkowego przekazywania pisma upoważniającego te osobę do dokonywania wpisu podpisanego zgodnie z reprezentacją. To z kolei wymusiłoby na rejestratorze konieczność weryfikowania, czy pismo upoważniające podpisały uprawnione osoby. Przedłużyłoby to proces rejestracji, uczyniłoby go bardziej skomplikowanym i kosztownym. Mając na uwadze wytyczną zawartą w art. 5b ust. 2 zdanie pierwsze rozporządzenia eIDAS, że proces rejestracji musi być efektywny kosztowo i proporcjonalny względem zagrożeń zaproponowano rozwiązanie w którym wykorzystywane będzie mogło być narzędzie, które bez żadnych wątpliwości zostało wydane określonej osobie prawnej, gdyż zostały wydane przez kwalifikowanych dostawców usług zaufania, stosujących polityki świadczenia usług zapewniające poprawne rozpoznanie osoby prawnej. Należy ponadto nadmienić, że uzyskanie wpisu do rejestru stron ufających nie będzie wystarczające do

				tego aby świadczyć usługi dla użytkowników europejskiego portfela tożsamości cyfrowej, gdyż w Polsce certyfikaty dostępu strony ufającej portfela będą wydawane wyłącznie przez kwalifikowanych dostawców usług zaufania mających doświadczenie w poprawnym rozpoznaniu osoby prawnej. Dopiero łącznie te dwa elementy (wpis i certyfikat dostępu) umożliwią korzystanie z portfela. Zdaniem projektodawcy spełnia to wymagania efektywnego kosztowo i proporcjonalnego względem zagrożeń procesu. Dlatego też w przypadku skorzystania przez stronę ufającą z możliwości złożenia wniosku za pośrednictwem dostawcy usługi zaufania wydającego certyfikaty dostępu (czyli załatwienia sprawy w jednym miejscu) wymagane jest podpisanie wniosku przez osobę upoważnioną.
20.	Art. 1 pkt 9 - dot. art. 22b ust. 3 pkt 2	IDENTT Sp. z o.o.	Rejestracja w rejestrze. Brak udogodnień polegających na delegacji procesu wpisu podmiotu do rejestru stron ufających. Propozycja zmiany: Dopuszczenie prawnej opcji wnioskowania do Ministerstwa Cyfryzacji o wpis do rejestru stron ufających przez zewnętrznego pośrednika w imieniu zainteresowanego podmiotu.	**Uwaga wyjaśniona** W art. 22b ust. 3 pkt 2 uregulowano możliwość złożenia wniosku przy wsparciu pośrednika.
21.	Art. 1 pkt 9 - dot. art. 22b ust. 8	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga nieuwzględniona** Przyjęcie założenia, że każdy może wskazać w rejestrze pośrednika (w tym osoby fizyczne), na którym będzie polegał bez jakiegokolwiek potwierdzenia/zgody na taki wpis ze strony tego pośrednika, łącznie z wymaganiami, o których mowa w art. 3 ust. 4-6 rozporządzenia 2025/848, może spowodować możliwość przypisywania znanym podmiotom publicznym i prywatnym roli pośredników mimo, że jej nie pełnią, co zostanie uwidocznione w publicznie dostępnym rejestrze. Zdaniem projektodawcy przypisywanie jakiejkolwiek roli innemu podmiotowi, bez jakiegokolwiek zwrotnego działania tego innego podmiotu jest niedopuszczalne. W tym przypadku nie chodzi o to, że wskazany pośrednik może nie realizować w praktyce przypisywanych mu usług, tylko o samą publicznie dostępną informację, że takim pośrednikiem jest.

22.	Art. 1 pkt 9 - dot. art. 22b ust. 13	PWPW S.A.	Projektowane brzmienie art. 22b ust. 13 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej wymaga konsekwentnego uzupełnienia o podmioty kwalifikowane. Zaproponowane aktualnie alternatywnego źródła wydania tych certyfikatów może negatywnie wpłynąć na przejrzyste warunki rozpoznawalności w otoczeniu tych certyfikatów.	**Uwaga wyjaśniona** Kwalifikowani dostawcy usług zaufania mogą wydawać takie certyfikaty na podstawie art. 22b ust. 12.
23.	Art. 1 pkt 9 - dot. art. 22b ust. 15 pkt 1	Polska Izba Ubezpieczeń	Przepis art. 22b ust. 15 pkt 1) nowelizowanej Ustawy o usługach zaufania oraz identyfikacji elektronicznej wskazuje na obowiązek ministra właściwego ds. informatyzacji w zakresie stworzenia „krajowej polityki rejestracji w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej, o której mowa w rozporządzeniu 2025/848". Jednocześnie, w proponowanej ustawie, powyższy obowiązek nie został obarczony żadnym wiążącym terminem. Takiego terminu nie wskazano również w przepisach Rozporządzenia 2025/848. Tym niemiej celem zapewnienia efektywności nowych przepisów należy postulować o jednoznaczne określenie terminu, w którym minister właściwy winien sporządzić powyższą krajową politykę rejestracji. Należy postulować, aby był on odpowiednio krótki, celem zapewnienia jak najszybszej przejrzystości nowych przepisów. Proponujemy redakcję art. 22b ust. 15 – w miejsce: „15. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej:" proponujemy: „15. Minister właściwy do spraw informatyzacji w terminie sześciu miesięcy od opublikowania ustawy, określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej:"	**Uwaga wyjaśniona** Polityka będzie udostępniona w terminie wejścia w życie przepisu odnoszącego się do niej.
24.	Art. 1 pkt 9 - dot. art. 22b, art. 22e, art. 22g	IDENTT Sp. z o.o.	Szerokie i wyłączne kompetencje Ministra Cyfryzacji. Projekt ustawy nadaje ministrowi właściwemu do spraw informatyzacji bardzo szerokie uprawnienia (odpowiada za system dopasowywania tożsamości, rejestry stron ufających, zgłaszanie atrybutów do UE oraz ich wydawanie). Taka koncentracja kompetencji może drastycznie ograniczyć udział i decyzyjność innych publicznych instytucji sektorowych, które dysponują odpowiednią wiedzą merytoryczną w swoich obszarach działania. Propozycja zmiany: Wprowadzenie mechanizmów współpracy międzyresortowej, obowiązku opiniowania przez odpowiednie resorty lub modelu współzarządzania ekosystemem atrybutów.	**Uwaga wyjaśniona** Przyjęcie w projekcie ustawy określonego katalogu kompetencji dedykowanego Ministrowi Cyfryzacji jest podyktowane specyfiką materii stanowiącej przedmiot niniejszej regulacji. Większość wskazanych w uwadze kompetencji ma charakter ściśle techniczny (prowadzenie rejestrów, systemów, zgłaszanie schematów) i nie wymaga merytorycznej współpracy międzyresortowej przy realizacji tych obowiązków. Natomiast w zakresie wydawania elektronicznych poświadczeń atrybutów ta kompetencja jest rozproszona zgodnie z rozporządzeniem eIDAS.
25.	Art. 1 pkt 9 - dot. art. 22d ust. 2 i 3	PWPW S.A.	W projekcie należy wprowadzić regulację umożliwiającą pośrednikom podmiotów prowadzących źródła zaufane (w szczególności, jeżeli są nimi podmioty publiczne) możliwość zgłaszania schematów poświadczeń atrybutów oraz realizacji innych obowiązków realizacyjnych w imieniu podmiotów prowadzących źródła autentyczne. W praktyce obrotu jeden pośrednik może realizować zadania na	**Uwaga wyjaśniona** Zgodnie z art. 1 pkt 9 projektowanego brzmienia 22e ust. 8 schematy elektronicznych poświadczeń atrybutów do katalogu schematów atrybutów zapewnianego przez Komisję Europejską mogą zgłaszać:

			rzecz wielu tej samej kategorii podmiotów. Umożliwienie pośrednikowi realizacji obowiązków wynikających z ustawy przyczyni się do zmniejszenia problemów proceduralnych, szybszego uruchomienia usług oraz odciąży podmioty – w szczególności podmioty publiczne - od dodatkowych obowiązków. Podobne rozwiązanie już dziś funkcjonuje w ustawie w zakresie krajowego schematu identyfikacji elektronicznej oraz rejestracji systemów identyfikacji elektronicznej.	1) podmioty odpowiedzialne za źródła autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014, 2) kwalifikowani dostawcy usług zaufania świadczący usługi wydawania kwalifikowanych poświadczeń atrybutów, 3) dostawcy usług online wpisani do rejestru stron ufających europejskim portfelom tożsamości cyfrowej, o którym mowa art. 22b ust. 1 - w zakresie elektronicznych poświadczeń atrybutów wykorzystujących wpisane do rejestru dane, poświadczenia lub atrybuty, o których mowa w pkt 9 załącznika I do rozporządzenia 2025/848. W ocenie projektodawcy brak przesłanek, by katalog ten dodatkowo rozszerzać. Przepisy w zaproponowanym kształcie nie zabraniają korzystać z eksperckiego wsparcia lub pełnomocników w procesie zgłaszania schematów elektronicznych poświadczeń atrybutów do katalogu KE.
26.	Art. 1 pkt 9 - dot. art. 22f	PWPW S.A.	Wątpliwości budzi zaproponowane w projektowanym brzmieniu art. 22f ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej rozwiązanie, zgodnie z którym wyłącznie minister właściwy do spraw informatyzacji będzie mógł wydawać, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, elektroniczne poświadczenia atrybutów, o których mowa w art. 45f 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, z późn. zm.), zwanego dalej „rozporządzeniem 910/2024”. W ocenie PWPW S.A. możliwość wydawania elektronicznego poświadczania tych atrybutów powinien posiadać każdy podmiot publiczny, który jest odpowiedzialny za źródło autentyczne, w szczególności zaś taką możliwość powinna mieć PWPW S.A. jako wytwórca wyłączny niektórych dokumentów publicznych, o którym mowa w art. 16a ust. 1 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych. Dodatkowo, w ocenie PWPW S.A. zasadne jest powierzenie uprawnienia do wydawania elektronicznych poświadczeń atrybutów podmiotom posiadającym odpowiednie doświadczenie i kompetencje w zakresie świadczenia usług zaufania, w szczególności kwalifikowanym dostawcom usług zaufania. W tym kontekście należy wskazać, że COI oraz minister właściwy do spraw informatyzacji pełnią przede wszystkim funkcję regulacyjną i nadzorczą w obszarze	**Uwaga częściowo uwzględniona** Uzasadnienie nie wymaga zmian w kontekście częściowo uwzględnionej uwagi. Nie jest możliwe powierzenie kwalifikowanym dostawcom możliwości wydawania poświadczeń atrybutów w trybie innym niż to przewidziano w rozporządzeniu eIDAS.

			usług zaufania, natomiast nie posiadają doświadczenia operacyjnego w świadczeniu kwalifikowanych usług zaufania. Doświadczenie to jest natomiast domeną podmiotów takich jak PWPW S.A., które od lat realizują zadania związane z bezpieczeństwem dokumentów publicznych oraz świadczeniem usług zaufania. Powierzenie wydawania elektronicznych poświadczeń atrybutów podmiotom nieposiadającym praktycznego doświadczenia w tym zakresie może rodzić ryzyka dla bezpieczeństwa systemu oraz jakości świadczonych usług. Jednocześnie koncentracja funkcji regulacyjnych, nadzorczych i operacyjnych w ramach jednego podmiotu (ministra właściwego do spraw informatyzacji) prowadzi do ryzyka konfliktu interesów oraz osłabienia przejrzystości systemu. PWPW S.A., jako podmiot o szczególnej roli w systemie bezpieczeństwa państwa oraz wytwórca dokumentów publicznych, posiada unikatowe kompetencje technologiczne, organizacyjne oraz doświadczenie w zakresie przetwarzania danych wrażliwych i zapewnienia wysokiego poziomu bezpieczeństwa. Okoliczności te uzasadniają powierzenie temu podmiotowi uprawnień w zakresie wydawania elektronicznych poświadczeń atrybutów, w szczególności w odniesieniu do danych powiązanych z dokumentami publicznymi. Dodatkowo wskazujemy na potrzebę uwzględnienia skutków finansowych ww. rozwiązania w OSR do projektu ustawy. Propozycja brzmienia przepisu 1) w celu realizacji uwagi projektowanemu brzmieniu art. 22f ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej PWPW S.A. proponuje nadać brzmienie: „Art. 22f. 1. Podmiot publiczny odpowiedzialny za źródło autentyczne może samodzielnie lub za pośrednictwem innego podmiotu zapewniającego system teleinformatyczny, w którym utrzymywane jest źródło autentyczne, wydawać elektroniczne poświadczenie atrybutów, o których mowa w art. 45f rozporządzenia 910/2014. 2.Podmiot publiczny będący emitentem dokumentów publicznych w rozumieniu art. 2 ust. 1 pkt 3 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881) może wydawać elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014,w oparciu o dane zawarte w dokumencie publicznym lub powierzać wydawanie tych poświadczeń innym podmiotom zapewniającym systemy teleinformatyczne, za pomocą których wytwarzane są blankiety dokumentów publicznych lub dokonywana jest ich indywidualizacja lub personalizacja.”. 2) w konsekwencji uwzględnienia tej uwagi w projekcie ustawy: a) w projektowanym brzmieniu art. 1 pkt 11 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej należy skreślić wyrazy „w	

			imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne”, b) do przepisu nowelizującego ustawę z dnia 22 listopada 2018 r. o dokumentach publicznych (vide uwaga z poz. 2) dodać nowelizację art. 17 tej ustawy, polegającą na dodaniu ust. 1a i 1b w brzmieniu: „1a. Prawo wyłączne obejmuje także wydawanie elektronicznych poświadczeń atrybutów, w tym elektronicznych poświadczeniach atrybutów przechowywanych i udostępnianych w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, związanych z danymi, które mają być zawarte w wytwarzanych, indywidualizowanych lub personalizowanych blankietach dokumentów publicznych, o których mowa art. 5 ust. 2 pkt 16, 17, 19 i 32 lit. a-e, g, h oraz m, lub w wytwarzanych, indywidualizowanych lub personalizowanych blankietach dokumentów publicznych określonych w przepisach wydanych na podstawie art. 16a ust. 2. 1b. Wytwórca wyłączny uzgadnia schemat wydawania elektronicznych poświadczeń atrybutów, o których mowa w ust. 1a, z właściwym ze względu na rodzaj atrybutów ministrem.”.	
27.	Art. 1 pkt 9 - dot. art. 22f, art. 22g, art. 22h	IDENTT Sp. z o.o.	Przepisy art. 22f oraz art. 22g w obecnym brzmieniu prowadzą do koncentracji kluczowych kompetencji w zakresie wydawania elektronicznych poświadczeń atrybutów po stronie ministra właściwego ds. informatyzacji. Wpływa to na to zmniejszenie konkurencyjności rynku, ograniczając możliwość świadczenia tych usług przez inne podmioty publiczne oraz podmioty rynkowe, w tym dostawców usług zaufania. Dodatkowo, w powiązaniu z art. 22h, powstaje ryzyko wydawania poświadczeń atrybutów w modelu, który nie jest jednoznacznie osadzony w reżimie usług zaufania. Może to prowadzić do ograniczenia interoperacyjności tych poświadczeń oraz ich rozpoznawalności na poziomie europejskim, w szczególności w kontekście wymogów eIDAS 2.0 oraz konieczności zapewnienia ich weryfikowalności poprzez infrastrukturę zaufania (np. listy zaufania). Propozycja zmiany: Zapewnienie otwartego modelu dopuszczania podmiotów do świadczenia usług wydawania poświadczeń atrybutów (w tym dostawców usług zaufania),oraz rozdzielenie funkcji nadzorczych i operacyjnych. Umożliwienie wydawania poświadczeń atrybutów przez podmioty publiczne odpowiedzialne za źródła autentyczne oraz podmioty działające w ich imieniu. Jednoznaczne osadzenie wydawania poświadczeń atrybutów w ramach ekosystemu usług zaufania, w tym powiązanie z krajową i europejską infrastrukturą zaufania, Usunięcie art. 22h	**Uwaga uwzględniona/ wyjaśniona** W celu wyeliminowania wątpliwości, czy skoro rozporządzenie eIDAS obowiązuje bezpośrednio, to znaczy, że oprócz kwalifikowanych dostawców usług zaufania elektroniczne poświadczenia atrybutów mogą być również wydawane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne (jako niekwalifikowana usługa zaufania) pod warunkiem spełnienia przez taki podmiot wymagań, o których mowa w art. 45f rozporządzenia eIDAS, to w związku z uwagą zmodyfikowany został art. 22f, aby obowiązek uzyskania przez taki podmiot wpisu do rejestru dostawców usług zaufania był oczywisty oraz wskazując, w jaki sposób taki dostawca ma potwierdzić wymaganie, o którym mowa w art. 45f ust. 2 rozporządzenia eIDAS. Ponadto, dla zapewnienia zgodności elektronicznych poświadczeń atrybutów ze standardami unijnymi dodano przepisy o krajowym katalogu schematów elektronicznych poświadczeń atrybutów. W zakresie rozdzielenia funkcji operacyjnych i nadzorczych zgodnie z proponowanym przepisami ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz ustawy o aplikacji mObywatel zadania ministra właściwego do spraw informatyzacji w

				zakresie dostawcy usług nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra, która sprawuje nadzór.
28.	Art. 1 pkt 9 - dot. art. 22g	PWPW S.A.	Należy wyraźnie wskazać, że zrównanie skutku prawnego atrybutu z dokumentem publicznym możliwe jest wyłącznie pod warunkiem ważności dokumentu publicznego w okresie ważności atrybutu. Należy także wprowadzić mechanizm ujawniania i weryfikacji ważności tego rodzaju atrybutów z ważnością dokumentów publicznych. Dodatkowo wskazujemy na potrzebę usunięcia dokumentu mobilnego z przepisu art. 22g ustawy o usługach zaufania. Obecnie dokument mobilny nie posiada mocy prawnej równej dokumentowi publicznemu i taka zasada powinna zostać podtrzymana (mtożsamości, wybrane legitymacje np. uczniowska itp.). Wprowadzenie jednak ogólnej zasady uznawania mdokumentów za równoważne dokumentom publicznym nie znajduje uzasadnienia, nie jest spójne z całym system prawa (nie wynika także z eIDAS 2.0) oraz potencjalnie jest niebezpieczne dla obrotu prawnego. Dodatkowo mdokumenty nie będą pochodziły z europejskiego portfela tożsamości a z aplikacji mObywatel (która ma nadal działać niezależnie od portfela). W przeciwieństwie do portfela aplikacja mObywatel nie została uwierzytelniona na poziomie wysokim. Dlatego dla bezpieczeństwa obrotu i zgodnie z rozporządzeniem eIDAS należy wprowadzić regulacje wyłącznie powiązaną z elektronicznymi poświadczeniami atrybutów pochodzącymi z europejskiego portfela tożsamości cyfrowej. W projektowanym art. 22g ustawy o usługach zaufania: 1) ust. 3 powinien otrzymać brzmienie: „3. Elektroniczne poświadczenie atrybutów, o którym mowa w ust. 1, wywołuje taki sam skutek prawny jak dokument wydany na podstawie przepisów prawa powszechnie obowiązującego potwierdzający dany stan prawny lub uprawnienia osób posługujących się nim, w tym dokument publiczny w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881), lub zaświadczenie w rozumieniu ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego. lub dokument mobilny w rozumieniu ustawy dnia 26 maja 2023 r. o aplikacji mObywatel.”; 2) należy dodać ust. 4 w brzmieniu: „4. Elektroniczne poświadczenie atrybutów, o którym mowa w ust. 1, zawierające zestaw danych tożsamy z danym zawartymi w dokumencie publicznym w rozumieniu ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669 i 1863 oraz z 2025 r. poz. 1881) wywołuje skutek, o którym mowa w ust. 1, pod warunkiem ważności tego dokumentu publicznego.”.	**Uwaga wyjaśniona** Dokumenty publiczne nie są i nie były również wcześniej przedmiotem 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 (rozporządzenie eIDAS). Ostatnie zmiany wprowadzone do rozporządzenia eIDAS rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ustanowiły między innymi europejski portfel tożsamości cyfrowej i nową usługę zaufania jaką jest wydawanie elektronicznych poświadczeń atrybutów. Zarówno europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów, zostały nie tylko zdefiniowane w rozporządzeniu eIDAS, aktach wykonawczych do tego rozporządzenia, ale również precyzyjnie opisano wymagania organizacyjne i techniczne wobec tych narzędzi wskazując na właściwe normy Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI). Z pewnością zatem europejski portfel tożsamości cyfrowej, jak również elektroniczne poświadczenia atrybutów, nie są dokumentami publicznymi w rozumieniu ustawy o dokumentach publicznych, jak również należą do odrębnego niezależnego reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim. Moc wiążąca dokumentów mobilnych wynika z ustawy o aplikacji mObywatel oraz dodatkowo z poszczególnych przepisów dziedzinowych. W ocenie projektodawcy zasadnym jest więc odniesienie w przedmiotowym przepisie również do dokumentu mobilnego.
29.	Art. 1 pkt 9 - dot. art. 22g	PWPW S.A.	Z uwagi na rolę MC jako organu nadzoru nad usługami zaufania proponujemy usunąć natomiast projektowane brzmienie art. 22g ustawy o usługach zaufania, tj.	**Uwaga wyjaśniona** Zgodnie z proponowanym przepisami ustawy o usługach

			nadawanie uprawnienia MC do wydawania elektronicznych poświadczeń atrybutów. MC jako dostawca portfela oraz nadzorca nie powinien łączyć tych funkcji. Rozłączenie tej roli jest także zasadne z uwagi na konieczność oddzielenia roli wytwórcy od roli związanej z bezpieczeństwem. Wydawanie poświadczeń atrybutów jako usługa zaufania powinna być realizowana przez dostawców usług zaufania, w szczególności kwalifikowanych dostawców usług zaufania, którzy zgodnie z eIDAS mogą także wydawać poświadczenia niekwalifikowane. Dlatego proponujemy nowy mechanizm wskazany w uwadze poniżej (dotyczącej nowego brzmienia przepisu art. 22g ustawy o usługach zaufania).	zaufania oraz identyfikacji elektronicznej oraz ustawy o aplikacji mObywatel zadania ministra właściwego do spraw informatyzacji w zakresie dostawcy usług nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra, która sprawuje nadzór.
30.	Art. 1 pkt 9 - dot. art. 22g	PWPW S.A.	W projekcie ustawy pominięto obszar związany z funkcjonowaniem niekwalifikowanych poświadczeń atrybutów. Atrybuty niekwalifikowane mogą pełnić istotną rolę w obrocie krajowym i ustawa powinna zawierać zasady tworzenia, zgłaszania schematów oraz zarzadzania elektronicznymi atrybutami. Dodatkowo postulujemy wprowadzenie przepisów zapewniających utworzenie krajowego mechanizmu (np. repozytorium) zawierającego informacje o atrybutach i schematach atrybutów o znaczeniu krajowym. Proponowane brzmienie art. 22g ustawy o usługach zaufania: „Art. 22g. 1. Podmioty wydające elektroniczne poświadczenia atrybutów w rozumieniu art. 3 pkt 44 rozporządzenia 910/2014, podmioty wydające elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub podmioty działające w ich imieniu, lub kwalifikowani dostawcy usług zaufania mogą tworzyć schematy elektronicznych poświadczeń atrybutów w rozumieniu art. 3 pkt 44 rozporządzenia 910/2014 w formacie danych określonym w rozporządzeniu wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. Urz. UE L z 2024/2979 z 4.12.2024 r.) i wydawać je użytkownikowi europejskiego portfela tożsamości cyfrowej. 2. Minister właściwy do spraw informatyzacji określi i udostępni na stronie podmiotowej Biuletynu Informacji Publicznej ministra właściwego do spraw informatyzacji: 1) w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz ministrem do spraw transportu wzorcowy schemat elektronicznych poświadczeń atrybutów; 2) wymagania dla wydawania, przechowywania i udostępniania elektronicznych poświadczeń z europejskim portfelem tożsamości cyfrowej; 3) struktury danych, okres ważności i zasady ich unieważniania; 4) rodzaj wymaganej pieczęci elektronicznej niezbędnej do opatrzenia elektronicznego poświadczenia.”.	**Uwaga częściowo uwzględniona** W ustawie o usługach zaufania oraz identyfikacji elektronicznej dodane zostały przepisy dotyczące funkcjonowania krajowego katalogu schematów elektronicznych poświadczeń atrybutów.

31.	Art. 1 pkt 9 - dot. art. 22h	PWPW S.A.	Jeżeli ustawodawca przewiduje możliwość wydawania elektronicznych poświadczeń atrybutów innych niż podmiotów publicznych i kwalifikowanych (co postuluje się także powyżej), które mają być udostępniane w europejskim portfelu tożsamości, należy dodać przepisy związane z samym bezpieczeństwem takich systemów (a nie tylko samych schematów). Proponowane brzmienie art. 22h ustawy o usługach zaufania: „Art. 22h. 1. Wydawca elektronicznego poświadczenia atrybutów: 1) stosuje metody ustalania źródła pochodzenia i autentyczności danych; 2) jeżeli jest to zasadne, mając na uwadze charakter atrybutu lub jego zastosowanie w obrocie prawnym, stosuje mechanizmy zapewniające aktualność danych lub deklarowany czas aktualności danych oraz wynikających z nich uprawnień niezwłocznie, nie później niż w terminie dwóch dni od daty wystąpienia zdarzenia wymagającego aktualizacji danych lub wynikających z tych danych uprawnień; 3) stosuje mechanizmy zapewniające integralność danych zawartych w atrybucie i jej nienaruszalności w czasie ważności atrybutu; 4) zapewnia, że środowisko teleinformatyczne, w którym jest prowadzone źródło autentyczne, zapewnia bezpieczeństwo systemów teleinformatycznych. 2. Wydawca, o którym mowa w ust. 1, opracowuje dokumentację zawierającą: 1) podstawy prawne do wydania elektronicznego poświadczenia atrybutu; 2) opis kluczowych elementów weryfikacji atrybutu; 3) zakres terytorialny, na którym będzie obowiązywał cyfrowy dokument publiczny; 4) wskazanie danych pochodzących ze źródła autentycznego, w którym jest prowadzone źródło autentyczne, w szczególności: a) zastosowane technologie zabezpieczeń, w tym zabezpieczeń kryptograficznych, b) wskazanie weryfikacji integralności, wskazanie zasad potwierdzania pochodzenia i integralności danych zawartych w źródle autentycznym, c) opis zastosowanych testów bezpieczeństwa oraz ich wynik, d) wykaz zmian wynikających z przeprowadzonych testów bezpieczeństwa, e) wysokopoziomową architekturę środowiska programistycznego i stosowanych interfejsów programistycznych, f) wskazanie podmiotu utrzymującego system teleinformatyczny. 3. Wydawca, o którym mowa w ust. 1, przekazuje informacje, o których mowa w ust. 2, ministrowi właściwemu do spraw informatyzacji wraz ze zgłoszeniem schematu elektronicznego poświadczenia atrybutu. Wystawca przechowuje dokumentacje, o której mowa w ust. 2, przez okres 5 lat od dnia jej ostatniej modyfikacji.”.	**Uwaga wyjaśniona** W ustawie o usługach zaufania oraz identyfikacji elektronicznej dodane zostały przepisy dotyczące funkcjonowania krajowego katalogu schematów elektronicznych poświadczeń atrybutów.

32.	Art. 2 ust. 1 pkt 3	NACZELNA IZBA PIELĘGNIAREK I POŁOŻNYCH	W projekcie zmian w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2025 r. poz. 1703 z późn. zm.) – dalej: „ustawa o informatyzacji”, przewidziano możliwość wystąpienia ewentualnych zobowiązań i kosztów po stronie podmiotów realizujących zadania publiczne. Norma art. 2 ust. 1 pkt 3 ww. ustawy na mocy art. 1 pkt 3) lit. a) ustawy z dnia 25 lipca 2025 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz. U. z 2025 r. poz. 1158), rozszerza zakres podmiotowy stosowania ww. ustawy o informatyzacji. W związku z powyższym ponawiam poniższe uwagi skierowane do Szefa Kancelarii Sejmu w dniu 16 lipca 2025 r. w piśmie znak NIPiP-NRPIP-DM 0023.77.2.2025.AA w ramach opiniowania projektu ustawy, na które nie otrzymano odpowiedzi do dnia dzisiejszego. W związku z wątpliwościami czy podmiotem obowiązków do którego kierowany jest projekt jest także samorząd zawodowy, prosimy o udzielenie odpowiedzi: czy w świetle treści art. 2 ust. 1 pkt 3 ustawy o informatyzacji samorządy zawodowe są włączone w jego reżim prawny? w przypadku odpowiedzi twierdzącej na pytanie 1, 2 na jakich zasadach planowane jest pokrycie samorządowi zawodowemu kosztów wdrożenia i utrzymania zmian przewidzianych w projekcie? Zgodnie z obowiązującymi przepisami, w szczególności z art. 2 ust. 4 ustawy z dnia 1 lipca 2011 r. o samorządzie pielęgniarek i położnych (t.j. Dz. U. z 2025 r. poz. 1760) – dalej: „ustawa o samorządzie”, Naczelna Izba Pielęgniarek i Położnych oraz okręgowe izby pielęgniarek i położnych są jednostkami organizacyjnymi samorządu posiadającymi osobowość prawną. Samorząd ten, z mocy ustawy, realizuje zadania publiczne, do których należy przede wszystkim sprawowanie pieczy nad należytym wykonywaniem zawodów pielęgniarki i położnej w granicach interesu publicznego i dla jego ochrony (art. 2 ust. 1 ustawy) tj. m.in. prowadzenie rejestrów pielęgniarek i położnych, które warunkują prawo wykonywania zawodu. Art. 2 ust. 1 pkt 3 wprowadza do ustawy o informatyzacji nową, szerszą definicję „podmiotu publicznego”, która za podmiot publiczny uznaje „inne niż określone w pkt 1 osoby prawne utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego”. Gdyby uznać, że w świetle zmian zarówno Naczelna Izba, jak i okręgowe izby pielęgniarek i położnych są objęte pełnym zakresem podmiotowym projektu, status ten rodzi fundamentalne konsekwencje dla całokształtu funkcjonowania samorządu stanowiące ograniczenie jego ustawowej niezależności. Fundamentalną zasadą ustrojową samorządu zawodowego, wyrażoną w art. 2 ust. 2 ustawy o samorządzie jest jego niezależność w wykonywaniu swoich zadań i podleganie wyłącznie przepisom prawa. Oznacza to autonomię w realizacji jego	**Uwaga wyjaśniona** Przedstawiony do niniejszych konsultacji projekt o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122) nie zmienia art. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Celem projektu jest wyłącznie dostosowanie polskiego porządku prawnego do zmian, jakie zostały wprowadzone do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 (rozporządzenie eIDAS) przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183. Rozporządzenie eIDAS posługuje się terminem zdefiniowanym w art. 3 pkt 7 w brzmieniu: „podmiot sektora publicznego" oznacza organ państwowy, regionalny lub lokalny, podmiot prawa publicznego lub stowarzyszenie utworzone przez jeden lub kilka takich organów lub jeden lub kilka takich podmiotów prawa publicznego, lub jednostkę prywatną, której co najmniej jeden z tych organów, podmiotów lub jedno z takich stowarzyszeń udzieliły upoważnienia do świadczenia usług publicznych, gdy działa ona na podstawie takiego upoważnienia; Rozporządzenie eIDAS stosuje się wprost, co znaczy, że wymogi nałożone na podmioty sektora publicznego w ww. rozumieniu nie wynikają z art. 2 ust. 1 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne.

			misji i zadań, bez nieuprawnionej ingerencji organów państwa. Choć przepis nie ingeruje bezpośrednio w merytoryczne kompetencje samorządu, takie jak treść zasad etyki zawodowej czy procedury odpowiedzialności zawodowej, w sposób istotny ograniczy jego faktyczną niezależność. Ograniczenie to przybierze formę zależności technologicznej i proceduralnej od administracji rządowej. Poprzez nałożenie obowiązku stosowania się do centralnie zdefiniowanych standardów technicznych (Architektura Informacyjna Państwa), sformalizowanych procedur (oceny interoperacyjności) i narzuconych narzędzi (Repozytorium Interoperacyjności, System Inwentaryzacji Systemów Teleinformatycznych), administracja państwowa wkracza w sferę autonomii operacyjnej i organizacyjnej samorządu. Aby móc legalnie i sprawnie prowadzić rejestr czy zarządzać swoimi systemami informatycznymi, samorząd będzie musiał uzyskać i utrzymywać zgodność z ramami technicznymi definiowanymi przez organ administracji rządowej – ministra właściwego do spraw informatyzacji. W ten sposób, pod pozorem technicznej modernizacji, tworzy się nowa, silna forma zależności samorządu od władzy wykonawczej. Włączenie samorządu zawodowego pielęgniarek i położnych w reżim prawny ustawy o informatyzacji nakłada na okręgowe izby oraz Naczelną Izbę szereg nowych, skomplikowanych i kosztownych obowiązków o charakterze technicznym, administracyjnym i sprawozdawczym. Zmiany dotkną kluczowego zadania samorządu, jakim jest prowadzenie okręgowych rejestrów pielęgniarek i położnych, które w świetle nowych przepisów stają się „rejestrami publicznymi". Wprowadzany przez art. 14 ustawy o informatyzacji przepis nakłada na podmiot prowadzący rejestr publiczny zawierający dane osób fizycznych obowiązek dokonywania uprzedniej weryfikacji danych wprowadzanych po raz pierwszy do tego rejestru pod względem zgodności z danymi zgromadzonymi w rejestrze PESEL. Stanowi to istotną zmianę w procesie stwierdzania i przyznawania prawa wykonywania zawodu oraz wpisu do rejestru. Realizacja tego obowiązku będzie wymagała budowy bezpiecznego, zautomatyzowanego połączenia (interfejsu) między systemem informatycznym izby a system centralnym PESEL. Każda rozbieżność danych (np. inna pisownia nazwiska, inny adres) będzie musiała być wyjaśniana przed dokonaniem wpisu, co może znacząco wydłużyć i skomplikować proces rejestracji nowych członków samorządu. Zmiany nakładają wymóg zgodności wszystkich systemów teleinformatycznych używanych przez podmiot publiczny z pryncypiami, standardami, wytycznymi i rekomendacjami Architektury Informacyjnej Państwa. Oznaczałoby to konieczność przeprowadzenia audytu istniejących systemów izb, a następnie ich kosztownej	

			modernizacji lub nawet całkowitej wymiany, jeśli nie będą one spełniać centralnie narzuconych standardów architektonicznych. Jest to proces ciągłej adaptacji, a nie jednorazowe działanie. Norma art. 13 ust. 5 ustawy o informatyzacji zobowiązuje do opracowania i zapewnienia aktualności szczegółowej dokumentacji interfejsu programistycznego aplikacji (API) dla systemów izby. Jest to zadanie, które wymaga albo zatrudnienia programistów, albo zlecenia zewnętrznym, wyspecjalizowanym firmom stworzenia i stałego utrzymywania API, co generuje wysokie i trwałe koszty. Implementacja wyżej wymienionych obowiązków wiąże się z ogromnymi kosztami. Należy tu wymienić koszty inwestycyjne (budowa interfejsów, modernizacja lub wymiana systemów), koszty stałe (utrzymanie API, opłaty licencyjne, koszty personelu IT) oraz koszty administracyjne (czas pracy pracowników oddelegowanych do sprawozdawczości, przeprowadzania ocen interoperacyjności, udziału w inwentaryzacji). Dodatkowo, w uzasadnieniu przedmiotowego projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122) zwrócono uwagę na możliwość wystąpienia konieczności bezpośredniej integracji z europejskim portfelem tożsamości cyfrowej wymagającej od podmiotu publicznego wpisania się do rejestru stron ufających, uzyskania certyfikatu dostępu strony ufającej portfela oraz certyfikatu rejestracji strony ufającej portfela, jak również dostosowania systemu teleinformatycznego do formatów danych przewidzianych dla komunikacji z portfelem (innych niż format danych przekazywany z węzła krajowego identyfikacji elektronicznej). Powyższe zmiany mogą więc również wiązać się w przyszłości z koniecznością zapewnienia odpowiednich środków i kosztów po stronie izby przy założeniu stosowania do niej wskazanych przepisów. Należy z całą mocą podkreślić, że w Ocenie Skutków Regulacji dołączonej do projektu nie przewidziano żadnych dedykowanych środków finansowych dla samorządów zawodowych na realizację tych zadań. Ustawodawca nakłada na podmioty powołane do realizacji zadań ustawowych dodatkowe zadania publiczne właściwe dla obowiązków podmiotów administracji państwowej. Obowiązki te w coraz szerszym zakresie nie są finansowane ze środków publicznych, lecz ze środków prywatnych lub jak w przypadku naszego samorządu środowiska pielęgniarek i położnych, jednocześnie ograniczana jest ich niezależność w działaniach przewidzianych ustawowo. Kierunek takich zmian, sprzeczny z zapisami Konstytucji RP oraz ustrojem prawnym samorządów zawodowych, budzi poważne zaniepokojenie w ustroju demokratycznym. Działalność samorządu pielęgniarek i położnych finansowana jest ze składek jego członków. Koszty implementacji projektu zostaną w całości przeniesione na	

			członków samorządu poprzez konieczność podwyższenia składek członkowskich lub drastyczne cięcia w innych, kluczowych obszarach działalności statutowej. Projekt reprezentuje klasyczny przykład nałożenia na podmioty nie będące organami administracji nowych zadań bezpodstawnie niefinansowanych z budżetu państwowego. Należy jednak pamiętać, iż kwestia poprawy tego budżetu nie należy do samorządów zawodowych i nie ich zadaniem jest finansowanie zadań administracji.	
33.	Art. 4 pkt 4 lit. d	PWPW S.A.	W celu zwiększenia bezpieczeństwa posługiwania się profilem zaufanym w obrocie prawnym, PWPW S.A. proponuje wprowadzenie rozwiązań zmierzających do wykorzystania w punktach potwierdzających ten profil weryfikacji biometrycznej użytkownika poprzez porównanie cech biometrycznych twarzy osoby dokonującej takiego potwierdzenia z wizerunkiem twarzy utrwalonym na fotografii tej osoby w dokumencie tożsamości. W celu realizacji powyższej uwagi projektowane brzmienie art. 20ad ust. 2a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oznaczyć jako ust. 2e i dodać ust. 2a-2d w brzmieniu: „2a. W procedurze potwierdzania profilu zaufanego osoby fizycznej dokonywanej przez punkt potwierdzający profil zaufany dokonuje się weryfikacji biometrycznej wizerunku osoby obiegającej się o potwierdzenie profilu zaufanego. 2b. Weryfikacja, o której mowa w ust. 2a, polega na potwierdzeniu zgodności zdjęcia zawartego w dokumencie tożsamości z danymi biometrycznymi osoby ubiegającej się o potwierdzenie profilu zaufanego. 2c. Dane biometryczne uzyskane w trakcie weryfikacji, o której mowa w ust. 2a, nie podlegają utrwaleniu i są przetwarzane wyłącznie przez okres przeprowadzenia procedury weryfikacji. 2d. Punkt potwierdzający profil zaufany potwierdza pozytywny wynik weryfikacji, o której mowa w ust. 2a, w Publicznym Systemie Identyfikacji Elektronicznej.”.	**Uwaga nieuwzględniona / wyjaśniona** Nie ma takich wymogów dla średniego poziomu bezpieczeństwa zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 7, z późn. zm.). Ponadto uwaga wykracza poza zakres przedmiotowy projektu.
34.	Art. 4 pkt 5	PWPW S.A.	PWPW S.A. proponuje uzupełnić projekt ustawy o przepisy umożliwiające wykorzystywanie kwalifikowanych pieczęci elektronicznych przez podmioty publiczne. Pieczęć elektroniczna jest coraz częściej wykorzystywana w obrocie, dlatego zasadne jest doprecyzowanie zasad wykorzystywania przez podmioty publiczne kwalifikowanych pieczęci elektronicznych. Doprecyzowanie to powinno wskazywać na krąg podmiotów uprawnionych do wykorzystywania tych pieczęci oraz zakresu ich wykorzystania. Motyw 24 rozporządzenia 910/2014 wskazuje, że państwa członkowskie mogą utrzymać lub wprowadzić przepisy krajowe, zgodne z prawem unijnym, odnoszące się do usług zaufania, o ile usługi te nie są w pełni zharmonizowane w drodze tego rozporządzenia, zaś usługi zaufania spełniające wymogi tego rozporządzenia powinny podlegać swobodnemu obrotowi na rynku wewnętrznym. Zgodnie z poglądami doktryny (Zaccaria A., Schmidt-Kessel M.,	**Uwaga nieuwzględniona** Uwaga wykracza poza zakres przedmiotowy projektu.

			Schulze R., Gambino AM. (edit.), EU eIDAS Regulation. Comentary, Wyd. Beck, Hart, Nowmos, Monachium 2020 s. 218 punkty 13/14 i powołana tam literatura) prawo krajowe może wskazywać szerszy zakres wykorzystania pieczęci niż tylko potwierdzenie źródła pochodzenia danych i integralności danych. Uwzględniając powyższe stanowisko doktryny, jak również dążąc do zachowania spójności z art. 14 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego oraz art. 26 ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, PWPW S.A. proponuje uzupełnić projekt ustawy o dodanie przepisu art. 20af do ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. W art. 4 dodać pkt 5 w brzmieniu: „5) po art. 20ae dodaje się art. 20af w brzmieniu: „Art. 20af. 1. Podmioty publiczne niezależnie od ich formy prawnej mogą do realizacji zadań publicznych, w tym wydawania aktów administracyjnych, stosować kwalifikowaną pieczęć elektroniczną. 2. Jeżeli z przepisu prawa wynika obowiązek opatrzenia dokumentu elektronicznego podpisem elektronicznym, obowiązek ten uznaje się za spełniony w przypadku opatrzenia dokumentu przez podmiot publiczny kwalifikowaną pieczęcią elektroniczną. 3. Przepisu ust. 1 i 2 nie stosuje się do składania oświadczeń woli w formie elektronicznej w rozumieniu art. 781 1 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2025 r. poz. 1071, 1172 i 1508 oraz z 2026 r. poz. 184).”.”.	
35.	Art. 5	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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,	**Uwaga wyjaśniona** Uwaga wykracza poza zakres przedmiotowy projektu. Uwaga nie dotyczy bezpośrednio KPP. Natomiast dotyczy funkcjonowania doręczeń elektronicznych.

			zamiast opierać się na nadzorowanym, interoperacyjnym i opartym na wielu dostawcach ekosystemie usług zaufania.	
36.	Art. 5 pkt 1	Krajowa Izba Rozliczeniowa	Potrzeba doprecyzowania pojęcia „podmiot niepubliczny realizujący zadania publiczne” W ustawie o doręczeniach elektronicznych proponuje się w art. 2 po pkt 6 dodanie pkt 6a w brzmieniu: 6a) podmiot niepubliczny realizujący zadania publiczne – podmiot niepubliczny niebędący osobą fizyczną, realizujący lub wspierający świadczenie tych zadań na podstawie odrębnych przepisów albo na podstawie powierzenia lub zlecenia tego zadania;”; Proponujemy doprecyzowanie definicji, mając na uwadze rolę i obowiązki takiego podmiotu. Wyjaśnienia wymaga zakres pojęciowy tej definicji, w szczególności w odniesieniu do powierzenia i zlecenia zadań, ale także sprecyzowanie, co oznacza wspieranie świadczenia zadań, gdyż już samo ich wspieranie kwalifikuje dany podmiot do kategorii podmiotu niepublicznego realizującego zadania publiczne.	**Uwaga wyjaśniona** Proponowana w przepisie definicja wyraźnie wskazuje, że chodzi tylko o takie podmioty, które „realizują lub wspierają świadczenie zadań publicznych na podstawie odrębnych przepisów albo na podstawie powierzenia lub zlecenia tego zadania”. Zatem samo wspieranie zadań publicznych nie kwalifikuje podmiotu do kategorii podmiotu niepublicznego realizującego zadania publiczne. Wsparcie podmiotu publicznego w realizacji zadania publicznego musi zatem wynikać z odrębnych przepisów albo na podstawie powierzenia lub zlecenia. Jako przykład można wskazać art. 5 ust. 4 pkt 1 ustawy o działalności pożytku publicznego i wolontariacie.
37.	Art. 5 pkt 1	Poczta Polska S.A.	W art. 2 dodano pkt 6a w brzmieniu: „6a) podmiot niepubliczny realizujący zadania publiczne – podmiot niepubliczny niebędący osobą fizyczną, realizujący lub wspierający świadczenie tych zadań na podstawie odrębnych przepisów albo na podstawie powierzenia lub zlecenia tego zadania; Wnosimy o rozważenie zasadności wprowadzenia tej kategorii podmiotów oraz nie wprowadzanie przepisu o zwolnienia z opłat korespondencji przekazywanej przy użyciu PURDE pomiędzy tymi podmiotami oraz podmiotami publicznymi. Przepisy te generują negatywne skutki finansowe dla operatora wyznaczonego i godzą w demokratyczne państwo prawa. Ponadto, należałoby również wskazać oznaczenie takiego podmiotu w BAE w celu właściwego przypisania dostępnych usług i prowadzenia rozliczeń za nadane przesyłki. Zmiana wymaga doprecyzowania w celu określenia wpływu na inne systemy uczestniczące w procesie w tym Systemu OW i integracje z systemami innych podmiotów zintegrowanych z Systemem OW, w tym systemy klasy EZD. W ramach obecnego rozwiązania wszystkie podmioty posiadające ADE w BAE mają przypisany odpowiedni atrybut oznaczający do jakiej grupy podmiotów należą, np. podmiot publiczny/zawód zaufania/komornik – korzystając z tego atrybutu podczas realizacji procesu zakładania SD dla danego podmiotu Operator Wyznaczony wie jaki typ SD i z jakimi dostępnymi usługami dla danego ADE ma założyć. Dla wprowadzanej nowej grupy podmiotów obsługiwanych przez OW na zasadach analogicznych jak podmioty publiczne niezbędne jest przypisanie odpowiednich atrybutów korzystając z już istniejących lub utworzenie nowych co wymaga zmian w API.	**Uwaga nieuwzględniona** Uwaga wykracza poza zakres przedmiotowego projektu ustawy. Uwaga nie dotyczy bezpośrednio KPP. Natomiast dotyczy funkcjonowania doręczeń elektronicznych.

			Wprowadzenie nowego atrybutu dla tego typów podmiotów wymaga analizy koniecznych zmian zarówno po stronie Systemu OW jak i innych interesariuszy. Analizy wymaga również podejście do podmiotów, które obecnie mają ADE jako podmiot niepubliczny a będą zobowiązane do posiadania ADE również jako podmiot publiczny. Po ustaleniu szczegółowego podejścia do proponowanych zmian i rozwiązania technicznego możliwe będzie oszacowanie wpływu na System OW oraz czasu i kosztów implementacji proponowanych zmian.	
38.	Art. 5 pkt 1	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga nieuwzględniona** Uwaga wykracza poza zakres przedmiotowego projektu ustawy. Uwaga nie dotyczy bezpośrednio KPP. Natomiast dotyczy funkcjonowania doręczeń elektronicznych.
39.	Art. 5 pkt 2	Poczta Polska S.A.	Katalog Podmiotów Publicznych Termin wejścia w życie zmiany musi być oszacowany po analizie wpływu na systemy teleinformatyczne uczestniczące w procesie, w tym System OW i integracje z systemami innych podmiotów zintegrowanych z Systemem OW, w tym systemy klasy EZD.	**Uwaga nieuwzględniona** Uwaga wykracza poza zakres przedmiotowy projektu ustawy. Uwaga nie dotyczy bezpośrednio KPP. Natomiast dotyczy funkcjonowania doręczeń elektronicznych
40.	Art. 5 pkt 2	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Dodanie przepisów wprowadzających system, w którym będzie prowadzony Katalog Podmiotów Publicznych (KPP), ma na celu m.in. wyeliminowanie zauważonych problemów związanych z kwalifikowaniem wybranych podmiotów jako publicznych, których dotyczą przepisy UoDE, możliwości zmiany tych danych, oraz zasad wymiany informacji między KPP a bazą adresów elektronicznych (BAE), ePUAP, KRS i REGON – w których są dane dotyczące również podmiotów publicznych, ale żaden z tych rejestrów nie posiada kompletnych danych o podmiotach publicznych.
41.	Art. 5 pkt 2	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie	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	**Uwaga nieuwzględniona** Uwaga wykracza poza zakres przedmiotowy projektu ustawy. Uwaga nie dotyczy bezpośrednio KPP.

		Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	doręczeń elektronicznych. W efekcie stanowi zwiększenie monopolizacji usług doręczeń elektronicznych i uzależnienie kolejnych pomiotów od Poczty Polskiej. Usunięcie zmiany.	Natomiast dotyczy funkcjonowania doręczeń elektronicznych.
42.	Art. 6	Krajowa Izba Rozliczeniowa	Konieczność doprecyzowania zasad świadczenia usługi wydawania kwalifikowanych certyfikatów podpisu elektronicznego w EPTC. Proponujemy, aby ustawa przesądzała, że użytkownik jest subskrybentem certyfikatu i nie jest wymagane zawarcie z nim umowy na świadczenie usług zaufania. Ma to krytyczne znaczenie w zakresie odpowiedzialności za usługę, RODO i sposób jej świadczenia. Należy zwrócić uwagę, że projekt ustawy zakłada, że subskrybent przy każdym złożeniu podpisu będzie korzystał z losowo wybranego dostawcy. Oznacza to de facto, że nie tylko zostanie pozbawiony wyboru dostawcy, ale także skazany na to, że jego dane osobowe będą przetwarzane przez wielu z nich, zamiast jednego. W naszej ocenie jest to sprzeczne z interesem subskrybenta oraz obowiązkiem RODO projektowania rozwiązań z zachowaniem zasady minimalizacji przetwarzanych danych. W całym procesie wydania i użycia kwalifikowanego certyfikatu do złożenia kwalifikowanego podpisu dochodzi do przetwarzania danych osobowych przez dostawcę usług zaufania. Użytkownik powinien mieć zatem zagwarantowane prawo do decydowania, który dostawca będzie przetwarzał jego dane osobowe oraz zadba o bezpieczeństwo całego procesu, w tym będzie zarządzał jego kluczem prywatnymi. Nie można przesądzać, że pozbawienie wyboru użytkownika służy jego wygodzie. Wręcz przeciwnie, narusza to jego interesy zarówno w zakresie wolności, ale także bezpieczeństwa, prywatności i zasad przetwarzania danych osobowych. Należy bowiem pamiętać, że korzystanie z usług zaufania opiera się właśnie na zaufaniu. Prawo wyboru dostawcy, powierzenia mu danych osobowych i prywatności, a także bezpieczeństwa obsługi to podstawowe elementy zaufania, które powinno być zasadą naczelną także dla podpisu zapewnianego w ramach EPTC. W szczególności wielu użytkowników EPTC będzie korzystało z komercyjnych usług zaufania i z całą pewnością chciałoby korzystać z usług tego samego dostawcy w przypadku korzystania z podpisów w EPTC. Wnosimy o wprowadzenie w ustawie zapisów gwarantujących użytkownikom możliwość wyboru dostawcy usługi. Proponujemy również, aby wytyczne świadczenia usługi określił MC w formie rozporządzenia, a nie w formie publikacji w BIP. Wydaje się, że sposób postępowania przez podmioty prywatne, w tym w zakresie zapewniania usługi na rzecz MC i obywateli, nie powinien być określany w innym trybie niż przepisami prawa. Proponujemy także jednoznacznie potwierdzić ustawą, że dostawcy usług zaufania	**Uwaga wyjaśniona** W odniesieniu do kwestii przesądzenia wprost przepisami ustawy, że „użytkownik jest subskrybentem certyfikatu i nie jest wymagane zawarcie z nim umowy na świadczenie usług zaufania”, rozporządzenie eIDAS w art. 24 ust. 2 lit. d wprost wymaga, aby dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania: „d) przed nawiązaniem stosunku umownego informuje w jasny, kompleksowy i łatwo dostępny sposób, w miejscu publicznie dostępnym oraz indywidualnie wszelkie osoby, które mają zamiar skorzystać z kwalifikowanej usługi zaufania, o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej;” Powyższe znaczy, że nie może tego obowiązku wyłączyć przepisami krajowymi. **Uwaga nieuwzględniona** W odniesieniu do kwestii umożliwienia wyboru dostawcy nieodpłatnego podpisu, przyjęto założenie, że rekompensata będzie zależna od liczby osób korzystających z nieodpłatnego podpisu, a nie od liczby składanych podpisów i dlatego też przyjęto losowy wybór dostawcy. **Uwagi nieuwzględnione** Umieszczenie szczegółowych zasad świadczenia usługi, która umożliwia użytkownikom europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, nieodpłatne składanie kwalifikowanych podpisów elektronicznych w formie wytycznych na BIP jest zabiegiem celowym ze względu na ich techniczny charakter, względy bezpieczeństwa i możliwość wprowadzania aktualizacji w razie konieczności. Jednoznacznie potwierdzenie przepisami ustawy, że dostawcy usług zaufania polegają wyłącznie

			przy weryfikacji tożsamości i wszelkich danych zawieranych w certyfikacie polegają na danych uwalnianych z EPTC.	na danych z EPTC nie jest potrzebne w związku z tym, że ta kwestia będzie określona w wytycznych.
43.	Art. 6 pkt 2	Związek Banków Polski (ZBP)	Należy doprecyzować przepisy projektu w zakresie kwalifikowanego podpisu elektronicznego udostępnianego w ramach europejskiego portfela tożsamości cyfrowej w taki sposób, aby: 1. jednoznacznie wskazać, że oznaczenie podpisu kwalifikowanego jako wykorzystywanego „do celów innych niż profesjonalne" nie wpływa na jego ważność ani skuteczność prawną; 2. wyraźnie określić, że strona ufająca nie jest zobowiązana do weryfikowania celu, w jakim podpis został użyty; 3. wskazać, że odpowiedzialność za wykorzystanie podpisu zgodnie z deklarowanym celem spoczywa na osobie składającej podpis.	**Uwaga wyjaśniona** Zakłada się, że faktyczny skutek prawny oświadczenia woli opatrzonego kwalifikowanym podpisem elektronicznym przeznaczonym do celów innych niż profesjonalne ale w celach profesjonalnych (bez względu na to czy przez omyłkę czy celowo) będzie taki sam jak podpisu własnoręcznego. Wynika to wprost z art. 25 ust. 2 rozporządzenia eIDAS. Nie ma zatem powodu aby strona ufająca była zmuszana do odróżniania podpisów "profesjonalnych" od "nieprofesjonalnych" i miała mieć z tego powodu obawy co do skuteczności wyrażenia woli. Celowo nie przewiduje się sankcji zakładając, że oznaczenie dokumentów klauzulą, która nie powoduje uszkodzenia dokumentu, że zostały opatrzone nieodpłatnym podpisem kwalifikowanym spowoduje powstanie samoregulującego się systemu. Zakłada się, że przedsiębiorcy (a tym bardzie podmioty publiczne) nie będą używali (lub będzie to zjawisko sporadyczne) nieopłatnego podpisu do celów profesjonalnych z uwagi na ich postrzeganie przez kontrahentów i klientów. Celowo nie ustala się sankcji za użycie nieodpłatnego podpisu przeznaczonego co celów innych niż profesjonalne do celów profesjonalnych. Nie zatem ma potrzeby wymagania od strony ufającej weryfikowania celu jak również dawania stronie ufającej możliwości nieprzyjęcia/ podważenia dokumentu podpisanego z wykorzystaniem darmowego podpisu.
44.	Art. 6 pkt 2	Związek Banków Polski (ZBP)	Wnosimy o doprecyzowanie przepisów projektu ustawy w zakresie zasad uznawania europejskich portfeli tożsamości cyfrowej wydawanych przez inne państwa członkowskie UE. W szczególności konieczne jest określenie, w jaki sposób prywatne strony ufające, w tym instytucje finansowe, powinny w praktyce realizować obowiązek uznawania takich portfeli oraz jak mechanizm ten ma funkcjonować w procesach identyfikacji klientów.	**Uwaga wyjaśniona** Zgodnie z art. 5a ust. 5 lit. a pkt II i III wszystkie europejskie portfele tożsamości cyfrowej, w szczególności muszą być zgodne ze wspólnymi protokołami i interfejsami: (...) "(ii) na potrzeby stron ufających do celów żądania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz ich walidacji; (iii) na potrzeby udostępniania i prezentacji stronom ufającym danych identyfikujących osobę,

				elektronicznych poświadczeń atrybutów lub selektywnie ujawnionych powiązanych danych w trybie online oraz, w stosownych przypadkach, w trybie offline;" Powyższe znaczy że skoro będą wspólne protokoły i interfejsy to niewątpliwie w taki sam sposób będzie można jako strona ufająca obsługiwać każdy portfel zgodny z tymi protokołami i interfejsami w taki sam sposób. Co do zasady wprost z art. 5f ust. 1 i 2 rozporządzenia eIDAS wynika, że określone podmioty pod pewnymi warunkami akceptują europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z tym rozporządzeniem. W związku z tym ewentualne interpretacje, wskazujące, że brak numeru PESEL w zestawie danych identyfikujących osobę przekazywanych przez portfel uniemożliwia przeprowadzenie identyfikacji, byłyby niezgodne z tymi przepisami. Ponadto zgodnie z art. 5b ust. 1 rozporządzenia eIDAS w przypadku, gdy strona ufająca zamierza polegać na europejskich portfelach tożsamości cyfrowej na potrzeby świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji, strona ufająca rejestruje się w państwie członkowskim, w którym ma siedzibę. Proces rejestracji w Polsce został określony w projektowanych przepisach art. 22b ustawy o usługach zaufania oraz identyfikacji elektronicznej. Przepisy rozporządzenia eIDAS stosuje się bezpośrednio, zatem nie ma potrzeby ich powtarzania w ustawie. Wyjątkiem jest projektowany art. 14d ustawy o aplikacji mObywatel, który wprowadza rozwiązanie idące dalej niż przepis rozporządzenia eIDAS i w tym zakresie przepis rozróżnia krajowy i zagraniczne europejskie portfele tożsamości cyfrowej.
45.	Art. 6 pkt 2	Związek Banków Polski (ZBP)	Należy doprecyzować przepisy projektu ustawy w zakresie podmiotów uprawnionych do założenia europejskiego portfela tożsamości cyfrowej, tak aby jednoznacznie określić, czy możliwość ta obejmuje wyłącznie osoby prawne w rozumieniu prawa cywilnego, czy również jednostki organizacyjne nieposiadające osobowości prawnej, które uczestniczą w obrocie gospodarczym.	**Uwaga wyjaśniona** Ustawa posługuje się pojęciami ustanowionymi w rozporządzeniu eIDAS, co znaczy że europejski portfel tożsamości cyfrowej dla osoby prawnej będzie oznaczał osoby prawne w rozumieniu eIDAS wyjaśnionym w motywie 68:

				"(68) Pojęcie "osób prawnych" zgodnie z postanowieniami Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) dotyczącymi prowadzenia przedsiębiorstwa pozostawia podmiotom gospodarczym swobodę wyboru formy prawnej, którą uznają za odpowiednią dla prowadzenia swojej działalności. Dlatego też termin "osoby prawne" w rozumieniu TFUE oznacza wszystkie podmioty ustanowione na mocy prawa państwa członkowskiego lub podlegające temu prawu, niezależnie od ich formy prawnej."
46.	Art. 6 pkt 2	Związek Banków Polski (ZBP)	Należy doprecyzować przepisy projektu ustawy w zakresie relacji pomiędzy wykorzystaniem europejskiego portfela tożsamości cyfrowej a obowiązkiem stosowania silnego uwierzytelnienia użytkownika (SCA) wynikającym z przepisów ustawy o usługach płatniczych. W szczególności konieczne jest: 1. jednoznaczne określenie, w jaki sposób wykorzystanie portfela może spełniać wymogi silnego uwierzytelnienia użytkownika w rozumieniu przepisów regulujących usługi płatnicze; 2. doprecyzowanie, czy uwierzytelnienie użytkownika w ramach portfela (np. z wykorzystaniem biometrii lub innych mechanizmów uwierzytelniania dostępnych w aplikacji) może być uznane za spełnienie wymogów SCA, czy też konieczne będzie zastosowanie dodatkowych elementów uwierzytelnienia po stronie dostawcy usług płatniczych; 3. określenie zasad odpowiedzialności w przypadku wykorzystania portfela do autoryzacji transakcji, które okażą się nieautoryzowane z uwagi na nieuprawnione użycie portfela przez osobę trzecią.	**Uwaga wyjaśniona** Kwestia zapewnienia rozwiązania i stosownych procedur dla wypełnienia obowiązku SCA przy wykorzystywaniu europejskiego portfela tożsamości cyfrowej do uwierzytelnienia leży niewątpliwie po stronie banków. Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje - zgodnie z rozporządzeniem 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). Bank otrzyma potwierdzanie tożsamości na wysokim poziomie bezpieczeństwa wraz danymi identyfikującymi osobę i/lub dodatkowymi danymi z elektronicznego poświadczenie atrybutów i będzie musiał to obowiązkowo uznać wprost na podstawie art. 5f ust. 2 rozporządzenia eIDAS. Odpowiedzialność podmiotów zapewniających europejskie portfele tożsamości cyfrowej wynika wprost z rozporządzenia eIDAS, a każde państwo członkowskie jest obowiązane zgodnie a art. 5a ust. 18 przekazać Komisji Europejskiej stosowne informacje, które następnie Komisja publikuje.
47.	Art. 6 pkt 2 - dot. art. 14a ust. 1 pkt 5	PWPW S.A.	W nowoprojektowanym art. 14a ustawy o aplikacji mObywatel w przepisach wskazujących na funkcje, jakie realizuje europejski portfel tożsamości pominięto możliwość wykorzystywana w portfelu kwalifikowanych poświadczeń atrybutów. Z punktu widzenia rozporządzenia eIDAS oraz sposobu działania portfela zasadne	**Uwaga wyjaśniona** Brak uwzględnienia przedmiotowej kwestii w przywołanym przepisie wynika z faktu, że rozporządzenie eIDAS stosuje się bezpośrednio. Funkcja

			jest umożliwienie przetwarzania w portfelu tego rodzaju poświadczeń. Postulujemy zatem rozszerzenie ww. regulacji o wskazany zakres. Propozycja dodania pkt 5 w art. 14a w ust. 1 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel: „5) bezpieczne przechowywanie i walidację elektronicznych poświadczeń atrybutów, kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu, a także bezpieczne zarządzanie tymi poświadczeniami na potrzeby udostępniania ich stronom ufającym.”.	ta będzie więc w europejskim portfelu tożsamości cyfrowej, gdyż minister właściwy do spraw informatyzacji zobowiązany będzie do zapewnienia tego portfela zgodnie z art. 5a i in. rozporządzenia eIDAS. Ponadto warto zwrócić uwagę, że nawet przedmiotowy przepis literalnie posługuje się zwrotem "w tym", wskazującym, że mamy do czynienia z katalogiem otwartym.
48.	Art. 6 pkt 2 - dot. art. 14a ust. 2	Fundacja Future Finance Poland	Obowiązek akceptacji EUDI Wallet Postulujemy wprowadzenie przepisu doprecyzowującego status numeru identyfikacyjnego EUDI Wallet w procesach identyfikacji tożsamości, w tym w procedurach przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (AML/KYC). Proponowana zmiana do Art. 6 ust. 2 Projektu ustawy, wprowadzająca art. 14a ust. 2, przewiduje dodanie przepisu w części dotyczącej danych identyfikujących osoby, w którym wskazuje się, że identyfikator przekazywany z europejskiego portfela tożsamości cyfrowej może być stosowany w rozumieniu numeru i serii dokumentu tożsamości w procesach weryfikacji tożsamości w sektorze finansowym. Nowy ustęp mógłby brzmieć następująco: „W procesach identyfikacji i weryfikacji tożsamości prowadzonych na podstawie przepisów odrębnych, w szczególności dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, „numer danych identyfikujących daną osobę”, o którym mowa w art. 14a ust. 2 pkt 4, przekazywany z europejskiego portfela tożsamości cyfrowej, może być traktowany jako numer dokumentu identyfikacyjnego osoby.” Doprecyzowanie to jest niezbędne, ponieważ sektor finansowy potrzebuje jednoznacznej podstawy prawnej do wykorzystywania identyfikatora z portfela w procedurach AML/KYC. Obecnie przepisy regulacji AML wymagają podczas identyfikacji pobrania numeru i serii dokumentu tożsamości, niezależnie od tego, czy identyfikacja przebiega na podstawie dokumentu tożsamości, czy środka identyfikacji elektronicznej. Ponadto postuluje się doprecyzowanie Projektu ustawy w zakresie tzw. „pełnego zestawu danych”, numeru PESEL oraz portfeli wydawanych w innych państwach UE, w taki sposób, aby brak PESEL nie uniemożliwiał przeprowadzenia identyfikacji. Art. 6 ust. 2 Projektu ustawy, wprowadzający art. 14a ust. 2, powinien obejmować następujące elementy: wprowadzenie definicji, że europejski portfel tożsamości cyfrowej w przepisach krajowych obejmuje także portfele wydane lub uznane przez inne państwa członkowskie UE, w zakresie uznawania wynikającym z eIDAS 2.0; doprecyzowanie, że europejski portfel cyfrowy zawiera Krajowy Numer Identyfikacyjny, o ile taki numer został	**Uwaga uwzględniona/wyjaśniona** W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d. Zgodnie z przepisami dotyczącymi rejestracji w rejestrze stron ufających, w tym wskazywania zakresu danych dla każdej usługi, jak również propozycji polegania na certyfikatach rejestracji strony ufającej portfele tożsamości cyfrowej automatycznie rozpoznają zakres danych, jaki jest wymagany dla określonej usługi i po stronie użytkownika pozostaje wybór czy z danej usługi skorzystać. Z drugiej strony w przypadku otrzymania żądania ujawnienia danych, które użytkownikowi wydaje się nadmiarowe lub podejrzane będzie miał on możliwość zgłoszenia tego faktu organowi ochrony danych osobowych. Wizerunek twarzy został dodany w projekcie ustawy do zakresu danych identyfikujących osobę zgodnie z przepisami rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej. Zgodnie z art. 3 ust. 2 tego rozporządzenia: "Dostawcy danych identyfikujących osobę zapewniają, aby dane identyfikujące osobę wydane do jednostek portfela zawierały informacje niezbędne do uwierzytelnienia i walidacji danych identyfikujących osobę". Wizerunek

			ustanowiony w danym kraju; oraz wskazanie, że dla Europejskich Środków Identyfikacji Elektronicznej wydawanych w Polsce Krajowym Numerem Identyfikacyjnym, o którym mowa w art. 14a ust. 2 pkt 5, będzie numer PESEL. Takie doprecyzowanie eliminuje ryzyko interpretacji, w której brak numeru PESEL w portfelu uniemożliwia identyfikację, co jest szczególnie istotne w przypadku klientów bez PESEL, w tym cudzoziemców, oraz w kontekście portfeli transgranicznych przekazujących różne zestawy danych. Wyraźne ujęcie tych zasad w art. 14a ust. 2 zapewnia, że procesy onboardingowe i dostęp do usług pozostaną możliwe, a praktyka rynkowa w zakresie stosowania europejskich portfeli tożsamości cyfrowej będzie jednolita. Proponowany mechanizm „selektywnego udostępniania danych" jest korzystny z perspektywy ochrony prywatności klientów, jednak może stanowić istotną barierę operacyjną dla wielu instytucji, ponieważ w praktyce skutkuje otrzymywaniem niekompletnych danych niezbędnych do przeprowadzenia procesów identyfikacji, zawarcia umowy lub realizacji transakcji. W związku z tym mechanizm powinien umożliwiać stronie ufającej, czyli instytucji, wymuszenie określonego profilu danych (pakietu), który jest niezbędny do realizacji danej usługi. Klient powinien mieć możliwość wyboru między udostępnieniem wszystkich danych wymaganych ustawowo a rezygnacją z korzystania z usługi, zamiast możliwości przesyłania niepełnych formularzy lub ograniczania zakresu zgód na przetwarzanie danych w odniesieniu do poszczególnych celów. Takie podejście pozwala zachować równowagę między ochroną prywatności a zapewnieniem prawidłowego funkcjonowania usług finansowych. Art. 14a Projektu ustawy określa zakres danych identyfikujących osobę fizyczną, obejmujący m.in. "wizerunek twarzy użytkownika portfela". W praktyce oznacza to, że w procesie identyfikacji przy wzajemnej fizycznej obecności stron strona ufająca może porównać wizerunek twarzy pobrany z EUDI Wallet z osobą, która faktycznie stoi przed nią, co jest równoważne weryfikacji z dokumentu tożsamości. Warto podkreślić, że eIDAS 2.0 nie nakłada obowiązku akceptacji wszystkich atrybutów portfela, w tym wizerunku twarzy, w relacjach z instytucjami przy identyfikacji użytkownika - polski projekt ustawy idzie w tym zakresie o krok dalej, umożliwiając w praktyce porównanie wizerunku z portfela z osobą fizycznie obecną, co w efekcie zrównuje PID z dokumentem tożsamości w procesach stacjonarnych. Jednocześnie projekt nie precyzuje, że akceptacja tej formy identyfikacji jest obligatoryjna w procesach onboardingowych, co może rodzić różne interpretacje po stronie instytucji finansowych. Doprecyzowanie art. 14a jest więc kluczowe dla zapewnienia zgodności procedur identyfikacyjnych oraz zachowania jednoznacznej praktyki rynkowej w zakresie stosowania europejskich portfeli tożsamości cyfrowej zarówno w procesach stacjonarnych, jak i zdalnych.	twarzy wymieniony jest w załączniku do tego rozporządzenia w katalogu opcjonalnych dane identyfikujące osobę w przypadku osoby fizycznej. Projektodawca ustawy na tej podstawie zdecydował się na dodanie wizerunku twarzy do zakresu danych identyfikujących osobę z uwagi na doniosłe znaczenie dla bezpieczeństwa potwierdzania tożsamości w warunkach fizycznej obecności stron. Należy przy tym zwrócić uwagę na obowiązek akceptacji europejskiego portfela w warunkach fizycznej obecności stron do celów stwierdzania tożsamości lub obywatelstwa, o którym mowa w art. 14d dodawanym do ustawy o aplikacji mObywatel na warunkach wskazanych w tym przepisie, który jest wzorowany na obecnie obowiązującym art. 7 ust. 4 tej ustawy.

49.	Art. 6 ust. 2 - art. 14a ust. 2 pkt 4	Związek Banków Polski (ZBP)	W art. 14a ust. 2 pkt 4 wskazano, że europejski portfel tożsamości cyfrowej zawiera dane obejmujące miejsce urodzenia. W jakim formacie będzie zapisywana ta informacja - czy będzie to wyłącznie kraj, czy również miejscowość?	**Uwaga wyjaśniona** Specyfikacje techniczne dotyczące danych identyfikujących osobę (w tym miejsce urodzenia) zostały zawarte w załącznikach do rozporządzenia wykonawczego 2024/2977 w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej.
50.	Art. 6 ust. 2 - dot. art. 14a ust. 2 pkt 4	Związek Banków Polski (ZBP)	Należy wprowadzić przepis jednoznacznie wskazujący, że numer identyfikacyjny europejskiego środka identyfikacji elektronicznej może być wykorzystywany jako odpowiednik numeru dokumentu tożsamości w procesach identyfikacji i weryfikacji tożsamości. W art. 6 ust. 2 projektu ustawy, wprowadzającym art. 14a ustawy o aplikacji mObywatel, zdaniem sektora zasadnym byłoby dodanie przepisu w części dotyczącej danych identyfikujących osobę, który wskazywałby, że identyfikator przekazywany z europejskiego portfela tożsamości cyfrowej może być wykorzystywany jako numer identyfikacyjny w procesach identyfikacji tożsamości prowadzonych przez podmioty sektora finansowego. Sugerujemy dodanie do projektu przepisu w brzmieniu: „W procesach identyfikacji i weryfikacji tożsamości prowadzonych na podstawie przepisów odrębnych, w szczególności dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, numer danych identyfikujących osobę, o którym mowa w art. 14a ust. 2 pkt 4, przekazywany z europejskiego portfela tożsamości cyfrowej, może być traktowany jako numer dokumentu identyfikacyjnego osoby.”	**Uwaga uwzględniona** W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d.
51.	Art. 6 pkt 2 - dot. art. 14a ust. 4 pkt 1	Polska Izba Ubezpieczeń	Zwracamy się z prośbą o doprecyzowanie znaczenia pojęcia „data i godzina wygaśnięcia ważności danych identyfikujących daną osobę”, zawartego w projektowanym art. 14a ust. 4 pkt 1 ustawy o aplikacji mObywatel, w szczególności wyjaśnienie, czy odnosi się ono do ważności dokumentu źródłowego (dowód osobisty lub paszport), czy też aktualności zestawu danych identyfikujących, pozyskiwanych w sposób opisany w ust. 5 tego przepisu.	**Uwaga wyjaśniona** Pojęcie „data i godzina wygaśnięcia ważności danych identyfikujących daną osobę” dotyczy zestawu danych identyfikujących, pozyskiwanych w sposób opisany w ust. 5 tego przepisu.
52.	Art. 6 pkt 2 - dot. art. 14a ust. 6	PWPW S.A.	Analiza przepisów projektu ustawy prowadzi do wniosku, iż celem ustawodawcy jest uniemożliwienie posiadania w jednym europejskim portfelu tożsamości danych dotyczących osoby fizycznej i danych dotyczących osoby prawnej (powiązanej z tą osobą fizyczną), nawet jeżeli biznesowo i kontekstowo z punktu widzenia używalności portfela jest to uzasadnione (np. jedyny wspólnik w spółce z o.o.). Proponujemy wprowadzenie wprost regulacji, która dopuszcza takie rozwiązanie albo takie przeformułowanie brzmienia przepisów w sposób dopuszczający tego rodzaju rozwiązanie. W naszej ocenie przyczyni się to do	**Uwaga wyjaśniona** W ocenie projektodawcy przepisy w zaproponowanym kształcie nie przesądzają o uniemożliwieniu posiadania w jednym europejskim portfelu tożsamości cyfrowej danych dotyczących osoby fizycznej i danych dotyczących osoby prawnej.

			zwiększania adopcji portfela także w obrocie gospodarczym. Propozycja nowego brzmienia art. 14a ust. 6 ustawy o aplikacji mObywatel: „6. W jednej instancji europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, jest możliwe ujawnienie danych, o których mowa w ust. 2 i 3.”.	
53.	Art. 6 pkt 2 - dot. art. 14a ust. 7	PWPW S.A.	Przyjęcie minimalnej stawki SOU na poziomie 1 zł może prowadzić do sytuacji, w której świadczenie usług stanie się nierentowne dla dostawców. Dlatego postuluje się zwiększenie minimalnej wartości stawki SOU do poziomu 1 zł 40 gr. Jednocześnie proponuje się wprowadzenie mechanizmu uzależniającego wysokość stawek SOU od liczby użytkowników (LUP), w sposób zapewniający proporcjonalność wynagrodzenia do skali systemu. Dodatkowo proponuje się w rozporządzeniu, o którym mowa w art. 14e ust. 13 pkt 2, zawrzeć poniższe przedziały i stawki dla SOU: - Kwota 2 zł 60 gr za wolumen użytkowników od 1 do 3 000 000 - Kwota 2 zł 20 gr za wolumen użytkowników od 3000 001 do 5 000 000 - Kwota 2 zł za wolumen użytkowników od 5 000 001 do 6 000 000 - Kwota 1 zł 80 gr za wolumen użytkowników od 6 000 001 do 7 000 000 - Kwota 1 zł 60 gr za wolumen użytkowników od 7 000 001 do 8 000 000 - Kwota 1 zł 40 gr za wolumen użytkowników od 8 000 001 wzwyż Propozycja brzmienia przepisu „7. Stawka opłaty SOU nie może być niższa niż 1 zł 40 gr i nie wyższa niż 2 zł 60 groszy, w zależności od liczby użytkowników europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014.”.	**Uwaga nieuwzględniona** W ocenie projektodawcy zaproponowana w projekcie stawka jest adekwatna do realiów rynkowych.
54.	Art. 6 pkt 2 - dot. art. 14a ust. 8	PWPW S.A.	W związku z wejściem w życie rozporządzenia eIDAS2 oraz wprowadzaniem nowych, bardziej rygorystycznych norm świadczenia usług zaufania, a także rosnącymi wymaganiami wynikającymi z implementacji dyrektywy NIS2, dostawcy usług zaufania zobowiązani są do poniesienia istotnych nakładów inwestycyjnych oraz zwiększonych kosztów osobowych w celu dostosowania swoich rozwiązań do podwyższonych standardów. Obecna wycena na poziomie 300 000 zł rocznie jest niewystarczająca i nie odzwierciedla realnych kosztów ponoszonych przez dostawców usług zaufania w związku z zapewnieniem usług na potrzeby portfela eIDAS2. Proponowane podniesienie stawki SOG do poziomu 600 000 zł rocznie pozwoli na częściowe zrekompensowanie kosztów związanych z budową i utrzymaniem niezbędnej infrastruktury oraz pokryciem bieżących kosztów operacyjnych, szczególnie w początkowym okresie funkcjonowania portfela, kiedy przewidywany poziom wykorzystania portfelowych usług zaufania będzie relatywnie niski. Zmiana ta przyczyni się do zapewnienia stabilności świadczenia usług oraz umożliwi dostawcom spełnienie rosnących wymagań regulacyjnych. Przepis art. 14e ust. 8 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel	**Uwaga nieuwzględniona** W ocenie projektodawcy zaproponowana w projekcie stawka jest adekwatna do realiów rynkowych. Należy mieć na uwadze, że dostawcy usług kwalifikowanych poza dostarczeniem podpisów dla użytkownika portfela również w oparciu o tożsamość z portfela będą realizowali transakcje komercyjne.

			powinien otrzymać brzmienie: „8. Opłata SOG wynosi 600 tysięcy złotych.”.	
55.	Art. 6 pkt 2 - dot. art. 14b ust. 1	Krajowa Izba Rozliczeniowa	Zakładanie EPTC z wykorzystaniem kwalifikowanego podpisu elektronicznego Proponujemy rozważenie możliwości zakładania EPTC z wykorzystaniem profilu zaufanego wraz z kwalifikowanym podpisem elektronicznym. Nie przewiduje tego proponowany w ustawie o aplikacji mObywatel – art. 14b ust. 1.	**Uwaga wyjaśniona** Przepis art. 14b ust. 1 przewiduje taką możliwość w ramach przepisu art. 14b ust. 1 pkt 1 na warunkach określonych w rozporządzeniu wykonawczym Komisji (UE) 2026/798z dnia 7 kwietnia 2026 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi wysokiego poziomu bezpieczeństwa.
56.	Art. 6 pkt 2 - dot. art. 14b ust. 1	PWPW S.A.	W projektowanych przepisach pominięto kwestie związane z zapewnieniem odpowiedniego poziomu bezpieczeństwa procesu wydania i aktywacji dokumentu cyfrowego w europejskim portfelu tożsamości cyfrowej (tzw. onboarding użytkownika). Mając na uwadze znaczenie tego procesu dla zapewnienia wiarygodności tożsamości oraz zapobiegania nadużyciom (w tym kradzieży tożsamości), zasadne jest wprowadzenie regulacji wskazujących na konieczność stosowania mechanizmów silnego uwierzytelnienia, w szczególności weryfikacji biometrycznej użytkownika. Analogiczne rozwiązania przewidziane są już w projekcie w odniesieniu do potwierdzania profilu zaufanego, co uzasadnia ich rozszerzenie na proces onboardingu do europejskiego portfela tożsamości cyfrowej. W projektowanym brzmieniu art. 14b ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel: 1) w ust. 1 pkt 2 i 3 powinny otrzymać brzmienie: „2) za pomocą profilu zaufanego z wykorzystaniem weryfikacji biometrycznej tożsamości oraz przy wykorzystaniu metod weryfikacji tożsamości spełniających wymagania określone w przepisach wykonawczych wydanych na podstawie art. 5a ust. 24 rozporządzenia 910/2014, albo 3) w punkcie potwierdzającym tożsamość podczas obecności fizycznej po okazaniu dokumentu stwierdzającego tożsamość i obywatelstwo, który zawiera dowody identyfikacji fotograficznej lub biometrycznej, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej,	**Uwaga nieuwzględniona** Propozycja sprowadza się de facto do wskazania alternatywnych metod uwierzytelnienia użytkownika europejskiego portfela tożsamości cyfrowej. W ocenie projektodawcy przepisy w zaproponowanym kształcie pozostają w zgodzie z przywołanymi w nich aktami prawnymi i pozwalają na zachowanie ewentualnej elastyczności w kształtowaniu tych rozwiązań.

			na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z 2015 r. Nr 235, str. 7, z późn. zm.), zwanego dalej „rozporządzeniem 2015/1502", umożliwiające potwierdzenie za pomocą metod weryfikacji biometrycznej deklarowanej tożsamości, w celu porównania co najmniej jednej cechy fizycznej osoby, której tożsamość jest weryfikowana."; 2) należy dodać nowy ust. 2 w brzmieniu (i przenumerować kolejne projektowane ustępy): „2. Dane biometryczne uzyskane w procesach weryfikacji tożsamości o których mowa w ust. 1 pkt 2 i 3, nie podlegają utrwaleniu i są przetwarzane wyłącznie przez okres przeprowadzenia procedury weryfikacji.".	
57.	Art. 6 pkt 2 - dot. art. 14b ust. 1 pkt 2	PWPW S.A.	W projektowanym art. 14b ust. 1 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel PWPW S.A. proponuje rezygnację z przywoływania nazwy konkretnego środka identyfikacji elektronicznej, ponieważ może to ograniczyć rozwój rynku. Przy takim bowiem sformułowaniu przepis nie będzie uwzględniał innych środków identyfikacji (spełniających wymagany poziom) i innych metod weryfikacji tożsamości, które są obecnie znane, ale nie zostały uwzględnione.	**Uwaga uwzględniona** Przepis został zmieniony..
58.	Art. 6 ust. 2 dot. art. 14b ust. 3	Związek Banków Polski (ZBP)	W art. 14b ust. 3 wskazano, że minister właściwy do spraw informatyzacji określi w drodze rozporządzenia wymagania dotyczące weryfikacji tożsamości. Do kiedy planowane jest wydanie tego rozporządzenia?	**Uwaga wyjaśniona** Rozporządzenie wejdzie w życie wraz z wejściem w życie projektowanej ustawy.
59.	Art. 6 pkt 2 - dot. art. 14d	Krajowa Izba Rozliczeniowa	Obowiązek uznawania EPTC podczas wzajemnej fizycznej obecności stron Proponujemy skreślić dodawany w ustawie o aplikacji mObywatel art. 14d. EPTC jest środkiem identyfikacji elektronicznej, a nie dowodem tożsamości. Co do zasady służy on do identyfikacji w dostępie do usług online, a w trybie offline wyłącznie „w stosownych przypadkach", a więc na zasadach wyjątku, a nie powszechnego obowiązku. Ponadto w przypadku użycia offline musi to być możliwe „przy użyciu technologii zbliżeniowych" i bez „dostępu do systemów zdalnych za pośrednictwem sieci komunikacji elektronicznej do celów tej interakcji" (art. 3 pkt 57 eIDAS) oraz, co istotne, z zachowaniem wymogu selektywnego ujawniania powiązanych danych (art. 5a ust. 4 lit. a). Spełnienie tych wymogów – w przypadku okazywania się wizualizacją danych EPTC wraz z wizerunkiem użytkownika – wydaje się trudne. Należy również pamiętać, że nałożenie obowiązku uznawania EPTC, w tym EPTC zagranicznych, na wszystkie instytucje w Polsce, na obecnym etapie wdrożenia EPTC, naraża je na niebagatelne koszty przy niemal zerowych korzyściach. mDowód był i jest krajowym rozwiązaniem, więc jego modyfikacja i rozbudowa nie zależała od regulacji unijnych. W chwili wprowadzania mDowodu pokrycie rynkowe było liczone w milionach. Ponadto mDowód był narzędziem gotowym do adopcji, działał na znanych schematach, a wdrożenie jego obsługi nie było nazbyt	**Uwaga nieuwzględniona** Dla użytkowników aplikacji mObywatel jest oczywiste, że zastępuje ona dokument tożsamości i taki był jeden z pierwotnych celów udostępnienia tej aplikacji. Mając uwadze powyższe zasadne jest, aby również za pomocą portfela potwierdzanie tożsamości w podczas obecności fizycznej było możliwe, zwłaszcza w kontekście jego zabezpieczeń zapewniających wysoki poziom bezpieczeństwa. Podsumowując, powyższą kwestię należy oceniać kompleksowo nie tylko w odniesieniu do stron ufających, ale również względem przewidywanych oczekiwań użytkowników. Wprowadzono stosowne vacatio legis dla omawianego art. 14d.

			kłopotliwe i nie wiązało się z większymi kosztami, choć i tak nastręczyło trudności. Dawało to jednak korzyść dla stron ufających, gdyż wielu ich klientów już go używało. W przypadku EPTC tak nie jest.	
60.	Art. 6 pkt 2 - dot. art. 14d	Związek Banków Polski (ZBP)	Należy jednoznacznie określić w przepisach, że uznawanie Europejskiego Portfela Tożsamości Cyfrowej (EPTC) w procesach identyfikacji prowadzonych w placówkach, tj. w sytuacji wzajemnej fizycznej obecności stron, nie stanowi obowiązku dla podmiotów sektora prywatnego, w tym banków. (…) W przypadku gdyby ustawodawca zdecydował się jednak na wprowadzenie obowiązku akceptacji portfela przez instytucje obowiązane, konieczne byłoby zapewnienie odpowiednio długiego okresu dostosowawczego. W szczególności należałoby rozważyć powiązanie takiego obowiązku z terminem wynikającym z art. 5f ust. 2 rozporządzenia eIDAS, tj. 24 grudnia 2027 r., i wprowadzenie co najmniej rocznego vacatio legis umożliwiającego dostosowanie systemów oraz procesów operacyjnych instytucji finansowych.	**Uwaga częściowo uwzględniona** Dla użytkowników aplikacji mObywatel jest oczywiste, że zastępuje ona dokument tożsamości i taki był jeden z pierwotnych celów udostępnienia tej aplikacji. Mając uwadze powyższe zasadne jest aby również za pomocą portfela potwierdzanie tożsamości w podczas obecności fizycznej było możliwe, zwłaszcza w kontekście jego zabezpieczeń zapewniających wysoki poziom bezpieczeństwa. Podsumowując, powyższą kwestię należy oceniać kompleksowo nie tylko w odniesieni do stron ufających, ale również względem przewidywanych oczekiwań użytkowników. Wprowadzono stosowne vacatio legis dla omawianego art. 14d.
61.	Art. 6 pkt 2 - dot. 14d	Związek Banków Polski (ZBP)	Zdaniem sektora należy doprecyzować przepisy projektu ustawy w celu: 1. jednoznacznego wskazania, że regulacje dotyczące europejskiego portfela tożsamości cyfrowej odnoszą się do wszystkich portfeli zapewnianych zgodnie z rozporządzeniem eIDAS, w tym portfeli wydawanych przez inne państwa członkowskie Unii Europejskiej; 2. wyeliminowania interpretacji, zgodnie z którą brak numeru PESEL w zestawie danych identyfikujących osobę przekazywanych przez portfel uniemożliwia przeprowadzenie identyfikacji; 3. doprecyzowania, że portfel zawiera krajowy numer identyfikacyjny właściwy dla państwa wydającego środek identyfikacji elektronicznej, przy czym w przypadku portfeli wydawanych w Polsce będzie nim numer PESEL.	**Uwaga wyjaśniona / częściowo uwzględniona** Zgodnie z art. 5a ust. 5 lit a pkt II i III rozporządzenia eIDAS wszystkie europejskie portfele tożsamości cyfrowej, w szczególności muszą być zgodne ze wspólnymi protokołami i interfejsami: (...) "(ii) na potrzeby stron ufających do celów żądania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz ich walidacji; (iii) na potrzeby udostępniania i prezentacji stronom ufającym danych identyfikujących osobę, elektronicznych poświadczeń atrybutów lub selektywnie ujawnionych powiązanych danych w trybie online oraz, w stosownych przypadkach, w trybie offline;" Powyższe znaczy że skoro będą wspólne protokoły i interfejsy to niewątpliwie w taki sam sposób będzie można jako strona ufająca obsługiwać każdy portfel zgodny z tymi protokołami i interfejsami w taki sam sposób. Co do zasady wprost z art. 5f ust. 1 i 2 rozporządzenia eIDAS wynika, że określone podmioty pod pewnymi warunkami akceptują europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z tym

				rozporządzeniem. W związku z tym ewentualne interpretacje wskazujące, że brak numeru PESEL w zestawie danych identyfikujących osobę przekazywanych przez portfel uniemożliwia przeprowadzenie identyfikacji, byłyby niezgodne z tymi przepisami. Przepisy rozporządzenia eIDAS stosuje się bezpośrednio, zatem nie ma potrzeby ich powtarzania w ustawie. Nie można w polskich przepisach ustanawiać wymagań regulowanych przepisami europejskimi. Zakres danych identyfikujących osobę, jaki ma obowiązkowo znaleźć się w europejskich portfelach tożsamości cyfrowej określa rozporządzenie wykonawcze 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). Nie jest wymagane umieszczenie w ramach tego zakresu elementu "personal_administrative_number", gdyż znajduje się on w tabeli 2 z danymi opcjonalnymi, co znaczy że państwa członkowskie UE same zdecydują o tym czy będzie się on znajdował w danych identyfikujących osobę w portfelach zapewnianych w tych państwach. Podobnie jest w przypadku elementu "document_number" wymienionego w ramach zbioru metadanych zdefiniowany, w tabeli 5 ww. rozporządzenia. Wyjątkiem jest projektowany art. 14d ustawy o aplikacji mObywatel, który idzie nieco szerzej od rozporządzenia eIDAS i w tym zakresie przepis rozróżnia krajowy i zagraniczne europejskie portfele tożsamości cyfrowej.
62.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	Jaka była intencja ustawodawcy przy formułowaniu art. 14d ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel, w szczególności poprzez dodanie sformułowania „podczas wzajemnej fizycznej obecności stron”? Warto wskazać, że podobne sformułowanie pojawia się również w art. 2 pkt 8 tej ustawy i pozwala na wykorzystanie mDowodu w procesie identyfikacji i weryfikacji tożsamości wyłącznie w kontaktach bezpośrednich bank–klient, co ogranicza weryfikację tożsamości w oparciu o mDowód w trybie online.	**Uwaga wyjaśniona** Należy zaznaczyć, że obowiązek polegania na europejskich portfelach tożsamości cyfrowej (w tym na danych identyfikujących osobę) wynika wprost z art. 5f ust. 1 i 2 rozporządzenia eIDAS. Z uwagi na to, że przepisy art. 5a ust. 4 jednoznacznie wskazują że portfele takie zapewniają uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych

				przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych w proponowanym nowym art. 14d ust. 1 wskazano taki stosowny przypadek – adekwatnie do tego jaki ma już miejsce przypadku dokumentu mObywatel. Mając na uwadze, że europejskie portfele tożsamości cyfrowej z założenia spełniają wymagania dla wysokiego poziomu bezpieczeństwa i wymagają certyfikacji w tym zakresie za oczywiste należało przyjąć, że to narzędzie powinno równie skutecznie potwierdzać tożsamość jak dokument mObywatel.
63.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	Czy identyfikacja w oparciu o portfel tożsamości cyfrowej lub dane identyfikujące osobę fizyczną zawarte w portfelu ma całkowicie zastępować identyfikację dokonywaną na podstawie dowodu osobistego lub paszportu? Czy w praktyce okazanie portfela zwalnia z obowiązku wglądu w fizyczny dowód osobisty lub paszport?	**Uwaga wyjaśniona** Dane identyfikujące osobę fizyczną zawarte w portfelu są równoważne z danymi w dowodach osobistych i paszportach.
64.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	W jakim zakresie bank jest zobligowany do stosowania portfela w procesach związanych z weryfikacją tożsamości? Czy obowiązek ten dotyczy wyłącznie ustalenia danych klienta i weryfikacji jego tożsamości, czy również całego procesu onboardingu, w tym przyjęcia wniosku o otwarcie produktu bankowego oraz podpisania umowy o produkt bankowy?	**Uwaga wyjaśniona** Przepisy rozporządzenia eIDAS obowiązują bezpośrednio – zarówno w zakresie obowiązkowej akceptacji portfela, o czym mowa w art. 5f ust. 1 i 2, jak również możliwości polegania na portfelu przez dowolna stroną ufającą o czym mowa w art. 5b. Zgodnie z tymi przepisami przedsiębiorca będzie mógł potwierdzać dane za pomocą europejskiego portfela tożsamości cyfrowej, jeżeli spełni wymagania art. 5b ust. 1, 2, 3, 8, 9 oraz rozporządzania wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848).
65.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	W odniesieniu do art. 14d ust. 1 ustawy prosimy o potwierdzenie, czy podmiot korzystający z portfela w celu identyfikacji osoby będzie musiał być zarejestrowany jako strona ufająca oraz zintegrowany z całym ekosystemem portfela, czy też przewidziany będzie uproszczony tryb korzystania z portfela.	**Uwaga wyjaśniona** Planuje się przygotowanie rozwiązania do weryfikacji przy fizycznej obecności stron w uproszczonym trybie przy użyciu technologii zbliżeniowych (bez konieczności rejestracji w rejestrze stron ufających) zgodnie z motywem 17 rozporządzenia 2014/1183, zgodnie z którym: "Proces rejestracji powinien umożliwiać szereg przypadków użycia, które mogą różnić się pod względem trybu działania - online lub w trybie offline - lub pod względem wymogu uwierzytelnienia urządzeń do celów

				połączenia z europejskim portfelem tożsamości cyfrowej. Rejestracja powinna mieć zastosowanie wyłącznie do stron ufających świadczących usługi za pośrednictwem interakcji cyfrowych."
66.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	W portfelu cyfrowym nie będą dostępne dane takie jak seria i numer dowodu osobistego oraz data jego ważności. Tymczasem banki są zobowiązane ustawą AML do ustalenia tych danych. Czy identyfikacja na podstawie portfela zwalniałaby bank z obowiązku ustalenia danych dokumentu tożsamości?	**Uwaga uwzględniona** W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d.
67.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	Czy zastosowanie portfela podczas weryfikacji tożsamości oznacza, że bank nie musi ustalać i weryfikować danych dokumentu tożsamości, tj. dowodu osobistego lub paszportu?	**Uwaga wyjaśniona** Dane identyfikujące osobę fizyczną zawarte w portfelu są równoważne z danymi w dowodach osobistych i paszportach.
68.	Art. 6 ust. 2 - dot. art. 14d	Związek Banków Polski (ZBP)	Od kiedy przepis art. 14d ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel ma obowiązywać w praktyce? Czy banki będą zobowiązane do jego stosowania od końca 2026 r., czy dopiero od końca 2027 r.?	**Uwaga uwzględniona** Wprowadzono stosowne vacatio legis dla omawianego art. 14d.
69.	Art. 6 pkt 2 - dot. art. 14d ust. 1	Polska Izba Ubezpieczeń	Poprosimy o zmianę redakcji w art. 14d ust. 1 nowelizowanej Ustawy o aplikacji mObywatel poprzez wykreślenie sformułowania „podczas wzajemnej fizycznej obecności stron”. „Art. 14d. 1. Jeżeli z przepisu prawa wynika obowiązek stwierdzenia tożsamości lub obywatelstwa na podstawie dokumentu tożsamości, w szczególności na podstawie dowodu osobistego lub paszportu, obowiązek ten uznaje się za spełniony w przypadku stwierdzenia tożsamości lub obywatelstwa na podstawie pełnego zestawu danych identyfikujących osobę fizyczną, jakie zawiera europejskie portfel tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a) rozporządzenia 910/2014, podczas wzajemnej fizycznej obecności stron.”	**Uwaga nieuwzględniona** Dla użytkowników aplikacji mObywatel jest oczywiste, że zastępuje ona dokument tożsamości i taki był jeden z pierwotnych celów udostępnienia tej aplikacji. Pozbawienie europejskiego portfela tożsamości cyfrowej takiej funkcjonalności uczyni go narzędziem pozbawionym kluczowej cechy i spowoduje konieczność stałego utrzymywania dwóch równoległych rozwiązań cyfrowych do potwierdzani tożsamości. Dodatkowo spowoduje trudne do wyjaśnienia użytkownikom ograniczenia, ponieważ w taki sposób będą to postrzegali. Mając uwadze powyższe, zasadne jest, aby również za pomocą portfela potwierdzanie tożsamości w podczas obecności fizycznej było możliwe, zwłaszcza w kontekście jego zabezpieczeń zapewniających wysoki poziom bezpieczeństwa. Podsumowując, powyższą kwestię należy oceniać kompleksowo nie tylko w odniesieniu do stron ufających, ale również względem przewidywanych oczekiwań użytkowników.
70.	Art. 6 pkt 2 - dot. art. 14e	PWPW S.A.	Rozważenia wymaga korekta projektowanego art. 14e ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. Co do zasady usługę związaną z wydaniem kwalifikowanych certyfikatów pozwalającą na świadczenie usługi składania podpisu może świadczyć podmiot kwalifikowany, a docelowo usługa składania	**Uwaga wyjaśniona** Przepis wskazuje na fakt, że minister będzie udostępniał usługę składania nieodpłatnych kwalifikowanych podpisów elektronicznych w celach innych niż

			podpisu będzie realizowana przez podmioty kwalifikowane. Wprowadzenie zaś upoważnienia dla ministra właściwego do spraw informatyzacji w tym zakresie jest uprawnieniem nadmiarowym, ponieważ to podmioty kwalifikowane będą udostępniały tę usługę.	profesjonalne. W art 14e ust. 2 jest informacja, że w celu zapewnienia usługi kwalifikowani dostawcy usług zaufania składają wniosek do ministra właściwego do spraw informatyzacji.
71.	Art. 6 pkt 2 - dot. art. 14e ust. 1	Fundacja Future Finance Poland	Podpisy elektroniczne W art. 14e ust. 1 Projektu ustawy przewidziano, że przy użyciu europejskiego portfela tożsamości cyfrowej możliwe będzie nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne. W związku z tym pojawiają się wątpliwości co do skutków prawnych użycia takiego podpisu w celach profesjonalnych, w tym czy podpis pozostaje wówczas ważny. Proponujemy więc doprecyzowanie, że cel podpisu nie wpływa na jego ważność ani skuteczność prawną, a odpowiedzialność za zgodność użycia podpisu z deklarowanym celem ponosi wyłącznie osoba składająca podpis. Strona ufająca nie powinna być zobowiązana do weryfikowania, czy podpis został użyty zgodnie z deklarowanym celem. Doprecyzowanie to jest niezbędne dla zapewnienia jednoznaczności przepisów i ma zapobiec sytuacjom, w których ważność kwalifikowanego podpisu mogłaby być podważana lub kwestionowana wyłącznie ze względu na deklarowany cel, chroniąc tym samym skuteczność prawną dokumentu, którym podpis został opatrzony.	**Uwaga wyjaśniona** W brzmieniu projektowanych przepisów zdefiniowano cel składania nieodpłatnego kwalifikowanego podpisu elektronicznego „inny niż profesjonalny”. Celowo nie ustala się sankcji za użycie nieodpłatnego podpisu przeznaczonego co celów innych niż profesjonalne do celów profesjonalnych. Nie ma potrzeby dawania stronie ufającej możliwości nieprzyjęcia/ podważenia dokumentu podpisanego z wykorzystaniem darmowego podpisu. Zgodnie z art. 25 ust. 1 rozporządzenia eIDAS: "Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu", przepis nie przewiduje od tego żadnych wyjątków. Zakłada się, że nie powinno się obciążać stron ufających (ani sądów) koniecznością precyzyjnego odróżniania celu złożenia podpisu. Taki podpis będzie równie ważny. Zakłada się jednak, że darmowy podpis nie będzie wykorzystywany do celów profesjonalnych z uwagi na dbałość przedsiębiorców o swój wizerunek.
72.	Art. 6 pkt 2 - dot. art. 14e ust. 1	Polska Izba Ubezpieczeń	Przepis art. 14e ust. 1 nowelizowanej Ustawy o aplikacji mObywatel posługuje się pojęciem „celów innych niż profesjonalne”. Ma to na celu wdrożenie tzw. opcji narodowej ustanowionej w art. 5a ust. 5 in fine Rozporządzenia eIDAS. W tym zakresie polska propozycja przepisów wprost powtarza pojęcie „celów innych niż profesjonalne”. Tym niemniej pojęcie takie nie jest powszechnie spotykane na gruncie przepisów krajowych i w efekcie może rodzić wątpliwości. W związku z tym należy postulować zmianę treści tego przepisu tak aby odwoływał się do ugruntowanego na gruncie prawa polskiego pojęcia „konsumenta”. W związku z tym, proponujemy zmianę brzmienia powyższego przepisu art. 14e ust. 1 w następujący sposób: „Art. 14e. ust. 1. Minister właściwy do spraw informatyzacji udostępnia przy użyciu europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, usługę, która umożliwia użytkownikom europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, będących konsumentami, nieodpłatne składanie kwalifikowanych podpisów elektronicznych, zgodnie z art. 5a ust. 5 lit. g rozporządzenia 910/2014.”	**Uwaga wyjaśniona/częściowo uwzględniona** Cel złożenia podpisu inny niż profesjonalny został doprecyzowany w art. 14f ust. 1 ustawy o aplikacji mObywatel. W ocenie projektodawców zaproponowana definicja jest dostatecznie jasna i nie ma potrzeby dodatkowego odwoływania się do pojęcia konsumenta. W art. 14f ust. 1 zostało poprawione odesłanie.

73.	Art. 6 pkt 2 - dot. 14e ust. 13 pkt 2	Krajowa Izba Rozliczeniowa	Zmiana zasad ustalania wysokości rekompensaty Proponujemy, aby udział danego dostawcy usług zaufania w łącznej kwocie rekompensaty był uzależniony od liczby obsłużonych przez nie kwalifikowanych podpisów elektronicznych. Proponujemy, aby mechanizm obsługi użytkowników – zarówno ze względu na zasadność i wysokość ponoszenia wydatków publicznych, jak i ochronę praw użytkowników, a także zasady świadczenia usług zaufania przez dostawców – był regulowany ustawą. Za niewystraczające należy uznać opisanie go w uzasadnieniu i OSR, a w przyszłości ewentualnie w BIP. Postulujemy, aby ustawa przesądzała, że rozporządzenie, o którym art. 14e ust. 13 pkt 2 mające określić wysokość stawki opłaty SOU, było każdorazowo wydawane raz w roku, a stawka obowiązywała przez cały rok i nie podlegała zmianie w trakcie roku kalendarzowego. Wreszcie proponujemy, aby kwoty wskazane w ustawie były kwotami netto.	**Uwaga częściowo uwzględniona** Przyjęto założenie, że rekompensata będzie zależna od liczby użytkowników, a nie od liczby składanych podpisów i dlatego też przyjęto losowy wybór dostawcy, aby zagwarantować dostawcom sprawiedliwą rekompensatę. Nie uzależniono rekompensaty od liczby podpisów, również dlatego, że celne oszacowanie, jakie koszty rekompensaty w takim przypadku należałoby zaplanować, jest niemożliwe z uwagi na to, że jest to zupełnie nowa usługa, realizowana za pomocą nowego narzędzia. Pilotaż, jaki ma miejsce obecnie z wykorzystaniem aplikacji mObywatel, potwierdza taki kierunek rozliczeń. Jeżeli chodzi o postulat, aby ustawa przesądzała, że rozporządzenie, o którym art. 14e ust. 13 pkt 2 mające określić wysokość stawki opłaty SOU, było każdorazowo wydawane raz w roku, a stawka obowiązywała przez cały rok, to w związku z tą uwagą zauważono potrzebę zmiany przepisu art. 14e ust. 6 pkt 2 lit b, tak aby liczba użytkowników nie dotyczyła „danego roku kalendarzowego”, gdyż literalnie stosowanie tego przepisu spowodowałoby „zerowanie” liczby użytkowników w każdym nowym rokiem kalendarzowym i co za tym idzie niesprawiedliwe traktowanie dostawców. Kwoty wskazane w ustawie są kwotami brutto.
74.	Art. 6 pkt 2 - dot. art. 14f ust. 1	Krajowa Izba Rozliczeniowa	Zmiana definicji celu nieprofesjonalnego składania kwalifikowanego podpisu elektronicznego Ustawa wprowadza znacznie szerszą definicją zastosowania nieprofesjonalnego niż zostało to przyjęte na etapie pilota z mObywatelem. Definicja zaproponowana w ustawie jest następująca (brakuje zapisu „niezwiązanej z zawieraniem umów konsumenckich”): 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. Obecnie zaproponowana definicja obejmuje również wszystkie przypadki	**Uwaga nieuwzględniona** Wyłączanie zawierania umów konsumenckich z nieprofesjonalnego użycia będzie niezrozumiałe dla użytkowników, którzy będą (przypuszczalnie skutecznie) dowodzić, że z ich strony zawarcie umowy konsumenckiej w celach prywatnych (niezwiązanych bezpośrednio z działalnością zawodową czy gospodarczą) jest całkowicie pozbawione cech działalności profesjonalnej z ich strony.

			zawierania przez osobę prywatną umowy na dostawę usług z podmiotem komercyjnym. Proponujemy, aby art. 14f ust. 1 brzmiał na wzór definicji przyjętej w pilotażu składania kwalifikowanego podpisu elektronicznego w ramach aplikacji mObywatel, tj.: 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.	
75.	Art. 6 pkt 2 - dot. art. 14f ust. 1	PWPW S.A.	W ocenie PWPW S.A. projektowane regulacje dotyczące wykorzystywania podpisów kwalifikowanych w ramach europejskiego portfela tożsamości wyłącznie w obrocie nieprofesjonalnym wymagają uzupełnienia. Obrót profesjonalny w rozumieniu przepisów rozporządzenia 910/2014 nie odnosi się wyłącznie do podmiotów gospodarczych (co zostało już ujęte w projekcie), ale także do podmiotów publicznych. Z tego powodu jako niedopuszczalne należy uznać wykorzystywanie takiego podpisu do realizacji zadań służbowych przez podmioty publiczne i ich pracowników. Dodatkowym ograniczeniem w używaniu takich podpisów powinno być także używanie ich przez osoby fizyczne nie będące przedsiębiorcami w relacji z podmiotami gospodarczymi. Takie relacje, ze względu na występowanie w nich podmiotów profesjonalnych, także należy zaliczyć do obrotu profesjonalnego W celu uwzględnieniu uwagi projektowanemu art. 14f ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel PWPW S.A. proponuje nadać brzmienie: „Art. 14f. 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 złożenia oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej w związku z załatwieniem sprawy prywatnej, niezwiązanej z wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, którą składający to oświadczenie reprezentuje. 2. Nieodpłatny kwalifikowany podpis elektroniczny, o którym mowa w ust. 1, nie może być wykorzystywany przez osoby fizyczne do: 1) opatrywania dokumentów zawierających oświadczenie woli lub oświadczenie wiedzy w relacjach z podmiotami prowadzącymi działalności gospodarczą lub zawodową, lub w kontaktach z osobami reprezentującymi te podmioty, w szczególności dla zawarcia umów przez konsumentów;	**Uwaga wyjaśniona** Zaproponowana regulacja art. 14f ust. 1, w ocenie projektodawcy, zapewnia dostateczną jasność w tym zakresie. Według zaproponowanej definicji w zakresie celu innego niż profesjonalny nie będą mieścić się przypadki używania takiego podpisu przez pracowników podmiotów publicznych w celach służbowych. Równocześnie należy zwrócić uwagę, że wykraczająca poza przepisy rozporządzenia eIDAS (i w konsekwencji z nimi niezgodna) byłaby regulacja, która jako cel profesjonalny traktowałaby składanie podpisu przez "zwykłą" osobę fizyczną (nie w kontekście jej działalności gospodarczej lub zawodowej) w jej relacji do przedsiębiorcy. Z tego względu zasadnym jest pozostanie przy obecnym brzmieniu zaproponowanego przepisu.

			2) wydawania aktów administracyjnych w imieniu podmiotów publicznych. 3. Dokumenty elektroniczne opatrzone nieodpłatnym kwalifikowanym podpisem elektronicznym w celu innym niż profesjonalny oznacza się w sposób umożliwiający stwierdzenie użycia takiego podpisu. 4. Użytkownik portfela potwierdza w europejskim portfelu tożsamości zapoznanie się z zasadami użycia nieodpłatnego kwalifikowanego podpisu elektronicznym w celu innym niż profesjonalny.”.	
76.	Art. 6 pkt 2 - dot. art. 14f ust. 1	Stowarzyszenie Nowoczesnej Edukacji Prawnej	Propozycja: Dopisanie w art. 14f ust. 1 projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122) następujących słów: "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, z wyjątkiem nieprowadzącej działalności gospodarczej organizacji pozarządowej, o której mowa w art. 3 ust. 2 ustawy o działalności pożytku publicznego i o wolontariacie, który składający to oświadczenia reprezentuje." Uzasadnienie: Art. 14f ust. 1 projektu ustawy wskazuje, że "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." Należy dodać, że zgodnie z art. 5a ust. 5 rozporządzenia Parlamentu Europejskiego 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 "państwa członkowskie mogą przewidzieć proporcjonalne środki w celu zapewnienia, aby nieodpłatne używanie kwalifikowanych podpisów elektronicznych przez osoby fizyczne było ograniczone do celów innych niż profesjonalne". Taki środek w odniesieniu do organizacji pozarządowych, nieprowadzących działalności gospodarczej, nie wydaje się proporcjonalny. Nie można zgodzić się z tym, że cel profesjonalny dotyczy działalności każdej osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej. Organizacje pozarządowe co do zasady nie mają charakteru profesjonalnego, a stanowią formę zrzeszania się jako realizacji prawa konstytucyjnego, często o skali	**Uwaga nieuwzględniona** Co do zasady nie należy robić wyjątków dla żadnych osób reprezentujących podmioty zbiorowe. Organizacje pozarządowe może nie mają charakteru komercyjnego, ale są niewątpliwie podmiotami profesjonalnymi.

			lokalnej lub regionalnej. Przeciętne przychody organizacji w 2023 roku wyniosły jedynie 50 tys. zł (Raport “Kondycja organizacji pozarządowych 2024”, Badania Klon/Jawor). Dodatkowo uzasadnienie projektu wskazuje jedynie, że "kwalifikowane podpisy elektroniczne używane nie tylko w celach nieprofesjonalnych, ale również w celu prowadzenia działalności biznesowej przez przedsiębiorców, byłoby nieetyczne, z uwagi na to, że ilość podpisów, jakie potrzebuje złożyć osoba fizyczna w celach nieprofesjonalnych, jest znikoma wobec ilości podpisów, jakie potrzebuje złożyć firma lub osoba fizyczna prowadząca działalność gospodarczą w celach profesjonalnych." Należy zgodzić się z tym uzasadnieniem, jednakże działalność biznesowa nie jest prowadzona przez te organizacje pozarządowe, które nie prowadzą działalności gospodarczej, więc to uzasadnienie nie znajduje zastosowania w ich przypadku. Liczba podpisów, która będzie tutaj niezbędna, także będzie znikoma wobec podmiotów prowadzących działalność gospodarczą. Nieetyczne będzie w tym przypadku wymaganie tych samych wydatków od podmiotów prowadzących działalność gospodarczą i od podmiotów non-profit. Organizacje pozarządowe szeroko korzystają z podpisu zaufanego. Niestety, aktualne brzmienie przepisów ogranicza zastosowanie podpisu zaufanego jako równoważnego formie pisemnej. Art. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne bowiem zawęża jej zakres zastosowania do podmiotów publicznych i to nie wszystkich (np. nie dotyczy do Kancelarii Sejmu, Kancelarii Prezydenta czy Narodowego Banku Polskiego). Wskutek tego ograniczenia, nie jest możliwe np. do podpisywania umów z zakresu prawa cywilnego czy dokumentów z zakresu prawa pracy. Szczególnie problematyczne jest zawieranie umów prawnoautorskich, które muszą mieć formę pisemną pod rygorem nieważności. To spory problem dla cyfryzacji organizacji pozarządowych. Problem ten jednak nie zostanie rozwiązany przez projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122) w aktualnym brzmieniu, stąd niezbędna jest zmiana.	
77.	Art. 6 pkt 2 - dot. art. 14g	PWPW S.A.	W projektowanym art. 14g ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel PWPW S.A. proponuje zdefiniowanie funkcjonalności określonego środka identyfikacji elektronicznej oraz jego czynników uwierzytelnienia w sposób umożliwiający wykorzystanie tego środka bez interakcji z innym zależnymi usługami lub innymi środkami identyfikacji elektronicznej. Wskazana funkcjonalność udostępniona w ramach portfela cyfrowego będąca czynnikiem uwierzytelnienia innego środka identyfikacji elektronicznej stanowi istotne ograniczenie wykorzystania profilu zaufanego w przypadku utraty kontroli nad samą aplikacją portfela cyfrowego. W takim przypadku użytkownik, tracąc z	**Uwaga wyjaśniona** Zgodnie z rozporządzeniem Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego par. 8 pkt. 4: Uwierzytelnienie z wykorzystaniem profilu zaufanego dokonywane jest w sposób zapewniający średni poziom bezpieczeństwa, przy wykorzystaniu co najmniej dwóch czynników uwierzytelnienia należących do co najmniej dwóch różnych kategorii, o których mowa w przepisach

			przyczyn losowych kontrolę nad jednym środkiem identyfikacji, jakim będzie portfel cyfrowy (dostęp do aplikacji), w rezultacie traci również możliwość wykorzystania środka identyfikacji o niższym poziomie ufności.	wydanych na podstawie art. 8 ust. 3 rozporządzenia 910/2014, przy czym: 1) jeden czynnik stanowi: a) identyfikator użytkownika i hasło do konta profilu zaufanego albo b) inny czynnik uwierzytelniania wymagający od osoby podlegającej uwierzytelnieniu określonej, znanej tylko tej osobie wiedzy, albo c) dane posiadacza profilu zaufanego zweryfikowane za pomocą kwalifikowanego certyfikatu podpisu elektronicznego; 2) drugi czynnik stanowi: a) hasło jednorazowe przesyłane na wskazany przez użytkownika numer telefonu komórkowego albo b) inny czynnik uwierzytelniania wymagający od posiadacza profilu zaufanego wykazania się posiadaniem ustalonej uprzednio rzeczy lub urządzenia niezbędnego dla wykorzystania tego czynnika. Co oznacza, że użytkownik w przypadku utraty kontroli nad portfelem (a z uwagi na jego konstrukcję i fakt, że spełnia on wysoki poziom bezpieczeństwa ryzyko tego jest niskie), będzie mógł wykorzystywać inne metody autoryzacji.
78.	Art. 6 pkt 2 - dot. art. 14g	PWPW S.A.	W projektowanych przepisach ustawy o usługach zaufania zmieniających ustawę m.in. o aplikacji mObywatel należy doprowadzić do ponownego powiązania wzajemnego danych stanowiących atrybuty, które mogą być udostępniane w europejskim portfelu tożsamości, z danymi, które są powiązane z dokumentami publicznym, funkcjonującym w obrocie prawnym. Ustawodawca powinien wprowadzić mechanizm wzajemnej koordynacji działań ministra właściwego do spraw informatyzacji i ministra właściwego do spraw wewnętrznych w zakresie wydawania atrybutów tożsamych z danymi zawartymi w dokumentach publicznych. Osobna współpraca powinna dotyczyć emitentów dokumentów publicznych. Poza proponowaną ogólną regulacją nakazującą współpracę należy wprowadzić regulacje proceduralne. Do projektowanego brzmienia art. 14g ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel proponuje się dodać ust. 4-6 w brzmieniu: „4. W przypadku przechowywania i udostępnienia w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, elektronicznych poświadczeń atrybutów, kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń	**Uwaga wyjaśniona** Ostatnie zmiany wprowadzone do rozporządzenia eIDAS rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ustanowiły między innymi europejski portfel tożsamości cyfrowej i nową usługę zaufania jaką jest wydawanie elektronicznych poświadczeń atrybutów. Europejski portfel tożsamości cyfrowej, jak również elektroniczne poświadczenia atrybutów, nie są dokumentami publicznymi w rozumieniu ustawy o dokumentach publicznych, jak również należą do odrębnego niezależnego reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim. Wdrożenie rozporządzenia eIDAS nie będzie miało negatywnego wpływu na jednolitość polityki bezpieczeństwa dokumentów publicznych.

			atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu na postawie przyjętych schematów zawierających zestaw danych tożsamych z danymi, które maja być zawarte w dokumentach publicznych, schematy poświadczeń atrybutów podlegają ocenie przez Komisję, o której mowa w art. 49 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych, na zasadach wskazanych w tej ustawie. 5. Przekazanie elektronicznych poświadczeń atrybutów na podstawie schematów, o których mowa w ust. 4, do europejskiego portfela tożsamości cyfrowej możliwe jest po uzyskaniu pozytywnej oceny Komisji. 6. Schematy , o których mowa w ust. 4, są przekazywane do oceny Komisji przez podmiot odpowiedzialny za źródło autentyczne albo kwalifikowanego dostawcę elektronicznego poświadczenia atrybutów lub podmiot działający w imieniu podmiotu, w tym podmiotu sektora publicznego odpowiedzialnego za źródło autentyczne. 7. Podmiot, o którym mowa w ust. 6, przekazuje Komisji: 1) schemat elektronicznego poświadczenia atrybutów; 2) odpowiednio informacje, o których mowa w art. 24h ustawy o usługach zaufania…". (w wersji proponowanej w niniejszych uwagach). W konsekwencji tej uwagi projekt ustawy należy uzupełnić o nowelizację art. 49 ustawy o dokumentach publicznych poprzez dodanie po ust. 2 ust. 2a i 2b w brzmieniu: „2a. Komisja ocenia schematy elektronicznych poświadczeń atrybutów, które mają podlegać przechowywaniu i udostępnieniu w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, jeżeli schematy te zawierają zestaw danych tożsamych z danymi, które mają być zawarte w dokumentach publicznych. 2b. Komisja ocenia schematy poświadczeń atrybutów pod kątem spójności zestawu prezentowanych danych z danymi, które mają być zawarte w dokumentach publicznych dla obu postaci dokumentów oraz bezpieczeństwa obrotu prawnego. ".	
79.	Art. 6 pkt 2 - dot. art. 14g ust. 1	Fundacja Future Finance Poland	W art. 14g ust. 1 Projektu ustawy przewidziano, że w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a eIDAS 2.0, mogą być udostępniane różne usługi umożliwiające użytkownikowi europejskiego portfela tożsamości cyfrowej, w tym m.in. „dokonywanie płatności elektronicznych związanych z usługami online świadczonymi na rzecz użytkownika europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014;". Zwracamy uwagę, że eIDAS 2.0 nie przewiduje obsługi przez europejski portfel tożsamości cyfrowej „dokonywania płatności elektronicznych". Oznacza to, że Projekt ustawy w tym zakresie wykracza poza ramy eIDAS 2.0 i nie jest niezbędny	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność sektora płatniczego. Projektowany przepis stanowi wyłącznie o umożliwieniu dokonania płatności elektronicznych w ramach świadczonych usług na rzecz użytkownika portfela usług.

			do jego implementacji. Należy również zaznaczyć, że eIDAS 2.0 nie nakłada obowiązku obsługi takich płatności na uczestników rynku. Obowiązek dotyczy wyłącznie stosowania silnego uwierzytelniania użytkownika (zob. art. 5f ust. 2 eIDAS 2.0). Wprawdzie Projekt ustawy również nie nakłada obowiązku na inne podmioty obsługi takich płatności (jest tam mowa tylko o „możliwości" udostępniania usług, o których mowa w tym przepisie), jednak – dla przejrzystości tej regulacji – proponujemy odpowiednie doprecyzowanie w formie ust. 3 do tego artykułu: 3. Umożliwienie korzystania z usług, o których mowa w ust. 1 i 2, przez strony ufające lub inne podmioty, jest dobrowolne, chyba że co innego wynika z niniejszej ustawy lub z przepisów odrębnych. Warto również dodać, że „dokonywanie płatności elektronicznych" jest co do zasady świadczeniem usług płatniczych. Należałoby zatem wyjaśnić, w jakim zakresie i na jakich zasadach usługi takie będą świadczone, oraz kwestie jak np. zakres odpowiedzialności dostawcy europejskiego portfela tożsamości cyfrowej wobec użytkowników z tytułu nieautoryzowanych transakcji płatniczych. Ponieważ rynek usług płatniczych jest bardzo konkurencyjny, potrzebne jest również uzasadnienie, dlaczego projektodawca uważa, że państwo (Minister właściwy do spraw informatyzacji) powinno świadczyć takie usługi, być może wypierając dostawców sektora prywatnego z tego rynku. Sugerujemy również rozważenie, czy celem projektodawcy nie było raczej, aby dostawca portfela był kwalifikowany nie jako dostawca usług płatniczych, ale jako dostawca usług technicznych, wzorem portfeli Apple albo Google. Wówczas należałoby odpowiednio przeredagować ten przepis i zrezygnować z frazy „dokonywanie płatności elektronicznych".	Jest to analogiczne rozwiązanie, które funkcjonuje już obecnie na gruncie ustawy o aplikacji mObywatel i nie stwarza wątpliwości w zakresie wskazanym w uwadze.
80.	Art. 6 ust. 2 - dot. art. 14g ust. 1 pkt 6	Polska Bezgotówkowa	Projekt ustawy nie nakłada jednak na podmioty trzecie żadnych obowiązków – nie jest również jasne, w jaki sposób dokonywanie takich płatności miałoby przebiegać. Zwracamy uwagę, że obsługa transakcji płatniczych przez dostawcę portfela — choćby w ograniczonym zakresie — w praktyce może oznaczać wejście w obszar regulowany przepisami dotyczącymi usług płatniczych. W takiej sytuacji konieczne byłoby bardzo precyzyjne określenie następujących zagadnień: 1) Podstawy prawne i zakres funkcjonalny usług płatniczych. Należy jednoznacznie wskazać, czy dostawca portfela miałby: a) świadczyć usługi płatnicze w rozumieniu ustawy o usługach płatniczych, b) jedynie pośredniczyć w inicjowaniu transakcji, c) czy wyłącznie udostępniać interfejs techniczny (np. przekierowanie do usługodawcy płatności).	**Uwaga wyjaśniona** Zgodnie z art. 2 pkt 9 rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej, poprzez pojęcie „dostawca portfela", należy rozumieć osobę fizyczną lub prawną, która dostarcza rozwiązania w zakresie portfela, natomiast art. 2 pkt 4 rozporządzenia wykonawczego 2024/2977 definiuje pojęcie „rozwiązanie w zakresie portfela", jako połączenie oprogramowania, sprzętu, usług, ustawień i konfiguracji, z uwzględnieniem instancji portfela, co najmniej jednej bezpiecznej aplikacji kryptograficznej portfela oraz co

				najmniej jednego bezpiecznego urządzenia kryptograficznego portfela. Powyższe rozporządzenie wykonawcze reguluje kwestie związane z potwierdzaniem tożsamości posiadacza portfela w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej lub możliwość poświadczenia atrybutu posiadacza portfela za pomocą elektronicznego poświadczenia atrybutu. Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane jeżeli chodzi o ich podstawowe funkcje - zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Oznacza to, że: a) Dostawca portfela nie będzie świadczyć usług płatniczych. b) i c) Dostawca portfela udostępni jedynie interfejs techniczny dla takich usług. Stosowne wyjaśnienie zostało wprowadzone do uzasadnienia do projektu ustawy.
81.	Art. 6 ust. 2 - dot. art. 14g ust. 1 pkt 6	Polska Bezgotówkowa	2) Zakres odpowiedzialności dostawcy portfela, w szczególności konieczne jest wskazanie, kto ponosi odpowiedzialność za: a) nieautoryzowane transakcje, b) nieprawidłową realizację transakcji, c) ewentualne awarie uniemożliwiające dokonanie płatności, d) błędne przekazywanie danych identyfikacyjnych lub atrybutów niezbędnych do wykonania płatności.	**Uwaga wyjaśniona** Należy mieć na uwadze, że Instytucje obowiązane (w rozumieniu ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu) otrzymają potwierdzanie tożsamości na wysokim poziomie bezpieczeństwa (art. 5a ust. 11 rozporządzenia eIDAS) wraz danymi identyfikującymi osobę i/lub dodatkowymi danymi z elektronicznego poświadczenie atrybutów i będzie musiał to obowiązkowo uznać wprost na podstawie art. 5f ust. 2 eIDAS. Odpowiedzialność podmiotów zapewniających europejski portfele tożsamości cyfrowej wynika wprost z rozporządzenia eIDAS, a każde państwo członkowskie jest obowiązane zgodnie z art. 5a ust. 18 przekazać

				Komisji Europejskiej stosowne informacje, które następnie Komisja publikuje.
82.	Art. 6 ust. 2 - dot. art. 14g ust. 1 pkt 6	Polska Bezgotówkowa	3) Zgodność z regulacjami nadzorczymi i europejskimi standardami rynku płatniczego. W przypadku, gdy państwowy dostawca portfela miałby świadczyć usługi płatnicze, należy określić: czy podlegałby wymogom nadzorczym właściwym dla instytucji płatniczych, czy stosowane byłyby wymogi w zakresie AML/CFT, PSD2/PSD3, DORA i innych, w jaki sposób zapewniona byłaby interoperacyjność z prywatnymi dostawcami usług płatniczych.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność sektora płatniczego. Projektowany przepis stanowi wyłącznie o umożliwieniu dokonania płatności elektronicznych w ramach świadczonych usług na rzecz użytkownika portfela usług. Jest to analogiczne rozwiązanie, które funkcjonuje już obecnie na gruncie ustawy o aplikacji mObywatel. W ocenie projektodawcy nie stwarza to wątpliwości w zakresie wskazanej w uwadze. Stosowne wyjaśnienie zostało wprowadzone do uzasadnienia do projektu ustawy.
83.	Art. 6 ust. 2 - dot. art. 14g ust. 1 pkt 6	Polska Bezgotówkowa	4) Wpływ na konkurencyjność sektora płatniczego. Sektor płatniczy cechuje się wysokim poziomem konkurencji i innowacyjności, w dużej mierze napędzanej przez podmioty prywatne. Wprowadzenie państwowej platformy potrafiącej obsługiwać płatności mogłoby: a) zakłócić równowagę rynkową, b) zmniejszyć dynamikę inwestycji i rozwoju innowacji, c) ograniczyć dostęp prywatnych firm do użytkowników, którzy zostaliby przekierowani do rozwiązania publicznego.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność sektora płatniczego. Projektowany przepis stanowi wyłącznie o umożliwieniu dokonania płatności elektronicznych w ramach świadczonych usług na rzecz użytkownika portfela usług. Jest to analogiczne rozwiązanie, które funkcjonuje już obecnie na gruncie ustawy o aplikacji mObywatel i w ocenie projektodawcy nie stwarza to wątpliwości w zakresie wskazanej w uwadze. Stosowne wyjaśnienie zostało wprowadzone do uzasadnienia do projektu ustawy.
84.	Art. 6 ust. 2 - dot. art. 14g ust. 1 pkt 6	Związek Banków Polski (ZBP)	Projekt przewiduje możliwość udostępniania w portfelu usług polegających na „dokonywaniu płatności elektronicznych”, choć rozporządzenie eIDAS nie przewiduje takiej funkcjonalności. W tym zakresie projekt wykracza zatem poza ramy niezbędnej implementacji eIDAS. Zasadne jest doprecyzowanie, że korzystanie z takich usług przez strony ufające i inne podmioty ma charakter dobrowolny, o ile obowiązek taki nie wynika z przepisów szczególnych.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność

			3. Umożliwienie korzystania z usług, o których mowa w ust. 1 i 2, przez strony ufające lub inne podmioty, jest dobrowolne, chyba że co innego wynika z niniejszej ustawy lub z przepisów odrębnych.	sektora płatniczego. Projektowany przepis stanowi wyłącznie o umożliwieniu dokonania płatności elektronicznych w ramach świadczonych usług na rzecz użytkownika portfela usług. Jest to analogiczne rozwiązanie, które funkcjonuje już obecnie na gruncie ustawy o aplikacji mObywatel. które nie stwarza wątpliwości wskazanych w uwadze. Stosowne wyjaśnienie dopisano do uzasadnienia do projektu ustawy: „Europejski portfel tożsamości cyfrowej nie będzie w swej istocie stanowić środka do dokonywania płatności, natomiast będzie jedynie stanowić interfejs techniczny dla usług płatniczych. W związku z tym nie wpłynie on na konkurencyjność sektora płatniczego.”
85.	Art. 6 pkt 2 - dot. art. 14g ust. 1 pkt 7	PWPW S.A.	W projektowanym art. 14g ust. 1 pkt 7 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel rozważenia wymaga celowość pozostawiania tak wielu dopuszczalnych form składania podpisu, które dla większości użytkowników nie są, choć powinny być, właściwie rozróżnialne i wykorzystywane. Celowym wydaje się ograniczenie do podpisu kwalifikowanego i podpisu osobistego, co powinno mieć pozytywny wpływ na popularyzację i rozpoznawalność usług elektronicznych wśród obywateli.	**Uwaga wyjaśniona** Podpis zaufany jest doskonale znanym i powszechnie używanym narzędziem (ponad 14,3 miliona użytkowników profilu zaufanego w dniu 24 marca 2026) umożliwiającym wygodne nieodpłatne podpisywanie podań i wniosków kierowanych do podmiotów publicznych. Podpis osobisty jest wydawany wraz dowodem osobistym każdemu chętnemu obywatelowi w celu zapewnienia nieodpłatnego podpisu elektronicznego w interakcjach nie tylko z podmiotami publicznymi, ale również w stosunkach cywilnoprawnych. Mając na uwadze, że wskazane rozwiązania są darmowe dla ich użytkowników należy przyjąć założenie, że nie jest możliwe wprowadzenie w przyszłości opłat za ich użytkowanie. Znaczy to również, że ewentualne zastąpienie takich podpisów wyłącznie kwalifikowanymi podpisami elektronicznymi wymagałoby zapewnienia przez Skarb Państwa takiego alternatywnego rozwiązania również za darmo. Wszystkie wymienione w tym przepisie rodzaje podpisów funkcjonują już powszechnie w obrocie prawnym i cieszą się dużą popularnością. Ograniczenie możliwości posługiwania się nimi tylko do wybranych podpisów mogłaby być dla użytkowników niezrozumiałe

				oraz mógłby negatywnie przyczynić się w przyszłości na rozwoju europejskiego portfela tożsamości cyfrowej.
86.	Art. 6 ust. 2 - dot. art. 14h	Związek Banków Polski (ZBP)	Art. 14h ustawy przewiduje wydanie przez Radę Ministrów rozporządzenia określającego zakres danych oraz wykaz rejestrów publicznych i systemów teleinformatycznych. Do kiedy planowane jest wydanie tego rozporządzenia?	**Uwaga wyjaśniona** Planowana jest rezygnacja z wydania rozporządzenia.
87.	Art. 6 pkt 2 i pkt 5	Związek Przedsiębiorstw Finansowych w Polsce	Postulujemy zatem doprecyzowanie Projektu ustawy przez jasne określenie relacji pomiędzy aplikacją mObywatel a europejskim portfelem tożsamości cyfrowej, w tym w szczególności docelowej architektury funkcjonalnej, zasad interoperacyjności oraz zakresu funkcji realizowanych przez każde z tych rozwiązań.	**Uwaga wyjaśniona** Wyjaśnienie w tym zakresie znajduje się w uzasadnieniu do projektu ustawy. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
88.	Art. 6 ust. 4 pkt 4) oraz Uzasadnienie (str. 28)	Związek Banków Polski (ZBP)	W odniesieniu do art. 6 ust. 4 pkt 4 projektu ustawy oraz uzasadnienia (str. 28), gdzie wskazano, że jedną z metadanych dotyczących zestawu danych identyfikujących osobę będzie numer danych identyfikujących o znaczeniu podobnym do numeru dokumentu mObywatel: a) czy numer ten powinien być traktowany jak numer dokumentu tożsamości i tym samym być rejestrowany w systemach bankowych analogicznie jak inne dokumenty tożsamości; b) czy będzie istniała możliwość jego zastrzeżenia lub odwołania (w odniesieniu do pojęcia „unieważnienia” użytego w ustawie) w aplikacji portfela.	**Uwaga wyjaśniona** Taki numer zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977) może, ale nie musi być nadawany. W Polsce zakłada się, że będzie nadawany. Wydaje się, odpowiedź na pytanie, czy numer ten może mieć znaczenie w procedurach bankowych, jest we właściwości banków. Ustalenia dotyczące zawieszenia, cofnięcie i przywrócenia krajowego portfela jako środka identyfikacji elektronicznej o którym mowa w cz. 2.2.3 załącznika do CIR 1502/2015 nie zostały jeszcze ostatecznie podjęte (trwają prace nad tzw. krajowym programem certyfikacji, o którym mowa w art. 5c rozporządzenia eIDAS).

89.	Art. 6 pkt 5 w zakresie art. 16	Konfederacja Lewiatan	Usunięcie z projektu podziału na dwa rozwiązania W projekcie nowelizacji ustawy o aplikacji mObywatel (art. 6 pkt 5 zmieniający art. 16) ustawodawca wskazuje, że “podmiot zainteresowany świadczeniem nowej usługi w aplikacji mObywatel oraz w ramach europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, może wystąpić do ministra właściwego do spraw informatyzacji z wnioskiem o opracowanie, udostępnienie oraz umożliwienie temu podmiotowi świadczenia takiej usługi w ramach obu tych rozwiązań”. Wprowadzenie tego rozgraniczenia na aplikację "mObywatel" oraz "europejski portfel" i traktowanie ich jako odmiennych usług może prowadzić do problemów natury prawnej i praktycznej. Przykładowo, wielu przedsiębiorców (m.in. z sektora finansowego czy telekomunikacyjnego) zainwestowało już czas i środki w integrację swoich systemów z krajowym rozwiązaniem. Projektodawca w uzasadnieniu wprost przyznaje, że "nie będzie możliwe przenoszenie dokumentów mobilnych z aplikacji mObywatel do europejskiego portfela", a także "nie będzie przepływu danych z aplikacji mObywatel" do nowego rozwiązania. Oznacza to, że w przypadku firmy świadczące usługi online będą musiały ponownie budować połączenie z nową aplikacją, a następnie utrzymywać zgodność z obydwiema architekturami. Natomiast w przypadku wyłączenia bądź drastycznej zmiany mObywatela, dobrze działające już rozwiązania biznesowe narażone są na wygaszenie, a przedsiębiorcy - na starty. Dlatego też rekomendujemy zmodyfikowanie zapisów projektu ustawy (w tym art. 16 ustawy o mObywatelu) tak, aby nie tworzyły one dwóch odizolowanych systemów. Aplikacja mObywatel powinna zostać odpowiednio przystosowana technologicznie i zyskać status certyfikowanego EPTC. Tylko takie podejście zagwarantuje minimalizację kosztów dla przedsiębiorców, wygodę użytkowników i szybką adaptację unijnych przepisów w polskiej gospodarce.	**Uwaga wyjaśniona/częściowo uwzględniona** Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). W szczególności muszą obsługiwać dane identyfikujące osobę i elektroniczne poświadczenie atrybutów wydawane w formatach danych ISO/IEC.18013-5:2021 oraz Verifiable Credentials Data Model 1.1. Ponadto muszą rozpoznawać i odpowiednio interpretować certyfikaty dostępu i certyfikaty rejestracji stron ufających portfela, 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 portfela (Dz. U. UE. L. z 2025 r. poz. 848). Istotne znaczenie ma również poziom bezpieczeństwa identyfikacji elektronicznej, jaki ma zapewniać portfel (wysoki) a poziom bezpieczeństwa, jaki zapewnia obecnie aplikacja mObywatel (średni). Tym niemniej dołożone zostaną wszelkie starania, aby zmiany jakie wymusza rozporządzenie eIDAS były w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku,

				możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
90.	Art. 7	Związek Przedsiębiorstw Finansowych w Polsce	W naszej ocenie niezbędne jest jednoznaczne doprecyzowanie, jaka jest relacja europejskiego portfela tożsamości cyfrowej do wymogów właściwych dla procesów wymagających silnego uwierzytelniania klienta, jakie warunki techniczne i organizacyjne muszą zostać spełnione, aby portfel mógł być wykorzystywany w takich procesach, oraz jaki jest zakres odpowiedzialności poszczególnych uczestników tego modelu.	**Uwaga wyjaśniona** Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje - zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Strona ufająca otrzyma potwierdzenie tożsamości na wysokim poziomie bezpieczeństwa wraz danymi identyfikującymi osobę i/lub dodatkowymi danymi z elektronicznego poświadczenie atrybutów i będzie musiał to obowiązkowo uznać wprost na podstawie art. 5f ust. 2 rozporządzenia eIDAS. Wprost z przepisów art. 5f ust. 2 rozporządzenia eIDAS wynika, że w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, oraz wyłącznie na dobrowolny wniosek użytkownika, również akceptują europejskie portfele tożsamości cyfrowej.
91.	Uzasadnienie	Związek Banków Polski (ZBP)	W uzasadnieniu projektu ustawy wskazano, że użytkownik portfela będzie mógł powiadomić organ ochrony danych o każdym nieuzasadnionym żądaniu danych przez stronę ufającą. W jaki sposób ma wyglądać takie powiadomienie kierowane do UODO oraz jakie skutki prawne będzie ono wywoływało?	**Uwaga wyjaśniona** Usługa zostanie zaprojektowana w sposób wskazany w przepisach wykonawczych do art. 5a rozporządzenia eIDAS. Zakłada się, że mogłoby mieć to skutek tożsamy lub zbliżony jak złożenie skargi do organu nadzorczego.
92.	Uzasadnienie	Związek Banków Polski (ZBP)	W uzasadnieniu do ustawy wskazano, że zestaw metadanych odnoszących się do wydawanego zestawu danych identyfikujących osobę obejmuje trzy elementy obowiązkowe (wynikające z rozporządzenia 2024/2977) oraz jeden opcjonalny: datę i godzinę wygaśnięcia ważności danych identyfikujących osobę, nazwę organu wydającego dane identyfikujące osobę (w przypadku portfela zapewnianego przez ministra właściwego ds. informatyzacji – ten minister), dwuznakowy kod ISO 3166-1 dla RP, numer danych identyfikujących osobę nadany przez dostawcę danych	**Uwaga wyjaśniona** Taki numer zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE.

			identyfikujących osobę (element opcjonalny). W praktyce numer danych identyfikujących osobę może pełnić funkcję zbliżoną do numeru dokumentu mObywatel nadawanego po ustaleniu tożsamości użytkownika. Czy można interpretować to w ten sposób, że numer danych identyfikujących osobę miałby być odpowiednikiem serii i numeru dokumentu tożsamości w rozumieniu art. 36 ustawy AML?	L. z 2024 r. poz. 2977) może, ale nie musi być nadawany. W Polsce zakłada się, że będzie nadawany. Wydaje się, odpowiedź na pytanie, czy numer ten może mieć znaczenie w bankowych procedurach, leży w kompetencjach banków.
93.	Uzasadnienie (str. 6)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Należy się zgodzić, że utrzymanie dwóch rozwiązań jest ekonomicznie, technicznie i logicznie nieuzasadnione. Tym niemniej oczywiste jest również, że niezbędny będzie okres przejściowy obecnie niemożliwy do precyzyjnego zaplanowania właśnie z uwagi na sukces jakim stała się aplikacja mObywatel. Mając na uwadze, że w tym przypadku nie mamy do czynienia z nowymi funkcjonalnościami istniejącego rozwiązania, tylko zastąpienie go nowym, opierającym się o inne struktury danych i inne interfejsy i co za tym idzie wymagającym nie tylko gruntownej przebudowy samej aplikacji mObywatel, ale także systemów po stronie podmiotów ufających aplikacji mObywatel w obecnej wersji - celem dostosowania do wymogów europejskiego portfela tożsamości cyfrowej - oparcie takiej zmiany o komunikat ministra właściwego do spraw informatyzacji wydaje się niewystarczające. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
94.	Uzasadnienie (str. 11 i str. 25)	Związek Banków Polski (ZBP)	W uzasadnieniu projektu ustawy (str. 11 akapit 2 oraz str. 25 akapit 2) opisano możliwość zgłaszania naruszeń do UODO bezpośrednio z poziomu aplikacji. W jaki sposób zostanie zaprojektowana ta usługa? Czy planowane jest wprowadzenie formularza wymagającego opisania problemu, czy też będzie to rozwiązanie w postaci uproszczonego „przycisku” do zgłoszenia skargi?	**Uwaga wyjaśniona** Usługa zostanie zaprojektowana w sposób wskazany w przepisach wykonawczych do art. 5a rozporządzenia eIDAS. Zakłada się, że mogłoby mieć to skutek tożsamy lub zbliżony jak złożenie skargi do organu nadzorczego.

95.	Uzasadnienie (str. 11)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Co do zasady, wprost na podstawie art. 5b ust. 5 rozporządzenia eIDAS dane rejestru stron ufających będą publicznie dostępne. Taki dostęp, zgodnie z art. 3 ust. 5 rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848) będzie możliwy za pośrednictwem jednego wspólnego interfejsu programowania aplikacji ("API") zgodnie ze wspólnymi wymogami dla jednego API określonymi w pkt 1 załącznika II do ww. rozporządzenia.
96.	Uzasadnienie (str. 11)	Związek Banków Polski (ZBP)	W uzasadnieniu do projektu ustawy (str. 11) wskazano możliwość zgłaszania przez użytkowników portfela nadużyć w zakresie ochrony danych osobowych bezpośrednio do organu ochrony danych osobowych. Czy przewidywana jest analiza potencjalnych skutków takiego rozwiązania, w szczególności: a) ryzyka masowego napływu zgłoszeń do organu nadzorczego; b) ryzyka mechanicznego akceptowania zgłoszeń przez użytkowników w sposób analogiczny do zgód na cookies; c) potrzeby prowadzenia działań edukacyjnych wśród obywateli dotyczących znaczenia takich zgłoszeń.	**Uwaga wyjaśniona** Działania edukacyjne związane z wdrożeniem portfela będą obejmowały również wskazane kwestie, jeżeli będzie taka potrzeba. Obowiązek zapewnienia użytkownikom europejskich portfeli tożsamości cyfrowych wygodnej usługi zgłaszania naruszeń ochrony danych osobowych przez strony ufające organowi nadzorczemu wynika wprost z art. 5a ust. 4 lit. d pkt (iii) oraz ust. 5 lit. a pkt (x) rozporządzenia eIDAS.
97.	Uzasadnienie (str. 14)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** Termin wejścia życie przepisu art. 45e ust. 1 rozporządzenia eIDAS jest jasny (24 miesiące od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6) czyli 24 grudnia 2026 r. Planowane wejście w życie przepisów krajowych zbiega się z tym terminem. Udostępnienie pojedynczego punktu weryfikacji atrybutów wymienionych w załączniku VI o czym mowa w art. 9 ust. 1 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r.

			imieniu podmiotów odpowiedzialnych za źródła autentyczne. Podejście takie umożliwi szybsze i sprawniejsze tworzenie.	poz. 1569 z późn. zm.) jest to rozwiązanie możliwe, ale nie obowiązkowe. Projektodawca nie widzi zatem żadnej sprzeczności ani zagrożenia, że obywatele mogą nie otrzymywać poświadczeń atrybutów w podobnym tempie jak w innych krajach UE. Nawet gdyby ustawodawca zdecydował o utworzeniu pojedynczego punktu weryfikacji atrybutów wymienionych w załączniku VI do rozporządzenia eIDAS, to nie znaczy, że przełożyłoby się to na przyspieszenie udostępnienia źródeł autentycznych. Odrębnego wyjaśnienia wymaga postulat dodania możliwości wydawania atestacji [elektronicznych poświadczeń atrybutów] w imieniu podmiotów odpowiedzialnych za źródła autentyczne. Taką możliwość przewiduje nowy projektowany przepis art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej wskazujący, że minister właściwy do spraw informatyzacji może wydawać elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, w imieniu podmiotów odpowiedzialnych za źródła autentyczne. Należy nadmienić, że zgodnie z definicją zawartą w art. 3 pkt 46 rozporządzenia eIDAS tylko podmiot sektora publicznego może być upoważniony do wydawania poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne. Z uwagi na to, że minister właściwy do spraw informatyzacji zapewnia aplikację mObywatel, w ramach której zapewniane są dokumenty mobilne zawierające dane pozyskiwane ze źródeł autentycznych w rozumieniu rozporządzenia eIDAS, wskazanie tego ministra jako podmiotu publicznego upoważnionego do wydawania poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne jest oczywistym wyborem.
98.	Uzasadnienie (str. 14)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie	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	**Uwaga wyjaśniona** Zgodnie z nowym projektowanym przepisem art. 22 ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej podmioty publiczne odpowiedzialne na

		Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	poziomie krajowym za źródła autentyczne, o których mowa w załączniku VI do rozporządzenia 910/2014, zapewniają kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z art. 45e ust. 1 rozporządzenia 910/2014. Przepis jest jednoznaczny i jest zobowiązujący. Czym innym jest możliwość wydawania elektronicznych poświadczeń atrybutów przez podmioty publiczne odpowiedzialne za źródła autentyczne. W tym przypadku jest to możliwość wynikająca z art. 3 pkt 46 i art. 45f rozporządzenia eIDAS. Celowo nie planuje się narzucenia obowiązku wydawania elektronicznych poświadczeń atrybutów przez podmioty publiczne odpowiedzialne za źródła autentyczne.
99.	Uzasadnienie (str. 15)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Co do zasady elektroniczne poświadczenia atrybutów mogą być wydawane przez kwalifikowanych dostawców usług zaufania. Żadne przepisy projektowanej ustawy, jak również wskazany fragment uzasadnienia nie zakazują tej możliwości.
100.	Uzasadnienie (str. 20-21)	Związek Banków Polski (ZBP)	W uzasadnieniu do projektu ustawy (str. 20–21) wskazano, że cyfrowy portfel będzie zapewniany w węźle krajowym. Czy wykorzystanie portfela jako środka uwierzytelniającego użytkownika za pośrednictwem węzła krajowego oraz w zakresie danych jak obecnie będzie wymagało rejestracji podmiotu jako strony ufającej, czy też stroną ufającą będzie wyłącznie minister właściwy do spraw informatyzacji?	**Uwaga wyjaśniona** Portfel będzie przyłączony do węzła krajowego identyfikacji elektronicznej w zakresie, w jakim stanowi on środek identyfikacji elektronicznej i w tym względzie nie będzie konieczna ponowna integracja usługodawców z węzłem krajowym identyfikacji elektronicznej. Założenie jest takie, aby usługa wykorzystująca portfel jako środek identyfikacji elektronicznej przyłączony do węzła krajowego identyfikacji elektronicznej była usługą ministra właściwego do spraw informatyzacji - gdyż to minister zgodnie z ustawą zapewnia w tym przypadku

				uwierzytelnianie. Jednakże podmioty świadczące usługi online przyłączone do węzła krajowego identyfikacji elektronicznej będą zobligowane do zintegrowania się z systemem dopasowywania tożsamości. Posługiwanie się elektronicznymi poświadczeniami atrybutów przez węzeł krajowego identyfikacji elektronicznej nie będzie jednak możliwe. Aby w pełni korzystać z wszystkich funkcjonalności portfela trzeba będzie przejść bezpośrednią integrację poprzez rejestr stron ufających.
101.	Uzasadnienie (str. 21)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** Z pewnością nie będą tworzone usługi online wykorzystujące środki identyfikacji elektronicznej osoby prawnej, jeżeli nie będą dostępne takie środki. Najpierw należy udostępnić narzędzie, aby potem można było tworzyć w oparciu o nie nowe usługi.
102.	Uzasadnienie (str. 22)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	Uzasadnienie str. 22 Następująca treść W ramach projektowanych przepisów określono sposób potwierdzania tożsamości przed rejestracją użytkownika europejskiego portfela tożsamości cyfrowej, zapewnianego przez ministra właściwego do spraw informatyzacji. Przewidziano trzy podstawowe sposoby potwierdzania tożsamości. 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?	**Uwaga wyjaśniona/częściowo uwzględniona** Art. 14b ust. 1 pkt 2 został zmieniony. Zgodnie z art. 5a ust. 24 rozporządzenia eIDAS: „Komisja, w drodze aktów wykonawczych, sporządza wykaz norm referencyjnych oraz, w razie potrzeby, ustanawia specyfikacje i procedury w celu ułatwienia rejestracji użytkowników w europejskim portfelu tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych z wysokim poziomem bezpieczeństwa albo środków identyfikacji

				elektronicznej zgodnych ze średnim poziomem bezpieczeństwa, w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełniają wymogi dotyczące wysokiego poziomu bezpieczeństwa". Weryfikacja tożsamości przed wydaniem kwalifikowanego certyfikatu podpisu elektronicznego i weryfikacja tożsamości przed wydaniem europejskiego portfela tożsamości cyfrowej, to nie są tożsame procedury. W Polsce jedynym dostępnym środkiem identyfikacji elektronicznej, którego poziom bezpieczeństwa jest notyfikowany w Komisji Europejskiej na średnim poziomie bezpieczeństwa jest profil zaufany. Istotnie nie wyklucza to możliwości notyfikacji innego środka lub (jeżeli rozporządzenie wykonawcze Komisji wydane na podstawie art. 5a ust. 24 rozporządzenia eIDAS ostatecznie to umożliwi) potwierdzenia osiągania średniego poziomu bezpieczeństwa przez akredytowaną jednostkę oceniającą zgodność zdefiniowaną w artykule 2(13). Podsumowując, należy zgodzić się z tym, aby nie wymieniać wprost profilu zaufanego w ustawie jako jedynej możliwości, ale również konsekwentnie nie wskazywać innej konkretnej możliwości.
103.	Uzasadnienie (str. 24)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** Inicjatywy, aby co do zasady w celu jednoznacznej identyfikacji osoby fizycznej zrezygnować z numeru PESEL jako unikatowego numeru jednoznacznie identyfikującego osobę fizyczną wpisaną do ewidencji ludności i zastąpić go innym identyfikatorem, który nie będzie zawierał daty urodzenia i oznaczenia płci albo zbiorem danych jednoznacznie identyfikujących osobę fizyczną były już przedkładane, ale nie doprowadziły do zmian w tym zakresie. Zadaniem projektodawcy celem tej ustawy nie powinna być realizacja takich postulatów. W tym kontekście warto podkreślić, że w przypadku rezygnacji z unikatowego identyfikatora osoby fizycznej i posługiwania się zamiast nim zestawem danych jednoznacznie identyfikujących osobę fizyczną nie

			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	wystarczy nawet obowiązkowy zestaw danych wskazany w tabeli 1 załącznika do rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977), czyli imię + nazwisko + data urodzenia + miejsce urodzenia + obywatelstwo. Taki zestaw nie daje bowiem całkowitej pewności, że nie ma więcej niż jednak osoby, którą takie dane określają. Gdyby tak było, to istotnie można byłoby zrezygnować z nadawania unikatowych identyfikatorów jednoznacznie identyfikujących osobą fizyczną na rzecz pakietów danych. Do ww. pakietu danych niezbędny jest dodatkowy atrybut. Znaczy to, że w praktyce w celu uniknięcia przetwarzania unikatowego numeru identyfikującego osobę fizyczną łącznie może być przetwarzany większy zestaw danych, który wszak i tak musi zapewnić niepowtarzalną identyfikację. Nie jest jednoznacznie udowodnione, że posługiwanie się szerszym zestawem danych jest lepsze dla obywateli od przetwarzania mniejszego zestawu danych, ale zawierającego niepowtarzalny identyfikator. Przykładowo zgodnie z art. 296 ust. pkt 1 ustawy Prawo komunikacji elektronicznej wystarczy podanie przez abonenta dostawy usług telekomunikacyjnych imienia (imion) i nazwisko i numeru PESEL. Nie ma potrzeby podawania większej ilości danych. Jednak w przypadku zamiast PESEL przekazywana byłaby kolekcja atrybutów jednoznacznie identyfikujących osobę fizyczną, niezawierająca numeru PESEL to zestaw danych przekazywanych dostawcy usług telekomunikacyjnych musiałby być znacząco szerszy. W efekcie niewątpliwie wpłynęłoby to na konieczność przebudowy systemów publicznych celem dostosowanie ich do innego sposobu identyfikacji użytkowników. Dlatego też tego rodzaju inicjatywa (choć interesująca) wymagałaby odrębnego projektu i odrębnej dyskusji w

				szczególności wymagającej kampanii wyjaśniającej ewentualne skutki rezygnacji z przetwarzania nr PESEL na rzecz innego identyfikatora lub klucza w tym też badania opinii publicznej i nie powinna być realizowana przy okazji przepisów wdrażających rozporządzenie eIDAS.
104.	Uzasadnienie (str. 26)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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 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. 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.	**Uwaga wyjaśniona** Nie można zgodzić się, że wizerunek twarzy użytkownika portfela jako element krajowego zestawu danych identyfikujących osobę doprowadzi do tworzenia procesów, które będą zawsze wymagały wizerunku. Jak to podkreślono w uzasadnieniu, chodzi o potwierdzenie danych podczas obecności fizycznej. Nie ma powodu, aby w usługach online żądać wizerunku użytkownika a tworzenie takich usług będzie praktycznie niemożliwe z uwagi na to, że dane rejestru stron ufających w tym wskazanie danych, o które strona ufająca będzie zwracać się do użytkowników, zgodnie z przepisem art. 5b ust. 2 lit. c, będą publicznie dostępne. Zatem gdyby nawet strona ufająca wpisała bezpodstawnie do rejestru stron ufających, że będzie się zwracać do użytkowników o udostepnienie wizerunku, to Prezes Urzędu Ochrony Danych Osobowych bardzo szybko zostanie o tym poinformowany przez użytkowników portfeli, będzie to mógł zweryfikować w rejestrze i podjąć stosowne działania. Zakłada się zatem, że powstanie samoregulujący się system i strony ufające same będą się cenzurowały czy nie żądają nadmiernej liczby danych.
105.	Uzasadnienie (str. 31)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** W uwadze przywoływany jest nieistniejący projekt „Rozporządzenia o portfelu osoby prawnej”. Jeżeli w uwadze chodzi o procedowany obecnie projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia Europejskich Portfeli Biznesowych, to w ramach tego projektu planuje się zmianę art. 5a rozporządzenia eIDAS w celu zagwarantowania, aby obowiązkowe wydawanie

			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.	europejskich portfeli tożsamości cyfrowej dotyczyło wyłącznie osób fizycznych. Znaczy to, że w przypadku uchwalenia przepisów w sprawie ustanowienia Europejskich Portfeli Biznesowych wydawanie europejskich portfeli tożsamości cyfrowej dla osób prawnych może nie tylko nie być obowiązkowe, ale również stracić sens. Jeżeli jednak przepisy w sprawie ustanowienia Europejskich Portfeli Biznesowych nie wejdą w życie lub ich kształt zostanie na tyle zmieniony, że zapewnienie w Polsce europejskiego portfela tożsamości cyfrowej osobom prawnym będzie potrzebne, to i tak sposób wykonania tego wymogu będzie zależał od przepisów krajowych. W tym zakresie ograniczenie możliwości uzyskania europejskiego portfela tożsamości cyfrowej tylko do osób posługujących się wydanym w kraju europejskim portfelem tożsamości cyfrowej osoby fizycznej jest uzasadnione prostotą takiego rozwiązania. Postulowana komplikacja systemu polegająca na powiązaniu wydawanego w kraju przez ministra właściwego do spraw informatyzacji europejskiego portfela tożsamości cyfrowej osoby prawnej z europejskim portfelem tożsamości cyfrowej osoby fizycznej wydawanym w innym kraju UE nie uzasadnia potencjalnych korzyści, jakie mogliby uzyskać w Polsce mieszkańcy innych krajów UE posługujący się portfelami tożsamości cyfrowej wydawanymi przez te kraje. Podobne wyjaśnienie dotyczy postulowanej rejestracji użytkowników europejskiego portfela tożsamości cyfrowej osoby prawnej za pomocą innych krajowych środków identyfikacji elektronicznej (np. profilu osobistego). Nie ma potrzeby komplikowania systemu skoro powiązanie pomiędzy środkiem identyfikacji elektronicznej osoby fizycznej i osoby prawnej w przypadku portfela tożsamości cyfrowej można zrealizować w prosty sposób. Warto przy tym nadmienić, że w planowanych wstępnie rozwiązaniach dla Europejskich Portfeli Biznesowych zarówno właściciele tych portfeli (czyli osoby prawne),

				jak i osoby fizyczne będące końcowymi użytkownikami tych portfeli mający określony ograniczony zakres pełnomocnictw będą się posługiwali elektronicznymi poświadczeniami atrybutów odpowiednio powiązanymi z tą samą jednostką portfela.
106.	Uzasadnienie (str. 32)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** Mając na uwadze, że planowane rozporządzenie w sprawie Europejskich Portfeli Biznesowych może w ogóle podważyć konieczność, a za co za tym idzie i sens wydawania europejskiego portfela tożsamości cyfrowej dla osoby prawnej, proponuje się rozwiązanie najprostsze, czyli poleganie na tej samej instancji portfel, jaka będzie zapewniana osobom fizycznym w celu korzystania przez taką osobę z portfela będącego środkiem identyfikacji elektronicznej osoby fizycznej. Ułatwi to powiązanie środka identyfikacji osoby prawnej (jakim będzie w szczególności taki portfel) ze środkiem identyfikacji osoby fizycznej. Jednocześnie planowane jest długie vacatio legis dla tych przepisów. Nie można jednak pominąć obowiązku zapewnienia europejskiego portfela tożsamości cyfrowej osobom prawnym, ponieważ wynika on wprost z art. 5a ust. 1 rozporządzenia eIDAS i dopóty dopóki nie zostanie on wyłączony ewentualnym rozporządzeniem w sprawie Europejskich Portfeli Biznesowych wymaga określonych formalnych działań. Nawet wielokrotnie powtarzane intencje Komisji Europejskiej nie są prawem i nie wyłączają obowiązku, o którym mowa w art. 5a ust. 1 rozporządzenia eIDAS.

			biznesowego 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.”	
107.	Uzasadnienie (str. 33)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga wyjaśniona** Uwaga bardzo ogólnie odnosi się do zacytowanego fragmentu uzasadnienia ani nie odnosi się do jakiegokolwiek fragmentu projektowanych przepisów. Odnosząc się jednak do pytania „po co Skarb Państwa ma utrzymywać 3 równoległe rozwiązania podpisu elektronicznego w Polsce”, wyjaśnienie jest następujące: - podpis zaufany jest doskonale znanym i powszechnie używanym narzędziem (ponad 14,3 miliona użytkowników profilu zaufanego w dniu 24 marca 2026) umożliwiającym wygodne nieodpłatne podpisywanie podań i wniosków kierowanych do podmiotów publicznych, - podpis osobisty jest wydawany wraz dowodem osobistym każdemu chętnemu obywatelowi w celu zapewnienia nieodpłatnego podpisu elektronicznego w interakcjach nie tylko z podmiotami publicznymi, ale również w stosunkach cywilnoprawnych, - inne rodzaje podpisów o jakie być może chodzi mają skutek prawny ograniczony tylko do wykorzystania w określonych systemach publicznych - np. podpis elektroniczny wersyfikowany certyfikatem umożliwiającym podpisywanie dokumentów elektronicznych z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym Zakładu Ubezpieczeń Społecznych znajduje zastosowanie tylko w systemie ZUS oraz do podpisywania zwolnień lekarskich skierowań i recept przez osoby wykonujące zawód medyczny. Mając na uwadze, że wskazane rozwiązania są darmowe dla ich użytkowników należy przyjąć założenie, że nie

				jest możliwe wprowadzenie w przyszłości opłat za ich użytkowanie. Znaczy to również, że ewentualne zastąpienie takich podpisów wyłącznie kwalifikowanymi podpisami elektronicznymi wymagałoby zapewnienia przez Skarb Państwa takiego alternatywnego rozwiązania również za darmo.
108.	OSR	Konfederacja Lewiatan	Optymalizacja kosztów wdrożenia i utrzymania Zgodnie z art. 10 projektu ustawy, limit wydatków z budżetu państwa na realizację zadania będzie systematycznie rósł - od 45,50 mln zł w 2026 r. aż do 84,11 mln zł w 2035 r. Utrzymanie i rozwój jednego ekosystemu opartego o kod i architekturę mObywatela (który ma już za sobą fazę kosztownego wdrożenia) pozwoli na znaczące obniżenie i zoptymalizowanie długofalowych kosztów wskazanych w projekcie. Podział środków na rozwój mObywatela i odrębnego oprogramowania portfela stanowi ryzyko zarzutów o niegospodarno	**Uwaga wyjaśniona** Rozwijanie architektury portfela wynika z przepisów rozporządzenia eIDAS i aktów wykonawczych. Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). W szczególności muszą obsługiwać dane identyfikujące osobę i elektroniczne poświadczenie atrybutów wydawane w formatach danych ISO/IEC.18013-5:2021 oraz Verifiable Credentials Data Model 1.1 umożliwiających selektywne udostępnianie danych. Ponadto muszą rozpoznawać i odpowiednio interpretować certyfikaty dostępu i certyfikaty rejestracji stron ufających portfela, 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 portfela (Dz. U. UE. L. z 2025 r. poz. 848). Istotne znaczenie ma również poziom bezpieczeństwa identyfikacji elektronicznej jaki ma zapewniać portfel (wysoki) a poziom bezpieczeństwa jaki zapewnia obecnie aplikacja mObywatel (średni). Z przepisów szczegółowych wynika wiele innych wymogów wymagających przygotowania architektury portfela.

109.	OSR	Związek Banków Polski (ZBP)	Dlaczego w ocenie skutków regulacji (OSR) nie została przedstawiona analiza kosztów wdrożenia nowych rozwiązań dla sektora prywatnego, w tym dla banków?	**Uwaga wyjaśniona** Niemożliwym byłoby ujęcia każdego sektora oddzielnie w OSR z uwagi na kompleksowy charakter ustawy.
110.	OSR (str. 8)	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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 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 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.	**Uwaga nieuwzględniona** Wyłączanie zawierania umów konsumenckich z nieprofesjonalnego użycia będzie niezrozumiałe dla użytkowników, którzy będą (przypuszczalnie skutecznie) dowodzić, że z ich strony zawarcie umowy konsumenckiej w celach prywatnych (niezwiązanych bezpośrednio z działalnością zawodową czy gospodarczą) jest całkowicie pozbawione cech działalności profesjonalnej z ich strony.
111.	Przepisy ogólne dot. logów systemowych	IDENTT Sp. z o.o.	Retencja logów a prywatność użytkowników. Projekt zakłada przechowywanie informacji o użyciu środków identyfikacji elektronicznej w logach systemowych. Zbyt długi okres retencji takich danych stwarza techniczne możliwości profilowania aktywności cyfrowej obywatela i jest niezgodny z zasadą minimalizacji przetwarzanych danych. Propozycja zmiany: Rozważenie wycofania tych założeń lub znaczące skrócenie	**Uwaga wyjaśniona** Przyjęto okres retencji jak dla wszelkich systemów w KRI - 2 lata.

			okresu retencji logów. Wprowadzenie mechanizmów bezwzględnej anonimizacji logów po upływie określonego czasu oraz jednoznaczne, ustawowe określenie celów ich przetwarzania.	
112.	Przepisy określające weryfikację tożsamości	IDENTT Sp. z o.o.	Wideoweryfikacja w procesie onboardingu. Brakuje jasnych zapisów wskazujących na to, czy wideoweryfikacja będzie w pełni legalną i akceptowalną formą potwierdzania tożsamości w trakcie onboardingu. Propozycja zmiany: Zaproponowanie i uwzględnienie w ustawie bezpośredniego odwołania do art. 3 normy 461 (ETSI TS 119 461), aby jednoznacznie usankcjonować wykorzystanie tej technologii.	**Uwaga wyjaśniona** Wyznaczenie dopuszczalnych metod zdalnej rejestracji użytkowników w europejskim portfelu tożsamości cyfrowej jest kompetencją Komisji Europejskiej. Szczegółowe wymagania techniczne w tym zakresie znajdują się w rozporządzeniu wykonawczym Komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi wysokiego poziomu bezpieczeństwa.
113.	Przepisy wprowadzające / przejściowe	IDENTT Sp. z o.o.	Brak vacatio legis dla rynku i biznesu. Brak określonych ram czasowych, procedur i odpowiedniego okresu przejściowego. Jeśli nowe poświadczenia atrybutów mają być traktowane na równi z dokumentami publicznymi, firmy potrzebują czasu na wdrożenie zmian technicznych. Propozycja zmiany: Zdefiniowanie i udostępnienie jasnych procedur oraz odpowiednich terminów adaptacyjnych, umożliwiających podmiotom rynkowym przygotowanie systemów do obsługi nowych poświadczeń	**Uwaga wyjaśniona** Zarówno obowiązek polegania na europejskim portfelu tożsamości cyfrowej (zob. art 5f rozporządzenia eIDAS), jak i zrównanie niektórych rodzajów elektronicznych poświadczeń atrybutów z poświadczeniami wydanymi zgodnie z prawem w postaci papierowej (zob. art. 45b ust. 2 rozporządzenia eIDAS) wynika wprost z przepisów unijnych , nie z przepisów ustawowych.
114.	Przepisy wprowadzające i zwalczanie prania pieniędzy (AML)	IDENTT Sp. z o.o.	Niejasny status prawny portfela wobec innych regulacji. Nie zdefiniowano wyraźnie, czy europejski portfel tożsamości cyfrowej będzie miał takie samo znaczenie prawne jak fizyczny dokument tożsamości. Rodzi to problemy w przypadku procesów objętych rygorystycznymi wymogami (np. procedury AML), które wymagają pobrania numeru dokumentu, co w przypadku EUDI Wallet jest niemożliwe. Brak wskazania, w jakich przypadkach instytucje mają bezwzględny obowiązek uznawać portfel, a kiedy jest to wykluczone. Propozycja zmiany: Wprowadzenie zapisów gwarantujących jednoznaczne zdefiniowanie przypadków wykorzystania EUDI Wallet w procesach identyfikacji oraz precyzyjne określenie wykluczeń i przypadków, w których jego uznanie nie będzie obowiązkowe. Dodanie elementów adresujących istniejące luki prawne w kontekście powiązanych wymogów sektorowych (np. wdrożenie mechanizmów zgodnych z AML).	**Uwaga wyjaśniona/uwzględniona** W projektowanej ustawie przyjęto rozwiązanie analogiczne jak w przypadku mDowodu, tzn. obowiązek akceptowania portfela (zestawu danych identyfikujących osobę) do celów stwierdzania tożsamości i obywatelstwa w warunkach fizycznej obecności stron. W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d.

115.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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 [więcej niż jednej listy zaufanej] Dodać nowy artykuł w art. 1 zmieniającym UoUZoIE Zmiana art. 2 pkt 2 „zaufane listy”	**Uwaga uwzględniona** Art. 2 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej został zmieniony.
116.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga nieuwzględniona** Z rozporządzania eIDAS nie wynika konieczność utrzymywania krajowych list innych niż zaufane listy, o których mowa w art. 22 rozporządzenia eIDAS. Dostawcy portfela, podmioty wydające PID, podmioty wydające certyfikaty stron ufających będą zgłaszane bezpośrednio do Komisji Europejskiej.
117.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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	**Uwaga częściowo uwzględniona** Należy się zgodzić, że potrzebna jest ewidencja atrybutów i schematów atrybutów ustanowionych na poziomie krajowym (zob. uznanie innych uwag w tej sprawie), ale nie z tym, że jest to element krajowej infrastruktury zaufania w rozumieniu art. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej. W art. 1 ust. 9 dodano przepis, który wprowadza krajowy katalog schematów elektronicznych poświadczeń atrybutów.
118.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga uwzględniona** Została wprowadzona stosowna zmiana w art. 3 ust. 4 ustawy o usługach zaufania oraz identyfikacji elektronicznej.

			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).”	
119.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania zostały zaproponowane zmiany w całym rozdziale 2 ustawy.
120.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga uwzględniona** Zaproponowana została zmiana w art. 5 ust. 2.
121.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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	**Uwaga uwzględniona** W związku z uwzględnieniem licznych uwag różnych podmiotów dotyczących niekwalifikowanych usług zaufania zostały zaproponowane zmiany w całym rozdziale 2 ustawy.

			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.	
122.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Przepisy art. 19a rozporządzenia eIDAS oraz rozporządzenie wykonawcze Komisji (UE) 2025/2160 z dnia 27 października 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych, specyfikacji i procedur dotyczących zarządzania ryzykiem związanym ze świadczeniem niekwalifikowanych usług zaufania (Dz. U. UE. L. z 2025 r. poz. 2160) obowiązują bezpośrednio i nie ma potrzeby wpisywania odniesienia do nich.
123.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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 autentyczne lub w jego imieniu stanowią część infrastruktury zaufania określonej w art. 2 ustawy UZoIE	**Uwaga wyjaśniona** Zgodnie z art. 6 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r. poz. 1569 z późn. zm.) Komisja ustanawia, prowadzi i publikuje wykaz dostawców elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu na podstawie informacji przekazanych przez państwa członkowskie zgodnie z art. 5.

124.	Brak w projekcie	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Przepisy art. 19a rozporządzenia eIDAS oraz rozporządzenie wykonawcze Komisji (UE) 2025/2160 z dnia 27 października 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych, specyfikacji i procedur dotyczących zarządzania ryzykiem związanym ze świadczeniem niekwalifikowanych usług zaufania (Dz. U. UE. L. z 2025 r. poz. 2160) obowiązują bezpośrednio. Zgodnie z art. 4 ust. 6 tego rozporządzenia „Niekwalifikowani dostawcy usług zaufania dokonują przeglądu wyników oceny ryzyka i planu postępowania z ryzykiem w zaplanowanych odstępach czasu, a co najmniej raz w roku, a także w przypadku wystąpienia istotnych zmian w infrastrukturze, operacjach lub ryzyku lub w przypadku poważnych incydentów, a także dokumentują i - w stosownych przypadkach - aktualizują te wyniki i plany.” Ponadto do projektu zostaną dopisane (brakujące obecnie) zaktualizowane przepisy dotyczące kar administracyjnych o których mowa a art. 16 eIDAS i które powinny dotyczyć również niekwalifikowanych dostawców usług zaufania. Mając na uwadze że kary muszę być skuteczne, proporcjonalne i odstraszające nie ma powodu aby żądać składania raportu.
125.	Uwaga ogólna	Konfederacja Lewiatan	Zgodność z wymogami Silnego Uwierzytelniania Klienta (SCA) Brak jasności, czy mObywatel/EPTC będzie spełniał wymogi SCA w kontekście transakcji płatniczych i dostępu do rachunków (PSD2/PSD3)	**Uwag wyjaśniona** Wymóg ten jest inaczej ustanowiony. To nie portfele mają zapewnić zgodność z SCA, tylko tam, gdzie się wymaga SCA portfele mają być akceptowane. Wprost z przepisów art. 5f ust 2 rozporządzenia eIDAS wynika, że w przypadku, gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, oraz wyłącznie na dobrowolny wniosek użytkownika, również akceptują europejskie portfele tożsamości cyfrowej. Znaczy to, że wprost z rozporządzenia wynika, że każdy portfel spełnia

				wymogi SCA. Można to również ustalić analizując przepisy dotyczące wymogów dla środków identyfikacji elektronicznej zapewniających wysoki poziom bezpieczeństwa oraz certyfikacji portfeli.
126.	Uwaga ogólna	Konfederacja Lewiatan	Ryzyko selektywnego udostępniania danych przez klienta Proponowany mechanizm „selektywnego udostępniania” pomimo, że jest korzystny dla zarządzania prywatnością klientów, może stanowić barierę operacyjną dla instytucji finansowych, z uwagi na otrzymywanie niekompletnych danych klientów. Mechanizm powinien umożliwiać „Stronie Ufającej” (instytucji) wymuszenie konkretnego profilu danych (pakietu), który będzie niezbędny do zawarcia umowy lub przeprowadzenia transakcji. Klient powinien mieć wybór w postaci „udostępnienia wszystkich danych, które są wymagane ustawowo” albo „rezygnacji z usługi”, zamiast możliwości wysłania "niepełnego" formularza lub ograniczania zakresu zgód na przetwarzanie danych na określone cele.	**Uwaga wyjaśniona** W związku z przepisami dotyczącymi rejestracji w rejestrze stron ufających, w tym wskazywania zakresu danych dla każdej usługi, jak również propozycji polegania na certyfikatach rejestracji strony ufającej portfele tożsamości cyfrowej automatycznie rozpoznają zakres danych, jaki jest wymagany dla określonej usługi wskazane zagrożenie nie wydaje się istotne. Użytkownicy z pewności szybko się nauczą możliwości, jakie daje im portfel.
127.	Uwaga ogólna	Konfederacja Lewiatan	Intuicyjność dla obywatela (user experience) Obywatele przywykli już do korzystania z państwowej aplikacji mObywatel jako cyfrowego medium dla dokumentów i poświadczania tożsamości. Wprowadzenie drugiego narzędzia (lub modułu na tyle odrębnego, że w ustawie nazywa się go odrębnym „rozwiązaniem”) wywoła dezorientację. Użytkownik nie powinien zastanawiać się, czy w danym momencie (np. w urzędzie czy podczas podpisywania dokumentu) ma użyć mObywatela czy europejskiego portfela tożsamości. Z perspektywy obywatela powinna istnieć jedna aplikacja, w której aktywacja "trybu europejskiego" (zgodnego z wymogami rozporządzenia eIDAS 2.0 i certyfikacją eIDAS) następuje wewnątrz aplikacji, w sposób dla niego niewidoczny.	**Uwaga wyjaśniona** Przykładowymi nowymi elementami, których obecnie aplikacja mObywatel nie zapewnia, a są wymagane przepisami rozporządzenia eIDAS i aktami wykonawczymi są: - elektroniczne poświadczenia atrybutów, które mogą być wydawane przez kwalifikowanych dostawców usług zaufania, bezpośrednio przez podmiotu odpowiedzialne za źródła autentyczne oraz przez ministra właściwego do spraw informatyzacji (dokumenty mobilne do aplikacji mObywatel użytkownik pobierał sam); - każdorazowe informowanie użytkownika portfela o stronie ufającej i zakresie danych, jaki zostanie jej przekazany (bez względu czy jest to dostawca usługi online czy poświadczeń atrybutów czy np. podpisu elektronicznego); - selektywne udostępnianie wybranych elementów danych; - panel zarządzania umożliwiający łatwe informowanie organu ochrony danych osobowych; - możliwość generowanie pseudonimów; - przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych; - łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO.

				Nie ma możliwości, aby te zmiany wprowadzić sposób niewidoczny. Tym niemniej dołożone zostaną wszelkie starania, aby zmiany, jakie wymusza rozporządzenie eIDAS były w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb.
128.	Uwaga ogólna	Konfederacja Lewiatan	Jednoznaczne określenie docelowego modelu integracji obu aplikacji Z analizy projektu wynika, że planowany europejski portfel tożsamości cyfrowej (EPTC) w wielu obszarach będzie powielał funkcjonalności już dostępne w aplikacji mObywatel. Równocześnie, jak wskazano w uzasadnieniu, aplikacja mObywatel i zapewniany w Polsce europejski portfel tożsamości cyfrowej będą stanowiły "całkowicie niezależne od siebie rozwiązania". Zauważono, że zapewnienie użytkownikom aplikacji mObywatel komfortowego przejścia do europejskiego portfela tożsamości cyfrowej będzie ogromnym wyzwaniem nie tylko techniczno-organizacyjnym, ale również informacyjnym - z uwagi na różnice pomiędzy wymogami systemów nie będzie możliwe oddanie użytkownikom do użytku europejskiego portfela tożsamości cyfrowej, który będzie zapewniał te same dokumenty mobilne co rodzimy "portfel" (zgodnie z wymogami rozporządzenia eIDAS w zakresie elektronicznego poświadczania atrybutów w określonym przepisami europejskimi formacie). Wskazano, że będzie to proces rozciągnięty w czasie, wymagający okresu przejściowego, w trakcie, którego będzie konieczne utrzymywanie obu aplikacji ze stopniowym przenoszeniem się użytkowników aplikacji mObywatel do aplikacji EPTC. W naszej ocenie rozwijanie całkowicie odrębnej architektury portfela nie znajduje pełnego uzasadnienia, biorąc pod uwagę istniejącą infrastrukturę mObywatela oraz wysoki poziom jego upowszechnienia wśród obywateli. Z tego względu pozytywnie oceniamy ogłoszone podczas konferencji prasowej deklaracje Ministerstwa Cyfryzacji wskazujące na to, że po etapie pilotażu europejskiego portfela i analizie jego wyników rozwiązanie to docelowo zostanie zintegrowane z ekosystemem mObywatela, tak aby użytkownicy mogli korzystać z usług i dokumentów cyfrowych w jednym środowisku. Jednocześnie postulujemy doprecyzowanie projektu ustawy w tym zakresie, tak aby jasno określić docelowy model integracji obu aplikacji i wskazać, że europejski portfel tożsamości cyfrowej znajdzie się w ekosystemie istniejącej już polskiej aplikacji. Obecnie treść uzasadnienia oraz publiczne wypowiedzi przedstawicieli administracji wskazują na różne kierunki rozwoju systemu, co może prowadzić do niejasności. Przykładowo, w komunikacji publicznej pojawiają się zapowiedzi włączenia europejskiego portfela do aplikacji mObywatel, podczas gdy z uzasadnienia projektu można wnioskować, że to funkcjonalności mObywatela będą stopniowo przenoszone do odrębnej aplikacji - europejskiego portfela.	**Uwaga wyjaśniona** Rozwijanie architektury portfela wynika z przepisów rozporządzenia eIDAS i aktów wykonawczych. Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). W szczególności muszą obsługiwać dane identyfikujące osobę i elektroniczne poświadczenie atrybutów wydawane w formatach danych ISO/IEC.18013-5:2021 oraz Verifiable Credentials Data Model 1.1 umożliwiających selektywne udostępnianie danych. Ponadto muszą rozpoznawać i odpowiednio interpretować certyfikaty dostępu i certyfikaty rejestracji stron ufających portfela, o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848). Istotne znaczenie ma również poziom bezpieczeństwa identyfikacji elektronicznej, jaki ma zapewniać portfel (wysoki) a poziom bezpieczeństwa jaki zapewnia obecnie aplikacja mObywatel (średni). Z przepisów szczegółowych wynika wiele innych wymogów wymagających przygotowania architektury portfela. Tym niemniej dołożone zostaną wszelkie starania, aby

				zmiany, jakie wymusza rozporządzenie eIDAS były w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
129.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Postulaty ZPP ● jednoznaczne określenie w ustawie i uzasadnieniu docelowego modelu integracji aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej, ● usunięcie z projektu podziału na dwa odrębne rozwiązania i przyjęcie modelu opartego na integracji funkcjonalnej w ramach ekosystemu mObywatela, ● dostosowanie projektu, w tym przepisów dotyczących ustawy o mObywatelu, tak aby aplikacja mogła zostać odpowiednio przystosowana technologicznie i uzyskać status certyfikowanego EPTC, ● zachowanie perspektywy obywatela jako użytkownika jednego, intuicyjnego środowiska usług cyfrowych państwa, ● korektę błędnego odesłania w projektowanym art. 22a ust. 2 pkt 2, ● uzupełnienie modelu danych albo doprecyzowanie projektu tak, aby portfel mógł lepiej odpowiadać na obowiązki AML/KYC, ● zapewnienie stronie ufającej możliwości żądania pełnego, ustawowo wymaganego pakietu danych w ramach mechanizmu selektywnego udostępniania, ● przyjęcie modelu wdrożenia, który będzie minimalizował koszty integracji, utrzymania i migracji po stronie przedsiębiorców oraz państwa, ● doprecyzowanie zgodności projektowanego rozwiązania z wymogami silnego uwierzytelniania klienta.	**Uwaga wyjaśniona/częściowo uwzględniona** Odnosząc się do zagadnienia modelu funkcjonowania europejskiego portfela tożsamości cyfrowej i aplikacji mObywatel wskazać należy, że europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem 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). Wszystkie te wymagania powodują, że użytkownicy będą musieli potwierdzić swoją tożsamość i uzyskać elektroniczne poświadczenia atrybutów - zamiast dokumentów mobilnych. Nie tylko dlatego, że w rozporządzeniu eIDAS wymagany jest inny sposób ich wydawania i unieważniania, ale przede wszystkim dlatego, że muszą mieć zasadniczą inną strukturę techniczną i co za tym idzie być inaczej zabezpieczone kryptograficznie. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności

				aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej. Odnosząc się do zagadnienia wprowadzenia regulacji dla sektorów regulowanych, szczególności w obszarze AML/KYC to zaproponowano rozwiązanie tego problemu przez zmianę art. 36 ust. 1 pkt 1 lit d w ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Jeżeli chodzi o zapewnienie stronie ufającej możliwości żądania pełnego, ustawowo wymaganego pakietu danych w ramach mechanizmu selektywnego udostępniania, to jest postulat sprzeczny wewnętrznie. Gdyby dowolna strona ufająca miała zagwarantowana możliwość wymagania pełnego pakietu danych, to byłoby to sprzeczne nie tylko z ideą selektywnego udostępniania danych, ale też niezgodne z ogólnymi zasadami przetwarzania danych osobowych. Należy zgodzić się z postulatem minimalizacji kosztów integracji, utrzymania i migracji po stronie przedsiębiorców oraz państwa. W art. 22a ust. 2 pkt 2 ustawy o usługach zaufania i identyfikacji elektronicznej poprawiono na odwołanie.
130.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Potrzebna jest jasność co do zgodności z wymogami silnego uwierzytelniania klienta W uwagach słusznie wskazano również brak jasności co do tego, czy mObywatel lub EPTC będą spełniały wymogi silnego uwierzytelniania klienta w kontekście transakcji płatniczych i dostępu do rachunków. Jest to kwestia szczególnie istotna dla sektora finansowego, płatniczego i fintechowego. Bez jednoznacznego wyjaśnienia tej relacji rynek nie będzie w stanie ocenić praktycznej użyteczności nowego rozwiązania w procesach wymagających zgodności z regulacjami sektorowymi. ZPP postuluje więc uzupełnienie projektu, uzasadnienia lub OSR o jasne stanowisko w zakresie zgodności projektowanego rozwiązania z wymogami SCA oraz jego potencjalnego wykorzystania w procesach regulowanych rynku finansowego.	**Uwag wyjaśniona** Wymóg ten jest inaczej ustanowiony. To nie portfele mają zapewnić zgodność z SCA, tylko tam, gdzie się wymaga SCA portfele mają być akceptowane. Wprost z przepisów art. 5f ust 2 rozporządzenia eIDAS wynika, że w przypadku, gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6 rozporządzenia eIDAS, oraz wyłącznie na dobrowolny wniosek użytkownika, również akceptują europejskie portfele tożsamości cyfrowej. Znaczy to, że wprost z

				rozporządzenia wynika, że każdy portfel spełnia wymogi SCA. Można to również ustalić analizując przepisy dotyczące wymogów dla środków identyfikacji elektronicznej zapewniających wysoki poziom bezpieczeństwa oraz certyfikacji portfeli.
131.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Wdrożenie powinno minimalizować koszty i wykorzystywać dorobek mObywatela Uwagi do projektu zwracają również uwagę na wymiar kosztowy. Utrzymanie i rozwój jednego ekosystemu opartego o kod i architekturę mObywatela mogłoby znacząco ograniczyć długofalowe koszty wdrożenia i utrzymania. Rozdzielanie środków na rozwój mObywatela oraz odrębnego oprogramowania portfela może prowadzić do nieefektywności, a w skrajnym przypadku do zarzutów o niegospodarność. ZPP uważa ten argument za istotny. Państwo powinno maksymalnie wykorzystywać już istniejące inwestycje technologiczne i społeczne, zwłaszcza gdy dotyczą one rozwiązania tak dobrze zakorzenionego jak mObywatel. Wdrożenie eIDAS 2.0 powinno wzmacniać istniejący ekosystem, a nie prowadzić do jego fragmentacji.	**Uwaga wyjaśniona/częściowo uwzględniona** Przykładowymi nowymi elementami, których obecnie aplikacja mObywatel nie zapewnia, a są wymagane przepisami rozporządzenia eIDAS i aktami wykonawczymi są: - elektroniczne poświadczenie atrybutów które mogą być wydawane przez kwalifikowanych dostawców usług zaufania, bezpośrednio przez podmiotu odpowiedzialne za źródła autentyczne oraz przez ministra właściwego do spraw informatyzacji (dokumenty mobilne do aplikacji mObywatel użytkownik pobierał sam); - każdorazowe informowanie użytkownika portfela o stronie ufającej i zakresie danych, jaki zostanie jej przekazany (bez względu czy jest to dostawca usługi online czy poświadczeń atrybutów czy np. podpisu elektronicznego); - selektywne udostępnianie wybranych elementów danych; - panel zarządzania umożliwiający łatwe informowanie organu ochrony danych osobowych; - możliwość generowanie pseudonimów; - przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych; - łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO. Nie ma możliwości, aby te zmiany wprowadzić sposób niewidoczny. Tym niemniej dołożone zostaną wszelkie starania, aby zmiany, jakie wymusza rozporządzenie eIDAS były na w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia

				dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
132.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Mechanizm selektywnego udostępniania danych musi uwzględniać obowiązki ustawowe stron ufających ZPP dostrzega wartość selektywnego udostępniania danych jako rozwiązania wzmacniającego ochronę prywatności i zasadę minimalizacji danych. Jednocześnie należy jasno wskazać, że w wielu przypadkach strona ufająca działa w reżimie obowiązków ustawowych. W takich sytuacjach nie może ona opierać się na niepełnym zestawie informacji przekazanych według swobodnego wyboru użytkownika, jeżeli do zawarcia umowy albo przeprowadzenia transakcji niezbędny jest pełen pakiet danych. Mechanizm ten powinien umożliwiać stronie ufającej wymuszenie konkretnego profilu danych, jeśli jest on wymagany prawem lub charakterem danej usługi. Dlatego ZPP postuluje, aby użytkownik miał w takim przypadku jasny wybór: albo udostępnia wszystkie dane wymagane ustawowo dla skorzystania z danej usługi, albo rezygnuje z usługi. Rozwiązanie to lepiej godzi ochronę danych z potrzebą zgodności regulacyjnej i bezpieczeństwa obrotu.	**Uwaga wyjaśniona** W związku z przepisami dotyczącymi rejestracji w rejestrze stron ufających, w tym wskazywania zakresu danych dla każdej usługi, jak również propozycji polegania na certyfikatach rejestracji strony ufającej portfele tożsamości cyfrowej automatycznie rozpoznają zakres danych, jaki jest wymagany dla określonej usługi.
133.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Minimalny zestaw danych jest niewystarczający dla procesów AML/KYC Kolejnym istotnym problemem jest zakres danych przewidzianych dla systemu scentralizowanego. Uwagi do projektu słusznie wskazują, że katalog danych oparty na minimalnym zestawie określonym w rozporządzeniu wykonawczym 2015/1501 nie odpowiada potrzebom sektorów objętych obowiązkami AML/KYC. Brakuje w nim danych kluczowych z perspektywy instytucji obowiązanych, takich jak seria i numer dokumentu tożsamości, data ważności dokumentu, miejsce urodzenia rozumiane jako miasto oraz kraj urodzenia. W praktyce oznacza to, że instytucje obowiązane, w tym instytucje pożyczkowe, nie będą mogły polegać wyłącznie na portfelu przy onboardingu klienta, zawieraniu umów czy procesowaniu transakcji. ZPP rekomenduje rozszerzenie projektowanego podejścia lub przynajmniej jednoznaczne doprecyzowanie, w jaki sposób system ma odpowiadać na potrzeby sektorów regulowanych. W przeciwnym razie powstanie rozwiązanie, które z perspektywy części rynku będzie miało charakter jedynie pomocniczy i nie zastąpi istniejących procedur weryfikacyjnych.	**Uwaga wyjaśniona / częściowo uwzględniona** W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d. Celem systemu scentralizowanego jest jednoznaczne dopasowanie tożsamości w rozumieniu art. 3 pkt 55 oraz art. 11a rozporządzenie eIDAS, jak również przepisów rozporządzenia wykonawcze Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846. Należy zaznaczyć że "dopasowywanie tożsamości" zgodnie z art. 3 pkt 55 eIDAS oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego

				do tej samej osoby. Powyższe oznacza, że celem przepisów nie jest ustalenie tożsamości celem wypełnienia obowiązków wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ale tylko dopasowanie tożsamości zweryfikowanej za pomocą środka identyfikacji elektronicznej wydanego w innym kraju UE do tożsamości już wcześniej zweryfikowanej. Należy podkreślić, że zakresy danych wskazane w projekcie ustawy wskazują na dane identyfikujące osobę jakie zostały wskazane w art. 2 ust. 3 i 4 rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846). Tamże wskazuj się, że odpowiednio należy polegać na danych o których mowa w rozporządzeniu wykonawczym (UE) 2024/2977 wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi lub zestawie danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. W związku z tym, jeżeli dopasowanie jest dokładne i jednoznaczne na podstawie ww. danych wraz zaproponowaną procedurę uzupełniającą dopasowanie uważa się za skuteczne. Podsumowując – celem scentralizowanego systemu dopasowania tożsamości jest: 1. wstępne ustalenie czy osoba fizyczna używająca zagranicznego środka identyfikacji elektronicznej (czyli jednoznacznie zidentyfikowana czego gwarantem jest państwo członkowskie UE) miała nadany nr PESEL i jaki to numer, co pozwoli na jednoznaczną jej identyfikacją w Polsce bez potrzeby weryfikacji dokumentów

				tożsamości, 2. przesłanie danych (za zgodą tej osoby) do końcowej strony ufającej z ustalonym nr PESEL lub w przypadku niedopasowania do rejestru PESEL – danych identyfikujących osobę przekazywanych transgranicznie. Celem tych przepisów nie jest weryfikacja w każdym przypadku serii i numeru dokumentu tożsamości, daty ważności dokumentu oraz miejsca i kraju urodzenia System dopasowywanie tożsamości co do zasady zgodnie z art. 2 ust. 1 rozporządzenie wykonawcze Komisji (UE) 2025/846 dotyczy usług online oferowanych przez podmiot sektora publicznego lub w jego imieniu. W przypadku gdy prywatna strona ufająca jest zobowiązana na podstawie art. 5f ust. 2 rozporządzenia eIDAS do akceptacji europejskich portfeli tożsamości cyfrowej i jednocześnie zobowiązana do stosowania przepisów wynikających z ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, to w zależności od tego czy akceptacja portfela dotyczy już istniejącego konta użytkownika (dla którego już stwierdzono komplet wymaganych danych) czy też nowego – procedury powinny być inne. W przypadku konieczności uzyskania dodatkowych danych wykraczających poza zakres danych identyfikujących osobę przewidziany w rozporządzeniu wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977) odpowiednio zakres tych dany powinien zostać wpisany przez taki podmiot do rejestru stron ufających. Kwestią wykraczającą poza możliwości krajowych regulacji jest zgłoszenie przez inne państwa członkowskie atrybutów potwierdzających niektóre wskazane dane (seria i numer dokumentu tożsamości, data ważności dokumentu). Dane te nie są wymienione

				w załączniku VI do eIDAS i co za tym idzie nie ma obowiązku ich zgłaszania.
134.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Z perspektywy obywatela powinno istnieć jedno, intuicyjne środowisko usług cyfrowych ZPP w pełni podziela argument, że obywatel nie powinien być obciążany koniecznością rozróżniania pomiędzy różnymi państwowymi narzędziami tożsamości cyfrowej. Użytkownicy są już przyzwyczajeni do aplikacji mObywatel jako podstawowego medium dla dokumentów cyfrowych i potwierdzania tożsamości. Wprowadzenie drugiego narzędzia, nawet jeśli formalnie uzasadnionego wymogami certyfikacyjnymi, może prowadzić do dezorientacji i osłabienia adopcji nowego rozwiązania. W ocenie ZPP z perspektywy obywatela powinna istnieć jedna aplikacja, w której aktywacja funkcjonalności zgodnych z eIDAS 2.0 następuje w sposób możliwie niewidoczny dla użytkownika. Europejski wymiar systemu powinien być zintegrowany na poziomie funkcjonalnym i technologicznym, bez przerzucania ciężaru zrozumienia architektury systemu na obywatela.	**Uwaga wyjaśniona** Przykładowymi nowymi elementami, których obecnie aplikacja mObywatel nie zapewnia, a są wymagane przepisami rozporządzenia eIDAS i aktami wykonawczymi są: - elektroniczne poświadczenie atrybutów które mogą być wydawane przez kwalifikowanych dostawców usług zaufania, bezpośrednio przez podmiotu odpowiedzialne za źródła autentyczne oraz przez ministra właściwego do spraw informatyzacji (dokumenty mobilne do aplikacji mObywatel użytkownik pobierał sam); - każdorazowe informowanie użytkownika portfela o stronie ufającej i zakresie danych jaki zostanie jej przekazany (bez względu czy jest to dostawca usługi online czy poświadczeń atrybutów czy np. podpisu elektronicznego); - selektywne udostępnianie wybranych elementów danych; - panel zarządzania umożliwiający łatwe informowanie organu ochrony danych osobowych; - możliwość generowanie pseudonimów; - przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych, - łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO. Nie ma możliwości, aby te zmiany wprowadzić sposób niewidoczny. Tym niemniej dołożone zostaną wszelkie starania, aby zmiany, jakie wymusza rozporządzenie eIDAS były na w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-

				organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
135.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	Należy usunąć z projektu podział na dwa odrębne rozwiązania Uwagi do projektu trafnie wskazują, że nowelizacja ustawy o aplikacji mObywatel utrwala rozgraniczenie pomiędzy aplikacją mObywatel a europejskim portfelem jako dwoma odmiennymi rozwiązaniami. Taka konstrukcja może prowadzić do poważnych problemów prawnych i praktycznych. Wielu przedsiębiorców, w tym z sektorów finansowego i telekomunikacyjnego, zainwestowało już zasoby w integrację z krajowym rozwiązaniem. Jeżeli nowe funkcjonalności miałyby być świadczone w ramach dwóch odrębnych środowisk, przedsiębiorcy byliby zmuszeni do ponownego budowania integracji i utrzymywania zgodności z dwiema architekturami jednocześnie. ZPP rekomenduje zatem zmianę zapisów projektu, w tym przepisów dotyczących ustawy o mObywatelu, tak aby nie tworzyły one dwóch odizolowanych systemów. Preferowanym kierunkiem powinno być odpowiednie technologiczne dostosowanie aplikacji mObywatel i nadanie jej statusu certyfikowanego EPTC. Takie podejście najlepiej odpowiada interesowi obywateli, przedsiębiorców i państwa.	**Uwaga wyjaśniona** Przykładowymi nowymi elementami, których obecnie aplikacja mObywatel nie zapewnia, a są wymagane przepisami rozporządzenia eIDAS i aktami wykonawczymi są: - elektroniczne poświadczenie atrybutów które mogą być wydawane przez kwalifikowanych dostawców usług zaufania, bezpośrednio przez podmiotu odpowiedzialne za źródła autentyczne oraz przez ministra właściwego do spraw informatyzacji (dokumenty mobilne do aplikacji mObywatel użytkownik pobierał sam); - każdorazowe informowanie użytkownika portfela o stronie ufającej i zakresie danych jaki zostanie jej przekazany (bez względu czy jest to dostawca usługi online czy poświadczeń atrybutów czy np. podpisu elektronicznego); - selektywne udostępnianie wybranych elementów danych; - panel zarządzania umożliwiający łatwe informowanie organu ochrony danych osobowych; - możliwość generowanie pseudonimów; - przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych; - łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO. Tym niemniej dołożone zostaną wszelkie starania, aby zmiany, jakie wymusza rozporządzenie eIDAS były w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości

				cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
136.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	mObywatel jako strategiczny dorobek polskiej cyfryzacji W ocenie ZPP aplikacja mObywatel stanowi jedno z najważniejszych osiągnięć polskiej administracji cyfrowej ostatnich lat. Jest to rozwiązanie pionierskie, szeroko rozpoznawalne społecznie, skutecznie wdrożone i oswojone przez obywateli, a zarazem będące dowodem, że państwo może tworzyć nowoczesne, użyteczne i masowo wykorzystywane narzędzia cyfrowe. Skala upowszechnienia mObywatela pokazuje, że Polska dysponuje już dziś realnym kapitałem instytucjonalnym, technologicznym i społecznym, który powinien być punktem wyjścia do dalszej implementacji europejskich ram tożsamości cyfrowej, a nie rozwiązaniem marginalizowanym lub stopniowo wygaszanym bez jasno określonej ścieżki integracji. Z perspektywy ZPP mObywatel zasługuje więc nie tylko na pozytywną ocenę, ale także na formalne potraktowanie jako naturalny fundament wdrożenia nowych funkcji wynikających z eIDAS 2.0. Polska powinna budować na tym, co już działa dobrze, co zdobyło zaufanie obywateli i co może stanowić konkurencyjną przewagę w zakresie cyfryzacji usług publicznych. Konieczne jest jednoznaczne określenie docelowego modelu integracji obu aplikacji Najważniejszym problemem projektu pozostaje brak pełnej jasności co do docelowej relacji pomiędzy aplikacją mObywatel a europejskim portfelem tożsamości cyfrowej. Obecnie komunikowane są równolegle dwa różne kierunki. Z jednej strony uzasadnienie projektu opisuje oba rozwiązania jako całkowicie niezależne od siebie i wskazuje na okres przejściowy oparty na równoległym funkcjonowaniu dwóch aplikacji. Z drugiej strony w przestrzeni publicznej pojawiają się deklaracje, że po etapie pilotażu europejski portfel zostanie docelowo zintegrowany z ekosystemem mObywatela. Ta niespójność osłabia przewidywalność otoczenia regulacyjnego i utrudnia planowanie po stronie rynku. ZPP postuluje zatem jednoznaczne doprecyzowanie projektu ustawy oraz uzasadnienia tak, aby jasno wskazać docelowy model integracji obu rozwiązań i potwierdzić, że europejski portfel tożsamości cyfrowej znajdzie się w ekosystemie istniejącej już polskiej aplikacji. W naszej ocenie takie rozwiązanie jest najbardziej racjonalne z punktu widzenia interesu publicznego, doświadczenia użytkownika oraz efektywności wdrożenia.	**Uwaga wyjaśniona** Przykładowymi nowymi elementami, których obecnie aplikacja mObywatel nie zapewnia, a są wymagane przepisami rozporządzenia eIDAS i aktami wykonawczymi są: - elektroniczne poświadczenie atrybutów które mogą być wydawane przez kwalifikowanych dostawców usług zaufania, bezpośrednio przez podmiotu odpowiedzialne za źródła autentyczne oraz przez ministra właściwego do spraw informatyzacji (dokumenty mobilne do aplikacji mObywatel użytkownik pobierał sam); - każdorazowe informowanie użytkownika portfela o stronie ufającej i zakresie danych jaki zostanie jej przekazany (bez względu czy jest to dostawca usługi online czy poświadczeń atrybutów czy np. podpisu elektronicznego); - selektywne udostępnianie wybranych elementów danych; - panel zarządzania umożliwiający łatwe informowanie organu ochrony danych osobowych; - możliwość generowanie pseudonimów; - przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych; - łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 RODO. Tym niemniej dołożone zostaną wszelkie starania, aby zmiany, jakie wymusza rozporządzenie eIDAS były na w jak najmniejszym stopniu uciążliwe dla użytkowników, a okres przejściowy był odpowiednio dostosowany do ich potrzeb. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności

				aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
137.	Uwaga ogólna	Związek Przedsiębiorców i Pracodawców (ZPP)	ZPP pozytywnie ocenia kierunek wdrożenia eIDAS 2.0 i budowy europejskiego portfela tożsamości cyfrowej w Polsce. ● Aplikacja mObywatel jest jednym z najbardziej udanych i pionierskich projektów cyfryzacyjnych państwa polskiego, który należy traktować jako strategiczny fundament dalszego rozwoju usług cyfrowych. ● Projekt wymaga jednoznacznego określenia docelowego modelu relacji między europejskim portfelem tożsamości cyfrowej a aplikacją mObywatel. ● Z perspektywy obywatela i rynku powinien istnieć jeden spójny ekosystem usług cyfrowych państwa, a nie dwa równoległe i odseparowane rozwiązania. ● Projekt powinien zostać doprecyzowany tak, aby nie prowadził do dublowania integracji, wzrostu kosztów po stronie przedsiębiorców i dezorientacji użytkowników. ● Należy uzupełnić projekt o rozwiązania odpowiadające potrzebom sektorów regulowanych, zwłaszcza w obszarze AML/KYC oraz silnego uwierzytelniania klienta. ● Mechanizm selektywnego udostępniania danych nie może uniemożliwiać przekazania pełnego zestawu danych wymaganych ustawowo przez stronę ufającą. ● Projekt wymaga również korekty techniczno-legislacyjnej w zakresie błędnego odesłania w art. 22a ust. 2 pkt 2.	**Uwaga wyjaśniona** Odnosząc się do zagadnienia modelu funkcjonowania europejskiego portfela tożsamości cyfrowej i aplikacji mObywatel wskazać należy, że europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem 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). Wszystkie te wymagania powodują, że użytkownicy będą musieli potwierdzić stoją tożsamości i uzyskać elektroniczne poświadczenia atrybutów - zamiast dokumentów mobilnych. Nie tylko dlatego, że w eIDAS wymagany jest inny sposób ich wydawania i unieważniania, ale przede wszystkim dlatego, że muszą mieć zasadniczą inną strukturę techniczną i co za tym idzie być inaczej zabezpieczone kryptograficznie. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej. Odnosząc się do zagadnienia wprowadzenia regulacji dla sektorów regulowanych, w szczególności w obszarze AML/KYC, to w ustawie z o przeciwdziałaniu praniu

				pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d. W art. 22a ust. 2 pkt 2 ustawy o usługach zaufania i identyfikacji elektronicznej poprawiono odwołanie.
138.	Uwaga ogólna	IDENTT Sp. z o.o.	Ograniczona rola podmiotów prywatnych. Projekt skupia się niemal wyłącznie na roli administracji publicznej, bardzo mocno ograniczając rolę i potencjał podmiotów prywatnych w tworzeniu ekosystemu portfela tożsamości. Propozycja zmiany: Wyraźne doprecyzowanie, w jaki sposób administracja rządowa będzie wspierać działania podmiotów prywatnych jako dostawców atrybutów (issuerów) i pośredników (intermediaries), a także jak wesprze proces integracji EUDI Wallet z usługami sektora prywatnego.	**Uwaga częściowo uwzględniona / wyjaśniona** Atrybuty mogą wydawać z mocy rozporządzenia eIDAS kwalifikowani dostawcy usług zaufania oraz zgodnie z projektowaną ustawą i wprowadzoną zmianą w art. 1 ust 9 w zakresie art. 22f. 1. Podmioty odpowiedzialne za źródła autentyczne mogą wydawać elektroniczne poświadczenia atrybutów: - o których mowa w art. 3 pkt 46 rozporządzenia 910/2014 - o których mowa w art. 3 pkt 44 rozporządzenia 910/2014 po złożeniu wniosku, o którym mowa w art. 4 ust. 1 pkt 5 lub 6 i uzyskaniu wpisu do rejestru. W zakresie wydawania elektronicznych poświadczeń atrybutów przez podmioty prywatne w dużej mierze stosuje się wprost przepisy rozporządzenia eIDAS, stąd wrażenie, że projekt nie wprowadza stosownych rozwiązań. Pośrednicy w składaniu wniosku o wpis do rejestru stron ufających zostali wskazani w art. 22b ust. 3 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej, natomiast pośrednicy w uwierzytelnianiu zostali wskazani w art. 5b ust. 10 eIDAS, oraz w pkt 14 i 15 załącznika I do rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848).
139.	Uwaga ogólna	Fundacja Future Finance Poland	Brak regulacji dotyczących przenoszenia oraz onboardingu użytkowników pomiędzy obecną a nową aplikacją Projekt ustawy nie zawiera żadnych przepisów ani wytycznych odnoszących się do zasad przenoszenia użytkowników oraz ich danych pomiędzy aktualnie funkcjonującą wersją aplikacji (“mObywatel”) a nową aplikacją opracowywaną na podstawie eIDAS 2.0 (“mObywatel Europa”). W szczególności brak jest jednoznacznych odpowiedzi na następujące kwestie:	**Uwaga wyjaśniona** Ustawa nie przewiduje wygaszenia aplikacji mObywatel. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości

			1. Czy migracja użytkowników nastąpi automatycznie, z zachowaniem dotychczasowych uprawnień, uwierzytelnienia oraz dostępnych dokumentów, czy też konieczne będzie ponowne przeprowadzenie całego lub częściowego procesu onboardingu (np. ponowna weryfikacja tożsamości, nie uwzględniając przy tym kwestii środków identyfikacji elektronicznej na poziomie high)? 2. Kiedy i w jakim trybie mObywatel Europa zastąpi aktualnie działającego mObywatela, a także czy przewidywany jest okres równoległego funkcjonowania obu aplikacji, umożliwiający płynne przejście użytkowników. 3. Co stanie się z danymi przechowywanymi w obecnej aplikacji mObywatel– w szczególności czy zostaną one automatycznie przeniesione do nowej aplikacji mObywatel Europa, w jakim zakresie, w jakiej formie oraz przy zastosowaniu jakich zabezpieczeń. Brak powyższych regulacji stwarza istotne ryzyko, że część użytkowników nie zrealizuje procesu migracji w sposób prawidłowy, co w efekcie może prowadzić do ich utraty jako aktywnych użytkowników. Tymczasem kluczowe z perspektywy ciągłości działania usług jest utrzymanie możliwie najszerszej i stabilnej bazy użytkowników. Z tego względu zasadne jest uzupełnienie projektu o przepisy lub przynajmniej delegację ustawową, które wprost określą zasady migracji, tryb zastępowania aplikacji oraz obsługę danych użytkowników. Ponadto projekt nie precyzuje, w jakim trybie nastąpi wycofanie dotychczasowej aplikacji ani jaki będzie los danych w niej zapisanych — czy zostaną one automatycznie przeniesione, zarchiwizowane, czy też usunięte. Brak jasnych wytycznych w tym zakresie może dodatkowo pogłębić ryzyko dezorientacji użytkowników oraz rozproszenia danych. W tym kontekście warto również zadbać o odniesienia definicyjne w ustawie o aplikacji mObywatel do nowej aplikacji mObywatel Europa.	cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
140.	Uwaga ogólna	Fundacja Future Finance Poland	Umożliwienie przekazywania danych Każdy użytkownik aplikacji ma w niej dostęp do swoich danych, a funkcjonalność i atrakcyjność aplikacji rośnie wraz z liczbą dostępnych w niej informacji. Aby korzystanie z aplikacji było jeszcze wygodniejsze i bardziej użyteczne, warto umożliwić podmiotom prywatnym wprowadzanie danych lub udostępnianie w niej usług w sposób prosty i zautomatyzowany. W praktyce oznacza to, że prywatne podmioty korzystające z aplikacji mogłyby jednocześnie przekazywać do aplikacji własne informacje lub usługi za pośrednictwem odpowiedniego API. Takie podejście ułatwi obywatelom korzystanie z ich uprawnień oraz weryfikację danych, zgodnie z zasadą obustronnej wymiany informacji. Minister odpowiedzialny za informatyzację mógłby zapewnić dostępność interfejsu API, który pozwoli podmiotom prywatnym na pełną integrację z	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej będzie oferował funkcjonalności, dzięki której usługodawcy będą mieli możliwość wydawania do portfela swoich informacji i zestawów danych (elektronicznych poświadczeń atrybutów) oraz - po uprzedniej rejestracji w rejestrze stron ufających - polegania na danych przekazywanych przez użytkowników portfela. Szczegółowe zasady przekazywania elektronicznych poświadczeń atrybutów wynikają z przepisów europejskich.

			aplikacją. Interfejs ten powinien obsługiwać zarówno pobieranie, jak i przekazywanie danych użytkowników, przy pełnym zachowaniu przepisów dotyczących ochrony danych osobowych i bezpieczeństwa informacji.	
141.	Uwaga ogólna	Fundacja Future Finance Poland	SCA Zgodnie z obowiązującą ustawą o usługach płatniczych, odpowiedzialność za prawidłowe przeprowadzenie silnego uwierzytelnienia klienta (Strong Customer Authentication, SCA) spoczywa na dostawcy usługi płatniczej, który realizuje transakcję. Podmiot ten zobowiązany jest do zapewnienia, aby każda autoryzacja płatności spełniała wymogi bezpieczeństwa przewidziane w tejże ustawie, w tym m.in.: zastosowania co najmniej dwóch niezależnych elementów uwierzytelnienia (wiedza, posiadanie, cecha), zapewnienia integralności i poufności danych w trakcie uwierzytelniania czy też ograniczenia ryzyka nadużyć i nieautoryzowanych transakcji. Brak dopełnienia tych obowiązków może skutkować odpowiedzialnością cywilną oraz sankcjami nadzorczymi ze strony Komisji Nadzoru Finansowego. Jednocześnie Projekt ustawy nie precyzuje zasad odpowiedzialności w przypadku dokonywania SCA za pomocą EUDI Wallet. Brak jasnych regulacji w tym zakresie rodzi istotne ryzyko prawne i praktyczne: nie jest określone, kto odpowiada za prawidłowe uwierzytelnienie, w jaki sposób należy zapewnić bezpieczeństwo transakcji ani jakie konsekwencje ponosi dostawca usługi lub użytkownik w przypadku błędów lub nadużyć. W związku z tym konieczne jest doprecyzowanie przepisów, które jednoznacznie wskażą odpowiedzialność stron i zasady przeprowadzania SCA w przypadku korzystania z EUDI Wallet, aby zapewnić bezpieczeństwo użytkowników i pewność prawną podmiotów świadczących usługi płatnicze.	**Uwaga wyjaśniona** Kwestia zapewnienia rozwiązania w jakim portfel zastąpi SCA leży niewątpliwie po stronie banków i innych dostawców usług płatniczych. Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje - zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Bank otrzyma potwierdzanie tożsamości na wysokim poziomie bezpieczeństwa wraz danymi identyfikującymi osobę i/lub dodatkowymi danymi z elektronicznego poświadczenie atrybutów i będzie musiał to uznać na podstawie art. 5f ust. 2 rozporządzenia eIDAS. Odpowiedzialność podmiotów zapewniających europejski portfele tożsamości cyfrowej wynika wprost z rozporządzenia eIDAS, a każde państwo członkowskie jest obowiązane zgodnie z art. 5a ust. 18 przekazać Komisji Europejskiej stosowne informacje, które następnie Komisja publikuje.
142.	Uwaga ogólna	Fundacja Future Finance Poland	Rozdzielenie roli nadzorcy od wykonawcy W projekcie ustawy konieczne jest wyraźne rozdzielenie roli nadzorcy od roli wykonawcy usług w zakresie funkcjonowania europejskiego portfela tożsamości cyfrowej. Obecnie projekt wskazuje ministra właściwego ds. cyfryzacji jako organ odpowiedzialny zarówno za nadzór nad wdrażaniem portfela, jak i za zapewnienie jego operacyjnego funkcjonowania. Takie połączenie funkcji może rodzić ryzyko konfliktu interesów i niejasności kompetencyjnych. W praktyce nadzór powinien obejmować monitorowanie zgodności działania portfela z przepisami prawa, natomiast funkcje wykonawcze — utrzymanie infrastruktury, udostępnianie danych i interfejsów API — powinny być realizowane przez niezależny podmiot lub wyspecjalizowany departament. Wyraźne oddzielenie tych ról pozwoli na większą przejrzystość procesów, wzmocni bezpieczeństwo operacyjne, ograniczy potencjalne konflikty interesów i zapewni, że nadzór będzie wykonywany w	**Uwaga wyjaśniona** Zgodnie z proponowanym przepisami ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz ustawy o aplikacji mObywatel zadania ministra właściwego do spraw informatyzacji w zakresie dostawcy usług nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra, która sprawuje nadzór.

			sposób obiektywny, a decyzje dotyczące funkcjonowania portfela nie będą obciążone bezpośrednim uczestnictwem ministra w procesie operacyjnym.	
143.	Uwaga ogólna	Fundacja Future Finance Poland	Katalog podmiotów publicznych W projekcie ustawy przewidziano utworzenie katalogu podmiotów publicznych. Należy jednak zwrócić uwagę, że istnieje już taki katalog, co rodzi pytanie o zasadność tworzenia kolejnego odrębnego rejestru. Wprowadzenie nowego katalogu mogłoby skutkować niepotrzebnym powielaniem danych, zwiększeniem kosztów administracyjnych i komplikacją procedur aktualizacji.	**Uwaga wyjaśniona** Projekt zakłada rozwój obecnie istniejącego Katalogu Podmiotów Publicznych poprzez umiejscowienie, go w przepisach powszechnie obowiązujących. Docelowe rozwiązania zawarte w przepisach kładą nacisk na automatyzację i wymianę danych pomiędzy systemami bez ingerencji użytkownika (podmiotu). Natomiast podmioty będą zobligowane przede wszystkim do aktualizowania danych oraz wprowadzania danych, których nie można pozyskać z innych źródeł.
144.	Uwaga ogólna	Fundacja Future Finance Poland	EUDI Wallet a EBW W pierwotnych założeniach projekt europejskiego portfela tożsamości cyfrowej (eUDI Wallet) miał obejmować wyłącznie osoby fizyczne, natomiast dla jednoosobowych działalności gospodarczych (JDG) i osób prawnych przewidziano odrębną aplikację EBW, która miała służyć do identyfikacji i uwierzytelniania podmiotów nieosobowych w kontaktach z administracją publiczną i instytucjami prywatnymi. W aktualnym Projekcie ustawy zakres EUDI Wallet został rozszerzony w sposób obejmujący także JDG i osoby prawne, co rodzi pytania o spójność regulacyjną, praktyczne konsekwencje dla przyszłych aplikacji EBW oraz potencjalne ryzyka wynikające z konkurencji między portfelami. W praktyce podmioty gospodarcze mogą nie wiedzieć, który portfel powinny stosować, a instytucje przyjmujące dane mogą otrzymywać niejednolity zestaw informacji identyfikacyjnych. Konieczne jest więc wyraźne wskazanie w Projekcie ustawy, czy stanowi ona też implementację regulacji unijnych dotyczących portfela biznesowego.	**Uwaga wyjaśniona** W uwadze przywoływany jest nieistniejący projekt „Rozporządzenia o portfelu osoby prawnej”. Jeżeli w uwadze chodzi o procedowany obecnie projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia Europejskich Portfeli Biznesowych, to w ramach tego projektu którego planuje się zmianę art. 5a rozporządzenia eIDAS w celu zagwarantowania, aby obowiązkowe wydawanie europejskich portfeli tożsamości cyfrowej dotyczyło wyłącznie osób fizycznych. Znaczy to, że w przypadku uchwalenia przepisów w sprawie ustanowienia Europejskich Portfeli Biznesowych wydawanie europejskich portfeli tożsamości cyfrowej dla osób prawnych może nie tylko nie być obowiązkowe, ale również stracić sens. Jeżeli jednak przepisy w sprawie ustanowienia Europejskich Portfeli Biznesowych nie wejdą w życie lub ich kształt zostanie na tyle zmieniony, że zapewnienie w Polsce europejskiego portfela tożsamości cyfrowej osobom prawnym będzie potrzebne, to i tak sposób wykonania tego wymogu będzie zależał od przepisów krajowych. Obecnie jednak rozporządzenie eIDAS nakazuje zapewniać europejskie portfele tożsamości cyfrowej zarówno osobom fizycznym i prawnym.
145.	Uwaga ogólna	Fundacja Future Finance Poland	Dane statystyczne Aktualnie brakuje informacji statystycznych dotyczących wykorzystywania usług zaufania oraz elektronicznej identyfikacji. Przez to rynek nie może być	**Uwaga wyjaśniona** Projektodawca zdecydował się na zbieranie do celów statystycznych i publikowanie (na portalu dane.gov.pl)

			zwymiarowany ilościowo, co wpływa negatywnie na jego transparentność, określenie wagi dla całego ekosystemu cyfrowych usług komercyjnych i publicznych. Proponujemy aby w Projekcie ustawy wprowadzić zapisy zobowiązujące: ● kwalifikowanych dostawców usług zaufania do przekazywania do Ministra Cyfryzacji, informacji o wykorzystaniu poszczególnych usług zaufania za poprzedni kwartał np. do 15-ego miesiąca po końcu danego kwartału i publikacji przez Ministra Cyfryzacji zagregowanych danych w tym zakresie do końca danego miesiąca; ● dostawcę krajowego Europejskiego Portfela Tożsamości Cyfrowej do przekazywania do Ministra Cyfryzacji informacji o wykorzystaniu EUDI Wallet (w zakresie liczby użytkowników oraz transakcyjności), za poprzedni kwartał, np. do 15. miesiąca po końcu danego kwartału, i publikacji przez Ministra Cyfryzacji zagregowanych danych w tym zakresie do końca danego miesiąca. Szczegółowe założenia do określenia statystyki w tym zakresie byłyby do uszczegółowienia w odpowiednim akcie wykonawczym do ustawy.	wyłącznie danych, o których mowa w art. 48a rozporządzenia eIDAS (tiret drugie uwagi). Kwalifikowane usługi zaufania świadczone są przez kwalifikowanych dostawców usług zaufania na zasadach komercyjnych i na tym etapie uznano, że niezasadnym byłoby zobowiązywanie ich do przekazywania wskazanych danych o świadczonych usługach celem ich publikacji.
146.	Uwaga ogólna	Izba Gospodarki Elektronicznej	Projektowane wdrożenie europejskiego portfela tożsamości cyfrowej (EPTC) przewiduje funkcjonalności w znacznej mierze nakładające się na już istniejące usługi dostępne w aplikacji mObywatel, przy jednoczesnym utrzymaniu obu rozwiązań jako od siebie niezależnych. Taki model, choć teoretycznie możliwy, w praktyce oznacza złożony i kosztowny proces migracji użytkowników oraz partnerów integracyjnych, a także ryzyko niespójnych komunikatów co do docelowego kierunku rozwoju systemu identyfikacji elektronicznej w Polsce. Rekomendujemy jednoznaczne przesądzenie w ustawie i uzasadnieniu, że EPTC będzie elementem ekosystemu mObywatel – jako certyfikowany moduł zgodny z eIDAS – co zapewni integralność architektury, ułatwi komunikację oraz uprości ścieżkę adopcji przez obywateli i rynek.	**Uwaga wyjaśniona** Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Wszystkie te wymagania powodują, użytkownicy będą musieli potwierdzić stoją tożsamości i uzyskać elektroniczne poświadczenia atrybutów - zamiast dokumentów mobilnych. Nie tylko dlatego że w eIDAS wymagany jest inny sposób ich wydawania i unieważniania ale przede wszystkim dlatego że muszą mieć zasadniczą inną strukturę techniczną i co za tym idzie być inaczej zabezpieczone kryptograficznie. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości

				cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
147.	Uwaga ogólna	Izba Gospodarki Elektronicznej	Model docelowy: konsolidacja zamiast dualizmu rozwiązań zapewnianych bezpośrednio przez państwo W zakresie europejskich portfeli tożsamości cyfrowej zapewnianych bezpośrednio przez państwo, utrzymywanie dwóch rozłącznych rozwiązań – aplikacji mObywatel i odrębnego portfela – powoduje powielanie komponentów, interfejsów i procesów, a w konsekwencji rodzi wątpliwości natury prawnej i organizacyjnej. W szczególności, wobec już zrealizowanych integracji po stronie sektora finansowego i telekomunikacyjnego, ponowne wdrażanie połączeń do nowej aplikacji oraz ich równoległe utrzymywanie stanowiłoby obciążenie operacyjne i kosztowe, bez proporcjonalnych korzyści funkcjonalnych. Wobec deklarowanego w debacie publicznej przez Ministerstwo Cyfryzacji zamiaru integracji portfela z mObywatelem potrzebne jest ustawowe doprecyzowanie, że to mObywatel – po uzyskaniu statusu certyfikowanego EPTC – jest jednym, docelowym środowiskiem dla usług i dokumentów cyfrowych, a nie że EPTC ma sukcesywnie przejmować funkcje obecnej aplikacji. Z perspektywy obywatela kluczowa jest prostota: czynności urzędowe, podpisy lub weryfikacja tożsamości powinny odbywać się w ramach jednego interfejsu. Dylemat „mObywatel czy europejski portfel” zwiększa barierę wejścia i ryzyko błędnej ścieżki, a w rezultacie osłabia zaufanie do rozwiązań państwowych. Docelowy model powinien przewidywać, że użytkownik otwiera mObywatela, a aktywacja trybu zgodnego z eIDAS 2.0 dzieje się w tle, automatycznie i tylko tam, gdzie to niezbędne z punktu widzenia wymagań danej usługi. Taka transparentna „jednoaplikacyjna” logika gwarantuje spójny odbiór, obniża koszty wsparcia i komunikacji oraz przyspiesza wdrożenie systemu.	**Uwaga wyjaśniona** Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Wszystkie te wymagania powodują, że użytkownicy będą musieli potwierdzić stoją tożsamości i uzyskać elektroniczne poświadczenia atrybutów - zamiast dokumentów mobilnych. Nie tylko dlatego że w rozporządzeniu eIDAS wymagany jest inny sposób ich wydawania i unieważniania, ale przede wszystkim dlatego, że muszą mieć zasadniczą inną strukturę techniczną i co za tym idzie być inaczej zabezpieczone kryptograficznie. Jednocześnie zdecydowano się na wprowadzenie przepisu, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
148.	Uwaga ogólna	Izba Gospodarki Elektronicznej	Koszty publiczne i zgodność z SCA (PSD2/PSD3) Plan finansowy nowelizacji przewiduje wieloletni wzrost nakładów budżetowych (od 45,50 mln zł w 2026 r. aż do 84,11 mln zł w 2035 r.). Tymczasem konsolidacja rozwiązań w jednym ekosystemie przez wykorzystanie istniejącego kodu i infrastruktury mObywatela pozwoliłaby na istotne ograniczenie kosztów utrzymania i rozwoju oraz zminimalizowała ryzyko zarzutów niegospodarności	**Uwaga wyjaśniona** W zakresie uzasadnienia dla kosztów publicznych należy wskazać, że europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem

			wynikających z równoległego finansowania dwóch podobnych środowisk. Jednocześnie projekt wymaga doprecyzowania, w jaki sposób mObywatel/EPTC będzie spełniał wymogi Silnego Uwierzytelniania Klienta na gruncie PSD2/PSD3, w tym określenia mechanizmów, poziomów zaufania i interfejsów technicznych umożliwiających stosowanie odpowiednich kombinacji czynników (posiadanie/wiedza/biometria) w procesach płatniczych i dostępu do rachunków. Dookreślenie tej ścieżki jest niezbędne dla przewidywalnego planowania integracji po stronie sektora finansowego.	wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Wszystkie te wymagania powodują, że użytkownicy będą musieli potwierdzić stoją tożsamości i uzyskać elektroniczne poświadczenia atrybutów - zamiast dokumentów mobilnych. Nie tylko dlatego że w eIDAS wymagany jest inny sposób ich wydawania i unieważniania, ale przede wszystkim dlatego że muszą mieć zasadniczą inną strukturę techniczną i co za tym idzie być inaczej zabezpieczone kryptograficznie. W zakresie zgodności z SCA wskazać należy, że kwestia zapewnienia rozwiązania i stosownych procedur dla wypełnienia obowiązku SCA przy wykorzystywaniu europejskiego portfela tożsamości cyfrowej do uwierzytelnienia leży niewątpliwie po stronie banków i innych podmiotów sektora finansowego. Wszystkie europejskie portfele tożsamości cyfrowej będą w taki sam sposób technicznie zorganizowane, jeżeli chodzi o ich podstawowe funkcje - zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). Bank otrzyma potwierdzanie tożsamości na wysokim poziomie bezpieczeństwa wraz danymi identyfikującymi osobę i/lub dodatkowymi danymi z elektronicznego poświadczenie atrybutów i będzie musiał to uznać na podstawie art. 5f ust. 2 eIDAS. Odpowiedzialność podmiotów zapewniających europejski portfele tożsamości cyfrowej wynika wprost z eIDAS, a każde państwo członkowskie jest obowiązane zgodnie a art. 5a ust. 18 przekazać Komisji Europejskiej stosowne informacje, które następnie Komisja publikuje.

149.	Uwaga ogólna	LegacyApp Prosta Spółka Akcyjna	Proponuje się dodanie przepisu w ustawie o usługach zaufania i identyfikacji elektronicznej w następującym brzmieniu: Art. X. Dostęp do kwalifikowanych atrybutów statusowych osoby fizycznej Użytkownik europejskiego portfela tożsamości cyfrowej lub krajowego środka identyfikacji elektronicznej może wyrazić zgodę na udostępnienie wybranym usługodawcom prywatnym kwalifikowanych atrybutów dotyczących jego statusu prawnego. Atrybuty, o których mowa w ust. 1, mogą obejmować w szczególności informacje dotyczące: potwierdzenia tożsamości użytkownika, potwierdzenia istnienia osoby fizycznej w rejestrach państwowych, zmiany informacji dotyczącej osoby fizycznej wynikającej z wpisu w rejestrach państwowych, w szczególności informacji o zgonie. Udostępnienie atrybutów, o których mowa w ust. 1, następuje wyłącznie za wyraźną zgodą użytkownika, w zakresie niezbędnym do realizacji usługi cyfrowej świadczonej na rzecz użytkownika, przy wykorzystaniu bezpiecznego mechanizmu przekazywania atrybutów przewidzianego dla europejskich portfeli tożsamości cyfrowej. Podmiot prywatny korzystający z takich atrybutów jest zobowiązany do przetwarzania ich wyłącznie w celu realizacji usługi, dla której użytkownik udzielił zgody. Udostępnienie informacji o zgonie osoby fizycznej może nastąpić wyłącznie w formie potwierdzenia faktu zgonu, bez przekazywania innych danych z rejestrów państwowych. Uzasadnienie: Coraz więcej informacji dotyczących życia i aktywów obywateli ma dziś formę cyfrową. Dotyczy to m.in.: kont bankowych i inwestycyjnych, polis ubezpieczeniowych, dokumentów elektronicznych, dostępu do usług cyfrowych, informacji o majątku, zobowiązaniach i ważnych sprawach rodzinnych. Po śmierci użytkownika dostęp do tych informacji często staje się bardzo trudny lub niemożliwy dla jego bliskich. W praktyce prowadzi to do wielu problemów: długotrwałych poszukiwań dokumentów, utraty części majątku, a także chaosu organizacyjnego w sprawach finansowych i prawnych. Dlatego na świecie rozwijają się usługi cyfrowe, które pozwalają użytkownikowi poufnie zawczasu uporządkować najważniejsze informacje oraz wskazać osoby, które powinny otrzymać do nich dostęp po jego śmierci.	**Uwaga wyjaśniona i nieuwzględniona** Rozporządzanie eIDAS wprost przewiduje w art. 5a ust. 4 lit a oraz lit f, że europejskie portfele tożsamości cyfrowej muszą umożliwiać użytkownikowi, w sposób przyjazny, przejrzysty i identyfikowalny dla użytkownika: a) bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację - pod wyłączną kontrolą użytkownika - danych identyfikujących osobę oraz, w stosownych przypadkach, w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych;(…) f) pobieranie, w zakresie, w jakim jest to technicznie wykonalne, danych użytkownika, elektronicznych poświadczeń atrybutów i konfiguracji; Znaczy to, że użytkownik portfela ma pełną kontrolę nad danymi jego dotyczącymi może z nimi robić to co w przepisach wskazanych powyżej. Ponadto rozporządzenie eIDAS przewiduje w art. 3 pkt 2 i pkt 3 możliwość istnienia środków identyfikacji elektronicznej osoby fizycznej reprezentującej inna osobę fizyczną. Dotąd jednak nie rozwiązano tego problemu na poziomie techniczno-organizacyjnym, głównie z powodu trudności w sposobie określenia zakresu pełnomocnictwa jakie miałaby osoba fizyczna reprezentującej inna osobę fizyczną – tak aby mogłoby to być automatycznie odczytywane i interpretowane przez dostawców usług online. Jak dotąd w Polsce nie są wydawane tego rodzaju środki identyfikacji elektronicznej i nie zostały też notyfikowane przez żaden inny kraju UE. Rozporządzenie eIDAS, jak i projektowana ustawa o wprowadzająca te przepisy do polskiego porządku prawnego, to akty prawne ustanawiające określone narzędzia, ale nie ich ewentualne szersze szczegółowe wykorzystywanie w procedurach cywilnoprawnych.

			Aby takie rozwiązania mogły działać w sposób bezpieczny i wiarygodny, konieczne jest istnienie mechanizmu pozwalającego na potwierdzenie zmiany statusu osoby w rejestrach państwowych, w szczególności informacji o zgonie. Proponowana regulacja umożliwia wykorzystanie infrastruktury identyfikacji elektronicznej do tego celu, przy zachowaniu pełnej kontroli użytkownika nad jego danymi. Jednocześnie rozwiązanie to: nie rozszerza zakresu danych dostępnych podmiotom prywatnym, nie tworzy nowych rejestrów ani baz danych, opiera się wyłącznie na zgodzie użytkownika oraz przekazywaniu minimalnego zakresu informacji. W praktyce oznacza to, że użytkownik może zdecydować, czy chce korzystać z usług cyfrowych, które po jego śmierci pomogą przekazać ważne informacje wskazanym osobom, np. członkom rodziny lub beneficjentom. Rozwiązanie to odpowiada na realną potrzebę społeczną – uporządkowanie informacji i spraw po śmierci użytkownika – oraz jest zgodne z kierunkiem rozwoju europejskiej infrastruktury tożsamości cyfrowej przewidzianej w rozporządzeniu eIDAS 2.0. Wprowadzenie takiej regulacji pozwoli rozwijać w Polsce nowoczesne i bezpieczne usługi cyfrowe, które działają w interesie użytkowników i ich bliskich.	Postulowane rozwiązania wymagałyby zmian, które wykraczają poza zakres niniejszej regulacji
150.	Uwaga ogólna	Naczelna Rada Lekarska	Prezydium Naczelnej Rady Lekarskiej po zapoznaniu się z projektem ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw, przekazanym przy piśmie Sekretarza Stanu w Ministerstwie Cyfryzacji pana Dariusza Standerskiego z dnia 18 lutego 2026 r. (znak: DP.MC.WLA.0211.35.2025) zwraca uwagę, że obecnie dla lekarzy i lekarzy dentystów dokumenty „Prawo wykonywania zawodu" są wydawane nie tylko w postaci spersonalizowanej dwustronnej karty identyfikacyjnej, ale także są udostępniane w postaci dokumentu mobilnego w aplikacji mObywatel. Mobilny dokument prawo wykonywania zawodu pozwala lekarzowi – poza sferą ściśle związaną z wykazywaniem uprawnień do wykonywania zawodu - również na identyfikację w obszarze funkcjonowania lekarza w samorządzie lekarskim, którego jest członkiem. Środowisko lekarskie niepokoją, wobec tego zawarte w uzasadnieniu do projektu ustawy informacje, że aplikacja mObywatel i wdrażany w ramach projektu ustawy europejski portfel tożsamości cyfrowej będą stanowiły całkowicie niezależne od siebie rozwiązania, a zapewnienie użytkownikom aplikacji mObywatel komfortowego przejścia do europejskiego portfela tożsamości cyfrowej będzie ogromnym wyzwaniem techniczno-organizacyjnym. W uzasadnieniu do projektu ustawy wskazano, że z uwagi na różnice techniczno-organizacyjne nie będzie możliwe oddanie użytkownikom do użytku europejskiego portfela tożsamości	**Uwaga wyjaśniona** Europejskie portfele tożsamości cyfrowej muszą spełniać ogólne wymagania określone w art. 5a rozporządzenia eIDAS oraz wymaganie techniczno-organizacyjne określone rozporządzeniem wykonawczym Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającym 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). W szczególności musza obsługiwać dane identyfikujące osobę i elektroniczne poświadczenie atrybutów wydawane w formatach danych ISO/IEC.18013-5:2021 oraz Verifiable Credentials Data Model 1.1. Ponadto muszą rozpoznawać i odpowiednio interpretować certyfikaty dostępu i certyfikaty rejestracji stron ufających portfela o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania

			cyfrowej, który będzie zapewniał te same dokumenty mobilne i te same usługi. 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. Samorząd lekarski oczekuje, że lekarze zachowają możliwość posługiwania się mobilnym dokumentem prawa wykonywania zawodu, które będzie umożliwiało wykazanie posiadania aktualnych uprawnień do wykonywania zawodu oraz identyfikację praw członka samorządu lekarskiego.	rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848). Istotne znaczenie ma również poziom bezpieczeństwa identyfikacji elektronicznej jaki ma zapewniać portfel (wysoki) a poziom bezpieczeństwa jaki zapewnię obecnie aplikacja mObywatel (średni). Tym niemniej dołożone zostaną wszelkie starania aby zmiany jakie wymusza rozporządzenie eIDAS były na w jak najmniejszym stopniu uciążliwe dla użytkowników. Jednocześnie zdecydowano się na wprowadzenie art. 14i, zgodnie z którym minister właściwy do spraw informatyzacji będzie miał możliwość zapewnienia dostępu do wszystkich lub niektórych funkcjonalności aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w ramach jednego rozwiązania techniczno-organizacyjnego. Decyzja w tym zakresie będzie podjęta w oparciu o potrzeby i oczekiwań użytkowników i rynku, możliwości technologiczne oraz stopień adopcji europejskiego portfela tożsamości cyfrowej.
151.	Uwaga ogólna	Osoba fizyczna	W ramach konsultacji publicznych projektu ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (projekt z 18.02.2026 r.) zgłaszam następujące uwagi. Popieram kierunek projektu w zakresie wdrożenia europejskiego portfela tożsamości cyfrowej i elektronicznych poświadczeń atrybutów (m.in. art. 22g–22h). To tworzy realną podstawę do prywatnościowego „selective disclosure" – potwierdzania wybranych atrybutów (np. wieku) bez ujawniania tożsamości. Wnoszę o wprowadzenie (wprost w ustawie albo w politykach/wytycznych publikowanych w BIP na podstawie art. 22g ust. 2 oraz art. 22b ust. 15) profilu „AGE-ONLY" dla usług online: poświadczenie atrybutu w postaci wyłącznie spełnienia progu wieku, np. „age_over_16 = tak/nie", bez przekazywania imienia, nazwiska, daty urodzenia, numeru PESEL, numeru dokumentu. Uzasadnienie: weryfikacja wieku nie wymaga pełnej identyfikacji, a brak takiego profilu może prowadzić do niepotrzebnego przetwarzania danych i ryzyk prywatnościowych, szczególnie w usługach wrażliwych (media społecznościowe/treści/komunikatory). Wnoszę o doprecyzowanie, że mechanizm dopasowywania tożsamości do rejestru PESEL (art. 22a) nie powinien być stosowany jako „domyślna" metoda weryfikacji wieku. W przypadku usług, których celem jest wyłącznie sprawdzenie progu wieku, strona ufająca nie powinna uzależniać dostępu od pozyskania numeru PESEL lub pełnych danych identyfikujących; właściwą ścieżką powinno być poświadczenie atrybutu	**Uwaga wyjaśniona** Co do zasady europejskie portfele tożsamości cyfrowej, z uwagi na wbudowaną funkcjonalność selektywnego udostępniania danych, mogą między innymi zapewnić możliwość uzyskania, przechowywania i posługiwania się elektronicznym poświadczeniem atrybutów potwierdzającym tylko określony wiek. Niestety nie przewidziano takiego elementu w zestawie danych identyfikujących osobę ustalonych rozporządzeniem wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977). Jednakże cel dopasowywania tożsamości do rejestru PESEL, o którym mowa w projektowanym art. 22a ustawy o usługach zaufania oraz identyfikacji elektronicznej jest inny i nie służy do weryfikacji wieku.

			wieku w trybie „AGE-ONLY”. Wnoszę o doprecyzowanie zasad prowadzenia i zakresu historii użycia środków identyfikacji (art. 21aa). Przepis przewiduje ujawnianie użytkownikowi m.in. „danych identyfikujących usługę online” wraz z datą i czasem użycia. Dla use-case „poświadczenie pojedynczego atrybutu” (np. wieku) oraz usług wrażliwych społecznie warto przewidzieć tryb podwyższonej prywatności (minimalizacja identyfikacji konkretnej usługi lub kategoryzacja), aby nie powstawał wrażliwy ślad aktywności użytkowników. Wnoszę o zapewnienie uproszczonej ścieżki integracji dla podmiotów, które chcą weryfikować wyłącznie atrybut wieku („AGE-ONLY”), tak aby mechanizm nie był dostępny wyłącznie dla największych platform. Pełny reżim rejestru stron ufających i certyfikatów (art. 22b i powiązane) może być dla wielu usług barierą, co zwiększy ryzyko pozostania przy praktykach gorszych (skany dokumentów/selfie/oświadczenia wieku). Uproszczony profil „age-check only” + jasne zakazy zbierania nadmiarowych danych poprawią bezpieczeństwo i prywatność. Postuluję, aby schemat poświadczenia „age_over_16” (lub ogólnie „age_over_X”) został potraktowany priorytetowo i zgłoszony do katalogów UE w ramach mechanizmów przewidzianych w projekcie (art. 22d–22e), aby zapewnić interoperacyjność i jednolity standard.	Również cele usługi o której mowa w art. 21aa (historia użycia środków identyfikacji elektronicznej) jest inny. Weryfikację wieku bez potrzeby ujawniania jakichkolwiek innych danych zapewni elektroniczne poświadczenie atrybutów wydane przez ministra właściwego do spraw informatyzacji w trybie projektowanego art. 22f w powiązaniu z art. 22e ust. 5 (zgodnie ze schematem zgłoszonym do katalogu schematów poświadczeń atrybutów zapewnianego przez Komisję Europejską schematem) i z 22e ust. 1 (na podstawie atrybutu złożonego przez ministra do katalogu atrybutów). Znaczy to już zaprojektowano ogólne przepisy, z których wynika, że minister jest zobowiązany zgłosić do Komisji Europejskiej atrybut, jakim jest wiek, do katalogu atrybutów i wskazać miejsce weryfikacji. Takie ogólne rozwiązania przewidziane w eIDAS (i projektowanej ustawie) są bardziej uniwersalne i nie wymagają uchwalania specjalnych przepisów w przypadku atrybutów, o których mowa w załączniku VI do eIDAS.
152.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	W ocenie autorów, w interesie samorządu radcowskiego konieczne jest wprowadzenie do projektowanych regulacji jednoznacznych rozwiązań prawnych zapewniających pełną ochronę tajemnicy zawodowej radcy prawnego w kontekście stosowania mechanizmów identyfikacji elektronicznej oraz usług zaufania przewidzianych w eIDAS 2.0. W szczególności należy wprost przewidzieć wyłączenie lub odpowiednie ograniczenie obowiązków wynikających z eIDAS 2.0 w zakresie, w jakim ich realizacja mogłaby prowadzić do naruszenia tajemnicy zawodowej. Regulacje te powinny mieć charakter wyraźny i niepozostawiający wątpliwości interpretacyjnych, tak aby wyeliminować ryzyko kolizji pomiędzy obowiązkami wynikającymi z prawa unijnego a obowiązkami o charakterze zawodowym. Uzasadnieniem dla wprowadzenia powyższego rozwiązania jest szczególny charakter tajemnicy zawodowej radcy prawnego, która – zgodnie z obowiązującymi przepisami – ma charakter bezwzględny oraz nieograniczony w czasie. Tajemnica ta stanowi podstawową gwarancję ochrony praw jednostki oraz warunek prawidłowego funkcjonowania wymiaru sprawiedliwości i obrotu prawnego. Jednocześnie rozwiązania przewidziane w eIDAS 2.0, w szczególności związane z wykorzystaniem Europejskiego Portfela Tożsamości Cyfrowej oraz mechanizmów udostępniania atrybutów tożsamości, mogą prowadzić do sytuacji, w których:	**Uwaga wyjaśniona** Zgodnie z art. 1 rozporządzenia eIDAS jego celem jest zapewnienie właściwego funkcjonowania rynku wewnętrznego oraz odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania wykorzystywanych w całej Unii, aby umożliwić i ułatwić osobom fizycznym i prawnym korzystanie z prawa do bezpiecznego uczestnictwa w społeczeństwie cyfrowym oraz dostępu do usług publicznych i prywatnych online w całej Unii. W ocenie projektodawców rozporządzenie eIDAS, jako akt prawny bezpośrednio obowiązujący w krajowym porządku prawnym, nie ukształtował reguł dotyczących funkcjonowania europejskich portfeli tożsamości cyfrowej czy funkcjonowania usług zaufania w sposób, który naruszały ochronę tajemnicy zawodowej zawodów zaufania publicznego, w tym zawodu radcy prawnego. W związku z powyższym próba wprowadzenia uregulowań dotyczących tajemnicy zawodowej w

			dochodzi do przekazywania danych identyfikacyjnych klienta za pośrednictwem podmiotów trzecich, zakres ujawnianych informacji wykracza poza minimum niezbędne dla realizacji celu, powstaje ryzyko nieuprawnionego dostępu do danych objętych tajemnicą zawodową. W tym stanie rzeczy brak jednoznacznych regulacji może prowadzić do powstania realnej kolizji norm prawnych, w której radca prawny będzie zobowiązany jednocześnie do realizacji obowiązków identyfikacyjnych wynikających z eIDAS 2.0 oraz do bezwzględnego zachowania tajemnicy zawodowej. W celu uniknięcia takiej sytuacji ustawodawca powinien wprowadzić przepisy szczególne, które: jednoznacznie potwierdzą pierwszeństwo obowiązku zachowania tajemnicy zawodowej w przypadku kolizji z obowiązkami wynikającymi z regulacji dotyczących identyfikacji elektronicznej, ograniczą zakres danych, które mogą być pozyskiwane lub przetwarzane przez radców prawnych przy wykorzystaniu narzędzi eIDAS 2.0 do minimum niezbędnego, wyłączą możliwość nakładania na radców prawnych obowiązków ujawniania informacji objętych tajemnicą zawodową w ramach mechanizmów identyfikacyjnych lub usług zaufania. Wprowadzenie powyższych rozwiązań jest konieczne dla zapewnienia spójności systemu prawnego oraz zagwarantowania, że rozwój narzędzi identyfikacji cyfrowej nie doprowadzi do osłabienia standardów ochrony prawnej jednostki ani do naruszenia istoty zawodu radcy prawnego jako zawodu zaufania publicznego.	przepisach mających zapewnić stosowanie rozporządzenia eIDAS nie jest celowa.
153.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Status radcy prawnego jako podmiotu zaufania w systemie eIDAS 2.0 W ocenie autorów, w interesie samorządu radcowskiego konieczne jest rozważenie wprowadzenia do krajowych przepisów implementujących eIDAS 2.0 rozwiązań przyznających radcom prawnym szczególną rolę w systemie identyfikacji elektronicznej oraz obiegu atrybutów tożsamości. W szczególności należy rozważyć normatywne ukształtowanie statusu radcy prawnego jako podmiotu zaufania publicznego uczestniczącego w procesie weryfikacji określonych atrybutów tożsamości lub uprawnień, w zakresie związanym z wykonywaniem zawodu. Rozwiązanie to mogłoby obejmować w szczególności możliwość potwierdzania przez radców prawnych określonych cech lub statusów prawnych (np. umocowania, reprezentacji, spełnienia określonych przesłanek formalnych), które następnie mogłyby być wykorzystywane w ramach ekosystemu eIDAS 2.0. Uzasadnieniem dla powyższego postulatu jest szczególna pozycja radcy prawnego jako zawodu zaufania publicznego, którego istotą jest zapewnienie bezpieczeństwa obrotu prawnego oraz ochrona praw jednostki. Włączenie radców prawnych w system weryfikacji atrybutów mogłoby przyczynić się do zwiększenia	**Uwaga wyjaśniona** Zasady funkcjonowania europejskiego portfela tożsamości cyfrowej oraz reguły dotyczące atrybutów, źródeł autentycznych, kwalifikowanych elektronicznych poświadczeń atrybutów czy elektronicznych poświadczeń atrybutów wydanych przez podmioty sektora publicznego odpowiedzialne za źródło autentyczne lub w jego imieniu zostały uregulowane w sposób kompleksowy w rozporządzeniu eIDAS oraz stosownych aktach wykonawczych wydanych na jego podstawie. Wprowadzanie partykularnych regulacji dotyczących określonej grupy zawodowej jest więc nie tylko niecelowe, ale może wręcz stanowić naruszenie bezpośrednio obowiązujących regulacji rozporządzenia eIDAS.

			wiarygodności danych wykorzystywanych w obrocie cyfrowym oraz ograniczenia ryzyk związanych z błędną lub niepełną identyfikacją. Jednocześnie brak odpowiednich regulacji w tym zakresie może prowadzić do marginalizacji roli profesjonalnych pełnomocników w procesach identyfikacyjnych, które, w świetle eIDAS 2.0, mogą być w coraz większym stopniu realizowane przez podmioty technologiczne lub dostawców usług cyfrowych. Taka sytuacja mogłaby skutkować osłabieniem gwarancji prawnych oraz przeniesieniem kluczowych funkcji związanych z weryfikacją tożsamości i uprawnień poza sferę zawodów zaufania publicznego. W związku z powyższym ustawodawca powinien rozważyć wprowadzenie przepisów, które: umożliwią radcom prawnym uczestnictwo w systemach potwierdzania atrybutów tożsamości lub uprawnień w ramach eIDAS 2.0, określą zakres i skutki prawne takich potwierdzeń, zapewnią odpowiedni poziom zaufania i odpowiedzialności związany z wykonywaniem tych funkcji, zagwarantują, że udział radców prawnych w tym systemie będzie zgodny z zasadami wykonywania zawodu, w tym obowiązkiem zachowania tajemnicy zawodowej. Wprowadzenie powyższych rozwiązań mogłoby przyczynić się do lepszego wykorzystania potencjału zawodów zaufania publicznego w procesie cyfryzacji obrotu prawnego oraz zapewnienia wyższego poziomu bezpieczeństwa i wiarygodności mechanizmów identyfikacji elektronicznej.	
154.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Europejski Portfel Tożsamości Cyfrowej a relacja pełnomocnik–klient W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne uregulowanie w przepisach krajowych zasad korzystania przez radców prawnych z danych pochodzących z Europejskiego Portfela Tożsamości Cyfrowej w relacji pełnomocnik–klient. W szczególności ustawodawca powinien w sposób wyraźny określić dopuszczalny zakres wykorzystania danych i atrybutów tożsamości udostępnianych przez klienta za pośrednictwem EU Wallet, tak aby wyeliminować niepewność prawną oraz zapewnić zgodność praktyki zawodowej z obowiązującymi standardami ochrony danych i tajemnicy zawodowej. Regulacja ta powinna w szczególności rozstrzygać: czy i na jakich zasadach radca prawny może korzystać z danych udostępnionych przez klienta za pośrednictwem Europejskiego Portfela Tożsamości Cyfrowej, w jakim zakresie dopuszczalne jest utrwalanie i przechowywanie tych danych w dokumentacji prowadzonej sprawy, czy oraz na jakich warunkach dane i atrybuty pozyskane z EU Wallet mogą być wykorzystywane jako materiał dowodowy w postępowaniach sądowych lub administracyjnych. Brak jednoznacznych regulacji w powyższym zakresie może prowadzić do istotnych	**Uwaga wyjaśniona** Kwestie poruszone w uwadze uregulowane zostały w rozporządzeniu eIDAS. Wprowadzanie partykularnych regulacji dotyczących funkcjonowania europejskiego portfela tożsamości cyfrowej czy usług zaufania w kontaktach określonej grupy zawodowej z jej klientami stanowiłoby naruszenie bezpośrednio obowiązujących przepisów rozporządzenia eIDAS.

			wątpliwości praktycznych, w szczególności: czy dane pozyskane z EU Wallet mogą być traktowane jako równoważne tradycyjnym dokumentom, czy ich wykorzystanie nie narusza zasady minimalizacji danych oraz obowiązku ograniczenia celu przetwarzania, jakie są granice odpowiedzialności radcy prawnego za prawidłowość i aktualność tych danych. W związku z powyższym konieczne jest wprowadzenie przepisów, które: określą status prawny danych i atrybutów pochodzących z Europejskiego Portfela Tożsamości Cyfrowej w obrocie prawnym, jednoznacznie uregulują dopuszczalność ich wykorzystania przez profesjonalnych pełnomocników, wskażą zasady ich przechowywania, w tym okresy retencji oraz warunki zabezpieczenia, określą ich wartość dowodową oraz warunki dopuszczalności jako środka dowodowego. Jednocześnie regulacje te powinny zapewniać pełną zgodność z obowiązkiem zachowania tajemnicy zawodowej oraz przepisami o ochronie danych osobowych, a także uwzględniać specyfikę relacji pełnomocnik–klient, w której szczególne znaczenie ma zaufanie oraz poufność przekazywanych informacji. Wprowadzenie powyższych rozwiązań jest niezbędne dla zapewnienia pewności prawa oraz umożliwienia bezpiecznego i efektywnego wykorzystania Europejskiego Portfela Tożsamości Cyfrowej w praktyce świadczenia usług prawnych.	
155.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Odpowiedzialność za błędną identyfikację W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne i wyczerpujące uregulowanie zasad odpowiedzialności za błędy identyfikacji elektronicznej w ramach systemu eIDAS 2.0, w szczególności w kontekście wykorzystania Europejskiego Portfela Tożsamości Cyfrowej. W szczególności ustawodawca powinien w sposób jednoznaczny określić podział odpowiedzialności pomiędzy dostawcami usług identyfikacji elektronicznej, użytkownikami (posiadaczami portfela) oraz profesjonalnymi uczestnikami obrotu, w tym radcami prawnymi. Brak takich regulacji prowadzić będzie do istotnej niepewności prawnej oraz ryzyka przerzucania odpowiedzialności na najsłabsze ogniwa systemu. Obecnie projektowane rozwiązania mogą prowadzić do sytuacji, w których: dane identyfikacyjne lub atrybuty okażą się nieaktualne, niepełne lub nieprawdziwe, dojdzie do nieuprawnionego użycia środków identyfikacji elektronicznej,	**Uwaga wyjaśniona** Kwestia poruszona w uwadze dotyczy kwestii uregulowanych bezpośrednio przepisami rozporządzenia eIDAS (np. art. 11 i 13 rozporządzenia eIDAS).

			błędna identyfikacja stanie się podstawą czynności prawnej lub procesowej. W takich przypadkach brak jasnych zasad odpowiedzialności może prowadzić do powstania sporów co do tego, czy odpowiedzialność ponosi: dostawca usługi identyfikacji (np. podmiot wydający portfel lub potwierdzający atrybuty), użytkownik posługujący się środkiem identyfikacji, czy też profesjonalny pełnomocnik, który polegał na uzyskanych danych. W związku z powyższym konieczne jest wprowadzenie przepisów, które: jednoznacznie przypiszą odpowiedzialność za prawidłowość danych identyfikacyjnych i atrybutów podmiotom je wydającym lub potwierdzającym, określą zakres odpowiedzialności użytkownika za posługiwanie się środkami identyfikacji elektronicznej, w tym w przypadku ich utraty lub nieuprawnionego użycia, wyraźnie wyłączą lub ograniczą odpowiedzialność profesjonalnych pełnomocników w sytuacji, gdy działali oni w zaufaniu do środków identyfikacji spełniających wymogi eIDAS 2.0, wprowadzą domniemania prawne dotyczące wiarygodności danych pochodzących z kwalifikowanych środków identyfikacji, przy jednoczesnym określeniu przesłanek ich obalenia. Należy podkreślić, że bez wprowadzenia powyższych rozwiązań istnieje realne ryzyko przeniesienia ciężaru odpowiedzialności na uczestników obrotu prawnego, którzy nie mają faktycznego wpływu na proces generowania i weryfikacji danych identyfikacyjnych. Taka sytuacja byłaby sprzeczna z zasadą zaufania do państwa i stanowionego prawa oraz mogłaby prowadzić do ograniczenia wykorzystania narzędzi eIDAS 2.0 w praktyce. Wprowadzenie jasnych i przewidywalnych zasad odpowiedzialności jest zatem warunkiem koniecznym dla zapewnienia bezpieczeństwa obrotu prawnego oraz efektywnego funkcjonowania systemu identyfikacji elektronicznej.	
156.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Interoperacyjność rozwiązań eIDAS 2.0 a praktyka krajowa W ocenie autorów, w interesie samorządu radcowskiego konieczne jest zapewnienie pełnej interoperacyjności rozwiązań przewidzianych w eIDAS 2.0 z krajowym porządkiem prawnym, w szczególności z regulacjami proceduralnymi oraz ukształtowaną praktyką stosowania prawa. W szczególności ustawodawca powinien jednoznacznie uregulować sposób funkcjonowania środków identyfikacji elektronicznej oraz atrybutów tożsamości w krajowych postępowaniach sądowych i administracyjnych, tak aby zapewnić ich rzeczywistą użyteczność w obrocie prawnym. Regulacje te powinny w szczególności obejmować: postępowanie cywilne – poprzez jednoznaczne określenie:	**Uwaga wyjaśniona** Rozporządzenie eIDAS jest aktem prawnym obowiązującym bezpośrednio w krajowym porządku prawnym. Rozporządzenie eIDAS wraz z aktami wykonawczymi wydanymi na jego podstawie zawiera kompleksową regulację dotyczącą środków identyfikacji elektronicznej, w tym europejskiego portfela tożsamości cyfrowej oraz funkcjonowania usług zaufania.

			statusu dowodowego danych i atrybutów pochodzących z Europejskiego Portfela Tożsamości Cyfrowej, zasad ich dopuszczalności jako środka dowodowego, relacji pomiędzy dokumentami elektronicznymi generowanymi w systemie eIDAS 2.0 a tradycyjnymi dokumentami prywatnymi i urzędowymi, postępowania administracyjne – poprzez: zapewnienie możliwości skutecznego posługiwania się środkami identyfikacji elektronicznej w kontaktach z organami administracji, określenie zasad uwzględniania atrybutów tożsamości przy załatwianiu spraw administracyjnych, doprecyzowanie wymogów formalnych dla czynności dokonywanych przy użyciu EU Wallet, praktykę sądową – poprzez: dostosowanie systemów teleinformatycznych sądów do obsługi środków identyfikacji elektronicznej zgodnych z eIDAS 2.0, wypracowanie jednolitych standardów akceptacji danych i atrybutów pochodzących z EU Wallet, zapewnienie spójności orzecznictwa w zakresie oceny wiarygodności takich danych. Brak odpowiednich regulacji w powyższym zakresie może prowadzić do sytuacji, w której rozwiązania eIDAS 2.0 – mimo formalnego obowiązywania – nie będą w pełni wykorzystywane w praktyce krajowej, co podważy ich funkcjonalność oraz ograniczy korzyści wynikające z cyfryzacji obrotu prawnego. W związku z powyższym konieczne jest wprowadzenie przepisów zapewniających spójność pomiędzy regulacjami unijnymi a krajowymi procedurami, w szczególności poprzez: jednoznaczne określenie skutków prawnych czynności dokonywanych przy wykorzystaniu środków identyfikacji elektronicznej, dostosowanie przepisów proceduralnych do nowych form identyfikacji i dokumentowania czynności prawnych, zapewnienie jednolitego stosowania prawa przez sądy i organy administracji. Zapewnienie interoperacyjności na poziomie normatywnym i praktycznym stanowi warunek konieczny dla skutecznego wdrożenia eIDAS 2.0 oraz dla zapewnienia, że nowe rozwiązania będą realnie wspierać, a nie komplikować, funkcjonowanie obrotu prawnego.	
157.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Interoperacyjność rozwiązań eIDAS 2.0 a praktyka krajowa W ocenie autorów, w interesie samorządu radcowskiego konieczne jest jednoznaczne doprecyzowanie relacji pomiędzy regulacjami eIDAS 2.0 a przepisami o ochronie danych osobowych, w szczególności w zakresie przetwarzania danych pochodzących	**Uwaga wyjaśniona** Wskazać należy, że już motyw 11 rozporządzenia eIDAS wskazuje, że niniejsze rozporządzenie powinno być stosowane w pełnej zgodności z zasadami dotyczącymi ochrony danych osobowych przewidzianymi w

			z Europejskiego Portfela Tożsamości Cyfrowej. W szczególności ustawodawca powinien w sposób wyraźny określić podstawy prawne przetwarzania danych i atrybutów tożsamości udostępnianych za pośrednictwem EU Wallet, z uwzględnieniem specyfiki relacji pomiędzy użytkownikiem, dostawcą usługi oraz podmiotem korzystającym z danych (w tym profesjonalnym pełnomocnikiem). Brak takiego doprecyzowania może prowadzić do niepewności co do legalności przetwarzania danych oraz ryzyka naruszenia przepisów o ochronie danych osobowych. Jednocześnie konieczne jest wprowadzenie jednoznacznych regulacji gwarantujących stosowanie zasady minimalizacji danych, zgodnie z którą przetwarzane powinny być wyłącznie dane niezbędne dla realizacji określonego celu. W kontekście eIDAS 2.0 oznacza to w szczególności zapewnienie, że mechanizmy udostępniania atrybutów tożsamości będą ograniczone do zakresu adekwatnego do konkretnej czynności prawnej lub faktycznej. Ponadto ustawodawca powinien zapewnić pełną zgodność rozwiązań eIDAS 2.0 z zasadą kontroli danych przez użytkownika, stanowiącą jeden z fundamentów systemu ochrony danych osobowych. Oznacza to konieczność zagwarantowania, że: użytkownik będzie miał realny wpływ na zakres udostępnianych danych i atrybutów, udostępnianie danych będzie następowało w sposób świadomy i dobrowolny, użytkownik będzie posiadał możliwość śledzenia oraz weryfikacji, komu i w jakim zakresie dane zostały udostępnione. Wskazane powyżej postulaty znajdują uzasadnienie w podstawowych zasadach przetwarzania danych osobowych, takich jak zasada legalności, minimalizacji danych oraz zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania. Brak ich odpowiedniego odzwierciedlenia w regulacjach krajowych może prowadzić do powstania napięć pomiędzy systemem identyfikacji elektronicznej a systemem ochrony danych osobowych. W związku z powyższym konieczne jest zapewnienie spójności pomiędzy eIDAS 2.0 a RODO na poziomie normatywnym i praktycznym, w szczególności poprzez: doprecyzowanie podstaw przetwarzania danych w różnych modelach wykorzystania EU Wallet, wprowadzenie mechanizmów technicznych i prawnych ograniczających zakres przetwarzanych danych, zapewnienie skutecznych instrumentów kontroli po stronie użytkownika. Zapewnienie tej spójności stanowi warunek konieczny dla budowy zaufania do systemu identyfikacji cyfrowej oraz dla jego efektywnego i zgodnego z prawem wykorzystania w praktyce obrotu prawnego.	dyrektywie 95/46/WE Parlamentu Europejskiego i Rady. W tym względzie, jeżeli chodzi o zasadę wzajemnego uznawania ustanowioną w niniejszym rozporządzeniu, uwierzytelnianie dla usługi online powinno dotyczyć przetwarzania tylko tych danych identyfikacyjnych, które są adekwatne, właściwe i nie wykraczają poza cele przyznania dostępu do tej usługi online. Ponadto dostawcy usług zaufania i organy nadzoru powinny przestrzegać wymogów na mocy dyrektywy 95/46/WE dotyczących poufności i bezpieczeństwa przetwarzania. Rozporządzenie eIDAS zawiera też szereg regulacji odnoszących się wprost do kwestii przetwarzania i ochrony danych osobowych (np. w art. 5a ust. 14 czy art. 45h). Materia przedstawiona w uwadze należy więc do zakresu rozporządzenia eIDAS.

158.	Uwaga ogólna	Ośrodek Badań, Studiów i Legislacji KRRP	Wnioski Regulacje eIDAS 2.0 wprowadzają fundamentalną zmianę w sposobie identyfikacji i komunikacji prawnej w środowisku cyfrowym, tworząc podstawy europejskiej infrastruktury zaufania. Zmiana modelu identyfikacji (z dokumentowego na atrybutowy) oraz wdrożenie Europejskiego Portfela Tożsamości Cyfrowej będą miały bezpośredni wpływ na sposób wykonywania zawodu radcy prawnego oraz funkcjonowanie obrotu prawnego. Z perspektywy samorządu radcowskiego konieczne jest podjęcie pilnych i skoordynowanych działań przygotowawczych – w szczególności w obszarze regulacyjnym, edukacyjnym i technologicznym – tak aby zapewnić bezpieczne i zgodne z prawem wykorzystanie nowych narzędzi w praktyce zawodowej. Jednocześnie projektowane regulacje wymagają istotnych doprecyzowań na poziomie ustawowym. Kluczowe znaczenie ma w szczególności: zapewnienie pełnej ochrony tajemnicy zawodowej w kontekście mechanizmów identyfikacji elektronicznej, jednoznaczne określenie zasad odpowiedzialności za błędną identyfikację, uregulowanie wykorzystania danych z Europejskiego Portfela Tożsamości Cyfrowej w relacji pełnomocnik–klient, zagwarantowanie spójności rozwiązań eIDAS 2.0 z krajowymi procedurami oraz przepisami o ochronie danych osobowych. Bez wprowadzenia powyższych rozwiązań istnieje ryzyko powstania niepewności prawnej oraz osłabienia standardów ochrony uczestników obrotu. Prawidłowe wdrożenie eIDAS 2.0 powinno zatem opierać się na równowadze pomiędzy rozwojem usług cyfrowych a zachowaniem fundamentalnych zasad wykonywania zawodu radcy prawnego oraz ochrony praw jednostki.	**Uwaga wyjaśniona** Uwaga zawiera podsumowanie wcześniej zgłoszonych uwag przez OBSiL KRRP. W ocenie projektodawcy większość kwestii poruszonych we wcześniejszych uwagach dotyczy materii, która już jest uregulowana rozporządzeniem eIDAS oraz aktami wykonawczymi wydanymi na jego podstawie.
159.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Uwaga o zbyt ogólnym charakterze, co uniemożliwia odniesienie się. Przypuszczalnie może dotyczyć projektowanego rozszerzenia profilu zaufanego o profil zaufany podmiotu publicznego oraz profil zaufany osoby reprezentującej podmiot publiczny, co zostało osobno wyjaśnione.
160.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg	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	**Uwaga wyjaśniona** Zapewnienie profilu zaufanego podmiotu publicznego oraz profilu zaufanego osoby reprezentującej podmiot publiczny jest wyjściem naprzeciw oczekiwanym społecznym przekazywanymi i wspieranym przez Prezesa Urzędu Ochrony Danych Osobowych i Rzecznika

		o (PTI) Związek Cyfrowa Polska (ZCP	mechanizmem powinny być elektroniczne poświadczenia atrybutów potwierdzające status podmiotu publicznego oraz wskazanie powiązania osób fizycznych z podmiotami publicznymi.	Praw Obywatelskich. Takie rozwiązania nie są niezgodne z eIDAS, gdyż z tego rozporządzenia nie wynika, że właściwym mechanizmem potwierdzającym możliwość reprezentowani osoby prawnej powinny być elektroniczne poświadczenia atrybutów potwierdzające status podmiotu publicznego oraz wskazanie powiązania osób fizycznych z podmiotami publicznymi. Rozporządzenie eIDAS wprost przewiduje w art. 3 pkt 2 i 3 istnienie środków identyfikacji elektronicznej, które mogą zawierać dane identyfikujące osobą prawną, lub osobę fizyczną reprezentującej inną osobę fizyczną lub osobę prawną i nie wymaga aby było to realizowane na podstawie elektronicznego poświadczenia atrybutów. Nie potwierdzają tego również wymagania dla środków identyfikacji elektronicznej określone przepisami rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 7, z późn. zm.). Należy nadmienić, że zgodnie z art. 5a ust. 15 rozporządzenia eIDAS „15 Używanie europejskich portfeli tożsamości cyfrowej musi być dobrowolne. Osobom fizycznym i prawnym, które nie korzystają z europejskich portfeli tożsamości cyfrowej, nie można w żaden sposób ograniczać ani utrudniać dostępu do usług publicznych i prywatnych, dostępu do rynku pracy i swobody prowadzenia działalności gospodarczej. Nadal musi być możliwy dostęp do usług publicznych i prywatnych za pomocą innych istniejących środków identyfikacji i uwierzytelniania.” Znaczy to, że jak najbardziej powinno być możliwe utrzymywanie możliwości korzystania z innych środków

				identyfikacji elektronicznej niż europejskie portfele tożsamości cyfrowej.
161.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Przepisy dotyczące KPP i związane z KPP przepisy w zakresie automatycznego tworzenia ADE dla podmiotów publicznych wpisanych do KPP zostaną uwzględnione w odpowiedniej ustawie na kolejnych etapach procedowania.
162.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP	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.	**Uwaga wyjaśniona** Możliwość łączenia w jednym portfelu danych osoby fizycznej i danych związanych z osobą prawną lub działalnością gospodarczą wynika wprost z projektowanych przepisów. Europejski portfel tożsamości cyfrowej jest środkiem identyfikacji elektronicznej, co wynika z definicji zawartej w art. 3 pkt 42 rozporządzenia eIDAS i co za tym idzie podlega w tym zakresie przepisom rozporządzenia wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. U. UE. L. z 2015 r. Nr 235, str. 7, z późn. zm.). W tym akcie prawnym w części 2.1.4 załącznika

				wskazuje się wymagania dotyczące powiązanie między środkami identyfikacji elektronicznej osób fizycznych i prawnych jakie powinny mieć miejsce „w stosownych przypadkach”. Takim właśnie stosownym przypadkiem będzie powiązanie, o którym mowa w projektowanych nowych przepisach art. 14 ust. 3-5 ustawy o aplikacji mObywatel. Ponadto w art. 3 ust. 7 rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977): „7 Państwa członkowskie wprowadzają do systemu użytkowników portfela zgodnie z określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 wymogami dotyczącymi wprowadzania do systemu na wysokim poziomie bezpieczeństwa. Podczas wprowadzania do systemu - przed wydaniem danych identyfikujących osobę jednostce portfela odpowiedniego użytkownika portfela - dostawcy danych identyfikujących osobę przeprowadzają weryfikację tożsamości użytkownika portfela zgodnie z wymogami w zakresie sprawdzania i weryfikacji tożsamości.” Mając przy tym na uwadze, że zgodnie art. 5a ust. 5 lit. f rozporządzenia eIDAS „muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej” oczywiste jest, że możliwe jest przetwarzanie w jednym portfelu danych osoby fizycznej i danych osoby prawnej, lub osoby fizycznej reprezentującą osobę fizyczną lub prawną - pod warunkiem, że dane te będą niepowtarzalnie reprezentowały wskazane osoby. W związku z powyższym nie można zgodzić się z

				twierdzeniem , że nie powinno być możliwe wydanie danych identyfikujących osobę prawną do tego samego portfela, który już zawiera dane identyfikujące osobę fizyczną i że byłoby to niezgodne z architekturą rozporządzenia eIDAS. Skoro do tego samego portfela można z założenia wydać elektroniczne poświadczenie atrybutów, to dlaczego nie można byłoby wydać (wydawanego w takim samym formacie) dodatkowego zestawu danych identyfikujących osobę. Jeżeli chodzi o zarzut wykluczenia części użytkowników, w szczególności osób nieposiadających numeru PESEL, to wyjaśnienie wynika z wymogów wskazanego powyżej rozporządzenia Komisji (UE) 2015/1502 . Tamże wymaga się aby przy weryfikacji tożsamości osoby fizycznej było wiadomo z wiarygodnego źródła, że deklarowana tożsamość istnieje. Znaczy to, że oczywistym odniesieniem w Polsce będzie ewidencja ludności, którą w Polsce prowadzi się w Powszechnym Elektronicznym Systemie Ewidencji Ludności. Co ważne nie ma obowiązku wydawania przez państwo członkowskie portfeli tożsamości cyfrowej dla osób niemieszkających w tym państwie. Zatem każdy środek identyfikacji elektronicznej wydany w Polsce do dyspozycji jakiejkolwiek osoby fizycznej powinien polegać na polskim rejestrze ludności. Przyjmując jako oczywiste założenie, że nie można udostępnić środka identyfikacji osoby prawnej osobie fizycznej, której tożsamość nie została w sposób jednoznaczny zweryfikowana jako tożsamość istniejąca, powiązanie środka identyfikacji osoby prawnej ze środkiem identyfikacji elektronicznej osoby fizycznej wydawanym w Polsce jest uzasadnione.
163.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek	[uwagę rozpoczyna cytat: pierwszy akapit cz. VII uzasadnienia] „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	**Uwaga wyjaśniona** Nie ma potrzeby wprowadzania zmian w przepisach sektorowych, ponieważ przepisy rozporządzenia eIDAS obowiązują bezpośrednio – zarówno w zakresie obowiązkowej akceptacji portfela, o czym mowa w art. 5f ust. 1 i 2, jak również możliwości polegania na portfelu przez dowolną stronę ufającą, o czym mowa w art. 5b. Zgodnie z tymi przepisami przedsiębiorca będzie

		Cyfrowa Polska (ZCP)	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	mógł potwierdzać dane abonentów za pomocą europejskiego portfela tożsamości cyfrowej, jeżeli spełni wymagania art. 5b ust. 1, 2, 3, 8, 9 oraz rozporządzania wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848).

			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.	
164.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Zgodnie z proponowanym przepisami ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz ustawy o aplikacji mObywatel zadania ministra właściwego do spraw informatyzacji w zakresie dostawcy usług nie mogą być realizowane przez tę samą komórkę organizacyjną w urzędzie obsługującym tego ministra, która sprawuje nadzór.
165.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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	**Uwaga uwzględniona** W celu wyeliminowania wątpliwości, że skoro rozporządzenie eIDAS obowiązuje bezpośrednio to znaczy, że oprócz kwalifikowanych dostawców usług zaufania elektroniczne poświadczanie atrybutów mogą być również wydawane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne (jako niekwalifikowana usługa zaufania) pod warunkiem spełnienie przez taki podmiot wymagań, o których

				mowa w art. 45f eIDAS, w związku z uwagą zostały dodane przepisy, aby obowiązek uzyskania przez taki podmiot wpisu do rejestru dostawców usług zaufania był oczywisty oraz w jaki sposób taki dostawca ma potwierdzić wymaganie, o którym mowa w art. 45f ust. 2 eIDAS. Dodano również przepis wprowadzający krajowy katalog schematów elektronicznych poświadczeń atrybutów. Zmieniono w konsekwencji treść art. 14h ustawy zmienianej w art 6.
166.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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	**Uwaga wyjaśniona** Zakładając że przez „dominującego operatora" należy rozumieć ministra właściwego do spraw informatyzacji, a przez „kluczowe elementy ekosystemu" należy rozumieć: a) podmiot wydający europejski portfela tożsamości cyfrowej, b) podmiot wydający dane identyfikujące osobę, c) podmiot zapewniający transgraniczne dopasowanie tożsamości, d) podmiot zapewniający rejestr stron ufających, e) podmiot publiczny upoważniony do wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialny za źródło autentyczne - należy wyjaśnić co następuje. W związku z tym że minister właściwy do spraw informatyzacji już zapewnia aplikację mObywatel i profil zaufany oraz jest podmiotem zapewniającym funkcjonowanie rejestru PESEL stanowiącego autentyczne źródło danych dla danych identyfikujących osobę, jak również zapewnia węzeł krajowy identyfikacji elektronicznej, realizacja przez ten organ zadań, o których mowa w lit. a-c, jest oczywistym wyborem. Nie ma powodu, aby kolejny (inny) podmiot przetwarzał dane osobowe użytkowników portfeli, skoro istnieje organ, który i tak je przetwarza w innym celu i ponadto ma doświadczenie (zasoby ludzkie i wiedzę) w zakresie zapewniania identyfikacji elektronicznej. Jeżeli chodzi o zadanie lit. d, to mogłoby być ono realizowane przez inny podmiot niż minister właściwy

				do spraw informatyzacji mający doświadczenie w zapewnieniu funkcjonowania rejestrów publicznych zawierających dane podmiotów – potencjalnych stron ufających portfelowi, jednakże każdy z tych podmiotów specjalizuje się w określonym obszarze (np. Minister Sprawiedliwości w zakresie KRS, minister właściwy do spraw gospodarki w zakresie CEiDG) i co za tym idzie trudno byłoby wskazać inny podmiot niż ministra właściwego do spraw informatyzacji. Należy ponadto podkreślić, że rozwiązania oznaczone lit. b-d to rozwiązania pojedyncze, gdzie nie ma mowy konkurencji. W zakresie europejskiego portfela tożsamości cyfrowej istnieje możliwość zapewnienia przez państwo członkowskie więcej niż jednego portfela tożsamości cyfrowej (np. przez uznanie portfela wydawanego niezależnie i w projekcie ustawy przewidziano taka możliwość). Jeżeli chodzi o wskazane w lit. e pełnienie roli (podmiot publiczny upoważniony do wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnego za źródło autentyczne), to zgodnie z definicją zawartą w art. 3 pkt 46 rozporządzenia eIDAS, tylko podmiot sektora publicznego może być wyznaczony przez państwo członkowskie do wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnego za źródło autentyczne. Zatem i w tym przypadku oczywistym wyborem jest, mający doświadczenie w zakresie zapewnienia użytkownikom aplikacji mObywatel dokumentów mobilnych, minister właściwy do spraw informatyzacji. W tym zakresie nie należy pomijać oczekiwań użytkowników dokumentów mobilnych, dla których oczywiste jest, że będą mieli ich odpowiedniki w europejskim portfelu tożsamości cyfrowej. Mając ponadto na uwadze, że elektroniczne poświadczenia atrybutów mogą wprost z mocy rozporządzenia eIDAS wydawać: 1) kwalifikowani dostawcy usług zaufania, którym podmioty publiczne odpowiedzialne za źródła

				autentyczne muszą zgodnie z art. 45e ust. 1 rozporządzenia eIDAS i projektowanym nowym, przepisem art. 22c ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej, umożliwić weryfikację atrybutów drogą elektroniczną, na żądanie użytkownika; 2) podmioty publiczne odpowiedzialne za źródła autentyczne - nie można zgodzić się z zarzutem „powstawania wąskich gardeł, ograniczenia konkurencji wpływającej na spadek poziomu innowacji i osłabienia presji”.
167.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Nie można zgodzić się ze stwierdzeniem, że projekt przewiduje osadzenie całości poświadczeń na usługach świadczonych przez ministra do spraw informatyzacji, co będzie ograniczeniem możliwości szybkiego wykorzystania potencjału portfela. Podmioty publiczne odpowiedzialne za źródła autentyczne zgodnie z art. 45e ust. 1 rozporządzenia eIDAS i projektowanym nowym przepisem art. 22c ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej muszą umożliwić na podstawie tych źródeł, kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację atrybutów drogą elektroniczną, na żądanie użytkownika. Ponadto zgodnie z art. 22c ust. 2 podmioty inne niż podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne, o których mowa w załączniku VI do rozporządzenia eIDAS, mogą zapewnić kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, możliwość weryfikacji tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z art. 45e ust. 1 rozporządzenia eIDAS.
168.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg	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.	**Uwaga wyjaśniona** w ocenie projektodawcy nie ma potrzeby, aby przepisy ustawy wprowadzającej rozporządzenie eIDAS zawierały mechanizmy rozwoju rynku oraz „wystarczająco silne instrumenty wspierające dialog z rynkiem”, gdyż ten

		o (PTI) Związek Cyfrowa Polska (ZCP)		dialog odbywa się w ramach procedowania projektu podczas konsultacji publicznych.
169.	Uwaga ogólna	Polska Izba Informatyki i Telekomunikacji (PIIT), Polskie Towarzystwo Informatyczneg o (PTI) Związek Cyfrowa Polska (ZCP)	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.	**Uwaga wyjaśniona** Nie można zgodzić się z tezą, że projektowane przepisy nie zapewniają możliwości bezpośredniego korzystania z portfela przez strony ufające oraz, że pośrednictwo w uwierzytelnianiu za pomocą portfela jest warunkiem skorzystania z portfela. Projektowane przepisy krajowe nie mogą i nie ingerują w możliwość wskazania pośrednika w uwierzytelnianiu za pomocą portfela, o którym mowa w art. 5b ust. 10 rozporządzenia eIDAS, oraz w pkt 14 i 15 załącznika I do rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848). Zgodnie z projektowanym nowym przepisem art. 22b ust. 5 ustawy o usługach zaufania oraz identyfikacji elektronicznej wniosek o wpis do rejestru stron ufających europejskim portfelom tożsamości cyfrowej zawiera dane określone w załączniku I do rozporządzenia 2025/848 oraz adres do doręczeń elektronicznych wpisany do bazy adresów elektronicznych, o której mowa w art. 25 ustawy o doręczeniach elektronicznych. Zatem to wnioskujący o wpis podmiot decyduje czy we wniosku składanym do ministra wskaże pośrednika w uwierzytelnianiu, o którym mowa w pkt 14 i 15 ww. załącznika I do rozporządzenia wykonawczego Komisji (UE) 2025/848, czy też tego z nie zrobi i co za tym idzie nie będzie korzystał w pośrednika. Opcjonalność wskazania pośrednika potwierdzają też projektowane nowe przepisy art. 22b ust. 8 i 9. Nie należy mylić pośrednictwa w uwierzytelnianiu z możliwym (również opcjonalnym) pośrednictwem w składaniu wniosku o wpis do rejestru stron ufających, o którym mowa w projektowanym nowym przepisie art. 22b ust. 3 pkt 2 ustawy o usługach zaufania oraz

				identyfikacji elektronicznej. Pośredniczenie w składaniu wniosku przez kwalifikowanego dostawcę usług zaufania ma na celu wyłącznie ułatwienie uzyskania przez stronę ufającą portfelowi tak zwanego certyfikatu dostępu, ale nie przesądza o tym, że wydający certyfikat dostępu kwalifikowany dostawca usług zaufania miałby być również pośrednikiem w uwierzytelnianiu.
170.	Uwaga ogólna	Polska Izba Ubezpieczeń	Jako sektor korzystający z funkcjonalności aplikacji mObywatel do realizacji procesów ubezpieczeniowych proponujemy dodanie przepisów, zgodnie z którymi rozwiązania oparte o aplikację mObywatel 2.0, używane dotychczas, będą nadal mogły być używane po wejściu w życie ustawy, z zapewnionym odpowiednim okresem przejściowym. Proponujemy dodanie przepisu w brzmieniu: „Art. X [przepisy przejściowe]. 1) Rozwiązania techniczne oparte o aplikację mObywatel, wdrożone na podstawie przepisów ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel przed dniem wejścia w życie niniejszej ustawy, mogą być nadal wykorzystywane po dniu wejścia w życie niniejszej ustawy. 2) Z zastrzeżeniem ust. 3, przyjęcie rozwiązań opartych o europejski portfel tożsamości cyfrowej nie wyłącza dopuszczalności równoległego korzystania przez stronę ufającą z rozwiązań, o których mowa w ust. 1. 3) Minister właściwy do spraw informatyzacji poinformuje podmioty korzystające z rozwiązań, o których mowa w ust. 1, o ostatecznym wyłączeniu tych rozwiązań z użycia, nie później niż 18 miesięcy przed planowanym terminem ich wyłączenia z użycia.”	**Uwaga wyjaśniona** Usługi w aplikacji mObywatel, jak i sama aplikacja nadal będą funkcjonować.
171.	Uwaga ogólna	Polska Izba Ubezpieczeń	Zwrócimy się z prośbą o wyjaśnienie w ustawie lub uzasadnieniu do niej charakteru urządzeń, które wskazane są w projekcie ustawy tj.: urządzenia mobilnego w celu obsługi jednego z czynników uwierzytelniania profilu zaufanego, urządzenia do składania podpisu elektronicznego, bezpieczne urządzenie kryptograficzne portfela, urządzeniu, na którym ich europejski portfel tożsamości cyfrowej, został zarejestrowany, urządzeniami do składania kwalifikowanego podpisu elektronicznego na odległość.	**Uwaga wyjaśniona** Pojęcia te należy rozumieć zgodnie ze znaczeniem nadanym im w rozporządzeniu eIDAS.
172.	Uwaga ogólna	Polska Izba Ubezpieczeń	Prosimy o zapewnienie by grupy kapitałowe mogły składać jeden wniosek o przyłączenie do węzła krajowego systemu teleinformatycznego, w którym udostępniane są usługi online i legitymizować się jednym wspólnym certyfikatem strony ufającej. Zdaniem członków Izby brak takiego rozwiązania prowadziłby do zbędnej złożoności, zwiększonych kosztów i rozproszenia odpowiedzialności operacyjnej.	**Uwaga wyjaśniona** Wymogi w zakresie integracji z węzłem krajowym identyfikacji elektronicznej nie zmieniają się, każdy podmiot odpowiedzialny za system teleinformatyczny udostępniający usługi online, musi zawnioskować oddzielnie, wynika to m. in ze względów konieczności zachowania odpowiedniej rozliczalności i

				bezpieczeństwa. Takie podejście pozwala na minimalizację ryzyka względem interesariuszy korzystających z usługi. Jeśli jest jeden system, za który odpowiada jeden lub kilka podmiotów można „podpiąć" system pod jeden certyfikat.
173.	Uwaga ogólna	Polska Izba Ubezpieczeń	Proponujemy dodanie w projekcie ustawy przepisów, które pozwolą zakładom ubezpieczeń na odmówienie identyfikacji klienta za pośrednictwem elektronicznego portfela tożsamości, w sytuacji braku zapewnienia odpowiednich warunków. Proponowana treść artykułu: „Art. X. [przepis przejściowy] 1) Podmiot niebędący podmiotem publicznym, który świadczy usługi na rzecz klientów z wykorzystaniem środków identyfikacji elektronicznej lub w ramach tych usług korzysta z danych potwierdzających określone atrybuty klienta, nie jest obowiązany do zapewnienia obsługi z użyciem europejskiego portfela tożsamości cyfrowej ani do przyjmowania elektronicznych poświadczeń atrybutów przez okres 36 miesięcy od dnia łącznego spełnienia następujących warunków: uruchomienia rejestru stron ufających europejskim portfelom tożsamości cyfrowej; wejścia w życie przepisów wykonawczych określających warunki techniczne korzystania z tego rejestru oraz uwierzytelniania stron ufających; udostępnienia w usługach krajowych rozwiązań technicznych umożliwiających wykorzystanie europejskiego portfela tożsamości cyfrowej zgodnie z przepisami ustawy. 2) W okresie, o którym mowa w ust. 1, odmowa dokonania czynności z użyciem europejskiego portfela tożsamości cyfrowej albo elektronicznego poświadczenia atrybutu nie stanowi naruszenia obowiązków podmiotu wobec klienta, jeżeli podmiot zapewnia klientowi alternatywny, zgodny z prawem sposób identyfikacji, uwierzytelnienia albo wykazania danego atrybutu. 3) Po upływie okresu, o którym mowa w ust. 1, obowiązek zapewnienia obsługi z użyciem europejskiego portfela tożsamości cyfrowej po stronie podmiotu niebędącego podmiotem publicznym powstaje wyłącznie w zakresie usług: zgłoszonych przez ten podmiot do rejestru stron ufających europejskim portfelom tożsamości cyfrowej, albo dla których obowiązek taki wynika z przepisów odrębnych. 4) Podmiot, o którym mowa w ust. 1, informuje klienta w sposób jasny i zrozumiały o braku możliwości skorzystania z europejskiego portfela tożsamości cyfrowej oraz o dostępnych alternatywnych sposobach dokonania czynności."	**Uwaga nieuwzględniona** Przepisy rozporządzenia eIDAS obowiązują bezpośrednio – zarówno w zakresie obowiązkowej akceptacji portfela, o czym mowa w art. 5f ust. 1 i 2, jak również możliwości polegania na portfelu przez dowolną stronę ufającą, o czym mowa w art. 5b. Zgodnie z tymi przepisami przedsiębiorca będzie mógł potwierdzać dane za pomocą europejskiego portfela tożsamości cyfrowej, jeżeli spełni wymagania art. 5b ust. 1, 2, 3, 8, 9 oraz rozporządzania wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848).
174.	Uwaga ogólna	Polska Izba Ubezpieczeń	Poprosimy o wyjaśnienie, czy oraz na jakich zasadach w Katalogu Podmiotów Publicznych, o którym mowa w dodawanym do ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych Rozdziale 1a, mogą być uwzględniane podmioty	**Uwaga wyjaśniona** Przepisy dot. KPP zawierają następującą definicję podmiotu niepublicznego realizującego zadania

			rynku ubezpieczeniowego realizujące zadania publiczne, takie jak np. Ubezpieczeniowy Fundusz Gwarancyjny.	publiczne – podmiot niepubliczny niebędący osobą fizyczną, realizujący lub wspierający świadczenie tych zadań na podstawie odrębnych przepisów albo na podstawie powierzenia lub zlecenia tego zadania. W związku z tym z obowiązujących przepisów dot. zadań danego podmiotu wynika, czy dany podmiot takie zadania realizuje i wspiera na podstawie odrębnych przepisów albo wykonuje te zadania na podstawie powierzenia lub zlecenia przez podmiot właściwy.
175.	Uwaga ogólna	Polska Izba Ubezpieczeń	Zwracamy się z prośbą o dodanie przepisu ograniczającego odpowiedzialność strony ufającej w przypadku awarii lub błędu leżącego po stronie dostawcy portfela, wystawcy atrybutu, autentycznego źródła danych albo infrastruktury państwa. Proponowane brzmienie przepisu: „Art. X. [brak odpowiedzialności podmiotu niepublicznego za błędy system 1) Podmiot niebędący podmiotem publicznym, który dokonał weryfikacji europejskiego portfela tożsamości cyfrowej albo elektronicznego poświadczenia atrybutu, zgodnie z przepisami ustawy oraz wydanymi na jej podstawie przepisami wykonawczymi, nie ponosi negatywnych skutków prawnych wynikających z: błędów, nieaktualności albo niekompletności danych zawartych w portfelu albo poświadczeniu, niewydania poświadczenia, braku możliwości walidacji danych, zawieszenia albo wycofania portfela z użytkowania, niedostępności systemów teleinformatycznych – jeżeli okoliczności te są przypisane dostawcy portfela, wystawcy poświadczenia, podmiotowi dysponującemu autentycznym źródłem danych albo podmiotowi odpowiedzialnemu za mechanizmy walidacji lub infrastrukturę teleinformatyczną. 2) Przepisu ust. 1 nie stosuje się, jeżeli szkoda albo naruszenie obowiązku pozostaje w związku z zawinionym naruszeniem przez podmiot niebędący podmiotem publicznym, o którym mowa w ust. 1, obowiązków w zakresie weryfikacji lub walidacji. 3) W przypadku braku możliwości skutecznej weryfikacji europejskiego portfela tożsamości cyfrowej albo elektronicznego poświadczenia atrybutu podmiot niebędący podmiotem publicznym, o którym mowa w ust. 1, może zastosować alternatywny, zgodny z prawem sposób identyfikacji, uwierzytelnienia albo wykazania atrybutu. 4) Skorzystanie z alternatywnej ścieżki, o której mowa w ust. 3, nie stanowi naruszenia obowiązków wobec klienta, jeżeli klient został o przyczynie i	**Uwaga wyjaśniona** Odpowiedzialność podmiotów zapewniających europejskie portfele tożsamości cyfrowej wynika wprost z rozporządzenia eiDAS, a każde państwo członkowskie jest obowiązane zgodnie a art. 5a ust. 18 przekazać Komisji Europejskiej stosowne informacje, które następnie Komisja publikuje. Co do zasady nie ma wyłączenia odpowiedzialności strony ufającej.

			dostępnych sposobach dokonania czynności poinformowany w sposób jasny i zrozumiały.”	
176.	Uwaga ogólna	Polska Izba Ubezpieczeń	Wnosimy o dodanie przepisu wyraźnie potwierdzającego dopuszczalność zachowania przez stronę ufającą minimalnego zestawu danych dowodowych z procesu uwierzytelnienia lub okazania atrybutu. Bez takiej normy sektor regulowany będzie miał trudność z pogodzeniem wymogu minimalizacji danych z obowiązkami dowodowymi. Proponowane brzmienie przepisu: „Art. X. [minimalny ślad dowodowy] Podmiot niebędący podmiotem publicznym, który korzysta z europejskiego portfela tożsamości cyfrowej albo elektronicznych poświadczeń atrybutów, może przechowywać dane niezbędne do wykazania faktu, czasu, zakresu i wyniku dokonanej identyfikacji, uwierzytelnienia albo weryfikacji atrybutu. 2) Dane, o których mowa w ust. 1, mogą obejmować wyłącznie: oznaczenie usługi albo czynności, datę i czas operacji, oznaczenie strony ufającej, informację o rodzaju żądanych i udostępnionych danych, wynik walidacji lub weryfikacji, identyfikator techniczny operacji albo poświadczenia, jeżeli jest dostępny, informację o potwierdzeniu operacji przez użytkownika. 3) Niedopuszczalne jest przechowywanie danych wykraczających poza zakres niezbędny do celów, o których mowa w ust. 1, w szczególności utrwalanie pełnej treści poświadczenia albo danych nieobjętych zakresem wykorzystanym do dokonania czynności, chyba że obowiązek taki wynika z przepisów odrębnych. 4) Dane, o których mowa w ust. 1, przechowuje się przez okres niezbędny do wykonania obowiązków wynikających z przepisów odrębnych, obrony przed roszczeniami albo wykazania prawidłowości dokonanej czynności.”	**Uwaga wyjaśniona** Zagadnienia poruszone w uwadze uregulowane są przepisami prawa europejskiego, bezpośrednio obowiązującymi w polskim systemie prawa.
177.	Uwaga ogólna	Polska Izba Ubezpieczeń	Zwrócimy się także o wyraźne uregulowanie, w jakim zakresie europejski portfel tożsamości i poświadczenia atrybutów mogą służyć do wykazywania umocowania do działania za inną osobę, w tym reprezentacji osoby prawnej, prokury, pełnomocnictwa, przedstawicielstwa ustawowego i innych form działania przez reprezentanta. Projekt przepisu: „Art. X. [wykazywanie umocowania] 1) Europejski portfel tożsamości cyfrowej oraz elektroniczne poświadczenia atrybutów mogą być wykorzystywane do wykazania: reprezentacji osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, prokury,	**Uwaga wyjaśniona** Zagadnienia poruszone w uwadze uregulowane są przepisami prawa europejskiego, bezpośrednio obowiązującymi w polskim systemie prawa.

			pełnomocnictwa, przedstawicielstwa ustawowego, innego umocowania do działania w imieniu albo na rzecz osoby trzeciej – jeżeli okoliczność ta wynika z elektronicznego poświadczenia atrybutu, którego skuteczność prawna została przewidziana w przepisach prawa albo uznana na podstawie przepisów odrębnych. 2) Do czasu zapewnienia powszechnej dostępności elektronicznych poświadczeń atrybutów potwierdzających umocowanie, o którym mowa w ust. 1, podmiot niebędący podmiotem publicznym może żądać dodatkowego wykazania umocowania w zakresie niezbędnym do dokonania czynności. 3) Samo potwierdzenie tożsamości osoby fizycznej z użyciem europejskiego portfela tożsamości cyfrowej nie jest równoznaczne z wykazaniem jej umocowania do działania za inną osobę.”	
178.	Uwaga ogólna	PWPW S.A.	W projektowanych przepisach, analogicznie jak w przypadku pominięcia podmiotów uczestniczących w systemie bezpieczeństwa dokumentów publicznych (w tym Komisji do spraw dokumentów publicznych oraz ekspertów w zakresie identyfikacji elektronicznej), co omówiono w uwadze poniżej, nie uwzględniono w sposób kompleksowy roli emitenta dokumentu cyfrowego. Projekt koncentruje się na wybranych aspektach funkcjonowania dokumentów cyfrowych, pomijając kluczową rolę emitenta jako podmiotu odpowiedzialnego za całościowe ukształtowanie dokumentu, jego bezpieczeństwo oraz funkcjonowanie w obrocie prawnym. Brak jednoznacznego określenia tej roli może prowadzić do niespójności systemowej oraz rozproszenia odpowiedzialności, podobnie jak w przypadku pominięcia udziału właściwych podmiotów w procesie poświadczania atrybutów. W ocenie PWPW S.A. zasadne jest uzupełnienie projektowanych przepisów o kompleksowe wskazanie roli emitenta dokumentu cyfrowego, analogicznie do roli emitentów dokumentów publicznych oraz z uwzględnieniem konieczności powiązania tych funkcji z systemem identyfikacji elektronicznej. Projektowana w przepisach rola emitenta dokumentu cyfrowego powinna obejmować w szczególności: 1) określanie struktury dokumentu cyfrowego, w tym zakresu danych oraz atrybutów identyfikujących dokument; 2) określanie niezbędnego zakresu danych (atrybutów) dokumentu cyfrowego, w tym danych służących potwierdzeniu tożsamości osoby, której dokument dotyczy; 3) określanie okresu ważności atrybutów dokumentu cyfrowego oraz zasad ich aktualizacji; 4) zapewnienie autentyczności dokumentu cyfrowego, w tym możliwości weryfikacji jego pochodzenia od emitenta; 5) zapewnienie integralności danych dokumentu cyfrowego od momentu jego	**Uwaga wyjaśniona** Dokumenty publiczne nie są i nie były również wcześniej przedmiotem 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 (rozporządzenie eIDAS). Ostatnie zmiany wprowadzone do rozporządzenia eIDAS rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/1183 ustanowiły między innymi europejski portfel tożsamości cyfrowej i nową usługę zaufania, jaką jest wydawanie elektronicznych poświadczeń atrybutów. Zarówno europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów, zostały nie tylko zdefiniowane w rozporządzeniu eIDAS, aktach wykonawczych do tego rozporządzenia, ale również precyzyjnie opisano wymagania organizacyjne i techniczne wobec tych narzędzi wskazując na właściwe normy Europejskiego Instytutu Norm Telekomunikacyjnych (ETSI). Z pewnością zatem europejski portfel tożsamości cyfrowej, jak również elektroniczne poświadczenia atrybutów, nie są dokumentami publicznymi w rozumieniu ustawy o dokumentach publicznych, jak również należą do odrębnego niezależnego reżimu organizacyjno-prawnego ustanowionego na poziomie

			wydania; 6) zapewnienie zgodności danych pomiędzy dokumentem fizycznym a dokumentem cyfrowym, w przypadku gdy dokument funkcjonuje równolegle w obu postaciach; 7) zarządzanie cyklem życia dokumentu cyfrowego, w tym zasadami jego wydawania, aktualizacji, zawieszania oraz unieważniania; 8) określanie zasad udostępniania danych dokumentu cyfrowego; 9) zapewnienie możliwości weryfikacji ważności dokumentu cyfrowego; 10) określanie zasad potwierdzania autentyczności oraz aktualności atrybutów dokumentu cyfrowego; 11) ponoszenie odpowiedzialności za treść oraz poprawność danych zawartych w dokumencie cyfrowym.	europejskim. Nie można zgodzić się zatem z tezą, że ww. przepisy europejskie wyłączające do odrębnego reżimu prawnego określone dokumenty w postaci elektronicznej będą miały jakikolwiek negatywny wpływ na jednolitość polityki bezpieczeństwa dokumentów publicznych, jak i szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami. Wprost przeciwnie, europejskie portfele tożsamości cyfrowej i elektroniczne poświadczenia atrybutów mogą i powinny stać się ważnym uzupełnieniem dokumentów publicznych w rozumieniu ustawy o dokumentach publicznych i skutecznie zastępować je w usługach online i stosownych przypadkach również w trybie offline (zob. art. 3 pkt 2, art. 5a ust. 4 lit. a oraz ust. 5 lit. a ppkt III rozporządzenia eIDAS). W tym miejscu warto podkreślić, że z uwagi na kryptograficzne zabezpieczenia europejskiego portfela tożsamości cyfrowej i elektronicznych poświadczeń atrybutów ich weryfikacja przez strony ufające nie będzie wymagała znajomości zabezpieczeń, o których mowa w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 1 lipca 2022 r. w sprawie wykazu minimalnych zabezpieczeń dokumentów publicznych przed fałszerstwem (Dz. U. poz. 1456) a jedynie posiadania oprogramowania do weryfikacji ważności elektronicznego poświadczenia atrybutów lub zestawu danych identyfikujących osobę. Co do zasady z przepisów europejskich już wynika, że państwa członkowskie są zobowiązane do zapewnienia co najmniej jednego europejskiego portfela tożsamości cyfrowej (który może być zapewniony bezpośrednio przez państwo członkowskie, na podstawie upoważnienia od państwa członkowskiego lub niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie). Rozporządzenie eIDAS wprost w art. 5f ust. 1 i 2 oraz art. 6 ustanawia obowiązek transgranicznego uznawania

				środków identyfikacji elektronicznej w tym europejskich portfeli tożsamości cyfrowej w usługach publicznych i w części usług prywatnych. Ponadto 45b ust. 2 stanowi, że kwalifikowane elektroniczne poświadczenie atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ma taki sam skutek prawny jak poświadczenia wydane zgodnie z prawem w postaci papierowej. Celem tych przepisów jest niewątpliwie zapewnienie w całej UE wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w Unii, co wynika z wprost motywów 1 i 2 preambuły. Mając na uwadze, że przepisy rozporządzenia eIDAS stosuje się wprost, znaczy to że zarówno kwalifikowani dostawcy usług zaufania, jak i krajowe podmioty odpowiedzialne za źródła autentyczne, mogą wydawać elektroniczne poświadczenia atrybutów ważne w całej UE pod warunkiem, że spełnią stosowne wymagania wynikające z przepisów rozporządzenia eIDAS i aktów wykonawczych. Dodatkowo rozporządzenie eIDAS umożliwia wyznaczenie przez państwa członkowskie podmiotu sektora publicznego, upoważnionego do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne. Istotne jest również, że przepisy rozporządzenia eIDAS nie przewidują wyznaczenia do takiej roli podmiotu innego niż publiczny. Wydaje się to oczywiste z uwagi na to, że państwa członkowskie co do zasady zgodnie z art. 45e zapewniają środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację atrybutów polegających na źródłach autentycznych w sektorze publicznym drogą elektroniczną, na żądanie użytkownika. Propozycja, aby podmiotem, który ma możliwość

				wydawania elektronicznych poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne był minister właściwy do spraw informatyzacji nie wyklucza możliwości wydawania elektronicznych poświadczeń atrybutów przez podmioty w swoim imieniu. W związku z niepewnością w tym zakresie wprowadzono zmianę w proponowanym art. 22f ustawy o usługach zaufania oraz identyfikacji elektronicznej. Warto również wskazać na projektowany przepisy ustawy o usługach zaufania oraz identyfikacji elektronicznej, z których wynika, że minister właściwy do spraw informatyzacji wydaje elektroniczne poświadczenia atrybutów na wniosek podmiotów zainteresowanych, zawierający w szczególności odniesienie do przepisów, norm lub wytycznych, jeżeli mają zastosowanie. Podsumowując, nie ma wątpliwości, że w związku z proponowanymi przepisami nie ucierpi szczelność systemu bezpieczeństwa dokumentów służących do identyfikacji osób, rzeczy lub potwierdzających stan prawny lub prawa osób posługujących się takimi dokumentami.
179.	Uwaga ogólna	Związek Banków Polski (ZBP)	Należy rozważyć rozszerzenie funkcjonalności portfela o możliwość przekazywania stronie ufającej danych identyfikujących osobę małoletnią przez osobę posiadającą wobec niej odpowiednie prawa, w zakresie zbliżonym do identyfikacji osoby pełnoletniej. Zasadne byłoby również umożliwienie przekazywania informacji o zakresie uprawnień przedstawiciela ustawowego wobec małoletniego, w tym ewentualnych ograniczeniach dotyczących dysponowania majątkiem dziecka. Dodatkowo warto rozważyć utworzenie wiarygodnego źródła lub rejestru pozwalającego na weryfikację tych uprawnień oraz doprecyzowanie zasad dostępu osób małoletnich do ich własnych europejskich portfeli tożsamości cyfrowej. Ma to istotne znaczenie z perspektywy ochrony małoletnich przed nadużyciami oraz prawidłowej weryfikacji umocowania opiekunów przez banki.	**Uwaga wyjaśniona** Rozporządzenie eIDAS przewiduje w art. 3 pkt 3 i 4 możliwość istnienia środków identyfikacji elektronicznej osoby fizycznej reprezentującej inną osobę fizyczną. Nie planuje się obecnie wydawania takiego środka identyfikacji elektronicznej w ramach publicznego systemu identyfikacji elektronicznej, o którym mowa w art. 20aa ust. 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, w tym również w ramach europejskiego portfela tożsamości cyfrowej zapewnianego przez ministra właściwego spraw informatyzacji. Warto dodać że konstrukcja tego typu danych identyfikujących osobę nie jest jeszcze rozwiązana w ramach dokumentu Architecture and Reference Framework dostępnego pod adresem https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-

				reference-framework/2.0.0/ Istnieje również możliwość wydawania kwalifikowanych elektronicznych poświadczeń atrybutów w szczególności zawierających dane o składzie rodziny lub pełnomocnictwach i upoważnieniach do reprezentowania osób fizycznych lub prawnych co wynika między innymi z art. 45e i załącznika VI do rozporządzenia eIDAS. Ponadto, zgodnie z przepisami art. 8 ust. 3 rozporządzenia wykonawczego Komisji (UE) 2025/1569 z dnia 29 lipca 2025 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do kwalifikowanych elektronicznych poświadczeń atrybutów oraz elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu (Dz. U. UE. L. z 2025 r. poz. 1569, z późn. zm.) istnieje możliwość zgłaszania schematów poświadczeń atrybutów do katalogu schematów prowadzonego przez Komisję Europejską. Takie schematy zgodnie z art. 8 ust. 3 lit. f ww. rozporządzenia w przypadku gdy nie jest możliwe odniesienie do atrybutu w katalogu atrybutów w art. 7 można odnieść się do atrybutu zdefiniowanego w sposób analogiczny w ramach schematu. Łącznie oznacza to, że możliwe są rozwiązania, które pozwolą na wydawanie elektronicznych poświadczeń atrybutów nawet w przypadku gdy nie istnieją źródła autentyczne które mogą być zgłoszone do katalogu o którym mowa w art. 7 rozporządzenia wykonawczego Komisji (UE) 2025/1569. Zarówno jednak rozwiązanie wskazanego problemu za pomocą środka identyfikacji elektronicznej, jak i za pomocą elektronicznego poświadczenia atrybutów jest niemożliwe z uwagi na brak rejestru źródłowego, w którym tego rodzaju pełnomocnictwa mogłyby być prowadzone. Gdyby taki rejestr istniał wydawanie w oparciu o niego elektronicznych poświadczeń atrybutów byłoby znacząco łatwiejsze.

				Ustanowienie takiego rejestru wykracza jednak poza zakres projektowanej ustawy.
180.	Uwaga ogólna	Związek Banków Polski (ZBP)	W jaki sposób banki miałyby dochować obowiązku zapewnienia dowodu audytowego (wynikającego z regulacji AML) z przeprowadzonej identyfikacji osoby z wykorzystaniem portfela, biorąc pod uwagę brak informacji dotyczących rejestrów logów po stronie stron ufających? Czy w praktyce konieczne będzie tworzenie własnego dokumentu potwierdzającego identyfikację, analogicznie jak w przypadku wykorzystania aplikacji mObywatel?	**Uwaga uwzględniona** W ustawie o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu zmieniono art. 36 ust. 1 pkt 1 lit d.
181.	Uwaga ogólna	Związek Banków Polski (ZBP)	W jaki sposób bank powinien postępować w przypadku rozbieżności pomiędzy danymi pozyskanymi z portfela a danymi znajdującymi się w jego własnych bazach KYC?	**Uwaga wyjaśniona** Wdrożenie portfela nie wpływa w tym względzie na procesy bankowe, weryfikacja zgodności danych powinna odbywać się jak dotychczas.
182.	Uwaga ogólna	Związek Banków Polski (ZBP)	Dotychczasowe rozmowy dotyczące eIDAS 2 wskazywały, że portfel będzie środkiem identyfikacji elektronicznej funkcjonującym niezależnie od Węzła Krajowego. Czy prawidłowo rozumiemy, że według aktualnej ustawy portfel ostatecznie będzie osadzony w Węźle Krajowym, a strony ufające będą musiały do Węzła przystąpić, aby móc z niego korzystać?	**Uwaga wyjaśniona** Portfel będzie przyłączony do węzła krajowego identyfikacji elektronicznej w zakresie jakim stanowi on środek identyfikacji elektronicznej. Z drugiej strony posługiwanie się elektronicznymi poświadczeniami atrybutów przez węzeł krajowy identyfikacji elektronicznej będzie niemożliwe. Aby w pełni korzystać ze wszystkich funkcjonalności portfela należy przejść bezpośrednią integrację poprzez rejestr stron ufających.
183.	Uwaga ogólna	Związek Banków Polski (ZBP)	Czy jeden użytkownik na jednym urządzeniu będzie mógł mieć zainstalowaną zarówno aplikację mObywatel, jak i portfel tożsamości cyfrowej? Czy jeden użytkownik będzie mógł posiadać kilka portfeli tożsamości cyfrowej, np. w konfiguracji polski portfel oraz portfel wydany w innym państwie?	**Uwaga wyjaśniona** Jeden użytkownik na jednym urządzeniu będzie mógł mieć zainstalowaną zarówno aplikację mObywatel, jak i europejski portfel tożsamości cyfrowej. Nie ma zakazu posiadania więcej niż jednego portfela tożsamości cyfrowej.
184.	Uwaga ogólna	Związek Banków Polski (ZBP)	W jaki sposób w przyszłości będzie można zastrzec numer PESEL w sytuacji, gdy eDowód nie ma być przeniesiony do portfela, a aplikacja mObywatel ma zostać docelowo wycofana?	**Uwaga wyjaśniona** Należy wskazać na projektowany przepis ustawy o aplikacji mObywatel, zgodnie z którym dostęp do aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w pełnym albo ograniczonym zakresie funkcjonalności, może być zapewniany przez ministra właściwego do spraw informatyzacji w ramach jednego rozwiązania techniczno-organizacyjnego.
185.	Uwaga ogólna	Związek Banków Polski (ZBP)	Czy przepis dotyczący równoważności dokumentu publicznego z atrybutem oznacza obowiązek dla banków przyjmowania atrybutów pochodzących z portfela?	**Uwaga wyjaśniona** Strona ufająca w procesie wpisu do rejestru stron ufających określa, jakich danych będzie żądała od użytkownika portfela w swoich usługach online.

186.	Uwaga ogólna	Związek Banków Polski (ZBP)	Czy prawidłowe jest rozumienie, że w obowiązujących przepisach nie ma ogólnego obowiązku uznawania portfela w innych procesach niż SCA i w szczególności brak jest odpowiednika art. 83 ustawy o aplikacji mObywatel?	**Uwaga wyjaśniona** Przepisy rozporządzenia eIDAS obowiązują bezpośrednio – zarówno w zakresie obowiązkowej akceptacji portfela dla wskazanych podmiotów, o czym mowa w art. 5f ust. 1 i 2, jak również możliwości polegania na portfelu przez dowolną stronę ufającą, o czym mowa w art. 5b. Zgodnie z tymi przepisami przedsiębiorca będzie mógł potwierdzać dane za pomocą europejskiego portfela tożsamości cyfrowej jeżeli spełni wymagania art. 5b ust. 1, 2, 3, 8, 9 oraz rozporządzania wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848). Ponadto, wzorem rozwiązania przewidzianego obecnie dla mDowodu, obowiązkowe będzie uznawanie portfela do celów potwierdzania tożsamości i obywatelstwa w warunkach fizycznej obecności stron.
187.	Uwaga ogólna	Związek Banków Polski (ZBP)	Czy bank może odmówić akceptacji portfela do czasu uzyskania certyfikacji EUDIW, a jeśli tak – przez jaki maksymalny okres?	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej, aby spełniał wymagania rozporządzenia eIDAS i został wobec tego notyfikowany Komisji, musi przejść certyfikację.
188.	Uwaga ogólna	Związek Banków Polski (ZBP)	Jakie sankcje grożą bankowi, który nie zarejestruje się w rejestrze stron ufających w terminie wynikającym z art. 5f rozporządzenia eIDAS 2.0?	**Uwaga wyjaśniona** Zarówno projektowana ustawa, jak i rozporządzenie eIDAS nie przewidują wprost dodatkowych sankcji za naruszenie obowiązku akceptowania portfela. Jednocześnie nie przesądza to o braku odpowiedzialności podmiotów prywatnych zobowiązanych na podstawie art. 5f rozporządzenia eIDAS za naruszenie prawa swoich klientów (w tym konsumentów) wprowadzonego tym przepisem na gruncie innych przepisów.
189.	Uwaga ogólna	Osoba fizyczna	Celem uwag jest w szczególności zapewnienie, aby mechanizmy wdrażane w związku z europejskim portfelem tożsamości cyfrowej mogły zostać wykorzystane w praktyce do bezpiecznej weryfikacji wieku w usługach online (w tym mediach społecznościowych) w modelu: „potwierdzenie atrybutu wieku bez ujawniania tożsamości" (selective disclosure), z zachowaniem zasad minimalizacji danych oraz ograniczeniem ryzyka tworzenia wrażliwego śladu aktywności użytkowników.	**Uwaga wyjaśniona** Co do zasady europejskie portfele tożsamości cyfrowej z uwagi na wbudowaną funkcjonalność selektywnego udostępniania danych mogą między innymi zapewnić możliwość uzyskania, przechowywania i posługiwania się elektronicznym poświadczeniem atrybutów potwierdzającym tylko określony wiek. Niestety nie

			I. Uwagi ogólne – poparcie kierunku projektu Projekt tworzy istotne podstawy prawne dla wdrożenia europejskiego portfela tożsamości cyfrowej oraz ekosystemu zaufania, m.in. poprzez: rejestr stron ufających europejskim portfelom tożsamości cyfrowej, dopasowywanie tożsamości, punkt weryfikacji atrybutów względem źródeł autentycznych, wydawanie elektronicznych poświadczeń atrybutów, zasady wnioskowania o włączenie atrybutów i schematów poświadczeń do katalogów Komisji Europejskiej. Szczególnie pozytywnie należy ocenić uregulowanie możliwości wydawania elektronicznych poświadczeń atrybutów użytkownikowi europejskiego portfela tożsamości cyfrowej oraz określania ich wzorów, struktur danych, okresu ważności i zasad unieważniania. II. Postulat kluczowy: wprowadzić profil „age-only” (weryfikacja wieku bez tożsamości) 1) Doprecyzowanie poświadczeń atrybutów (profil „ukończone X lat”) Wnoszę o doprecyzowanie (wprost w ustawie lub w aktach wykonawczych/politykach publikowanych w BIP), że dla scenariusza weryfikacji wieku w usługach online (np. próg 16+) możliwe i rekomendowane jest poświadczenie atrybutu w postaci: age_over_16 = true/false (lub analogicznie age_over_X), bez przekazywania danych identyfikujących osoby fizycznej, takich jak imię, nazwisko, data urodzenia, numer PESEL, numer dokumentu. Uzasadnienie: projekt zakłada wydawanie poświadczeń atrybutów w standardowym formacie unijnym, a także określanie wzorów i struktur danych w BIP. Daje to możliwość ustanowienia jednoznacznego „profilu” minimalizacji danych, kluczowego dla prywatności w usługach wrażliwych społecznie (w tym mediach społecznościowych). Proponowany kierunek dopisu (koncepcyjnie): „Dla potrzeb weryfikacji progu wiekowego dopuszcza się elektroniczne poświadczenia atrybutów potwierdzające wyłącznie spełnienie progu wieku (np. 16+), bez ujawniania danych identyfikujących osobę fizyczną.” III. Ograniczyć ryzyko nadużycia dopasowywania tożsamości/PESEL w scenariuszu weryfikacji wieku 2) Dopasowywanie tożsamości (PESEL) – doprecyzować, że nie jest właściwą ścieżką dla age-check Projekt przewiduje system scentralizowany dopasowywania tożsamości m.in. do	przewidziano takiego elementu w zestawie danych identyfikujących osobę ustalonych Rozporządzeniem wykonawczym Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. U. UE. L. z 2024 r. poz. 2977). Weryfikację wieku bez potrzeby ujawniania jakichkolwiek innych danych zapewni elektroniczne poświadczenie atrybutów wydane przez ministra właściwego do spraw informatyzacji w trybie projektowanego art. 22f w powiązaniu z art. 22e ust. 5 (zgodnie ze schematem zgłoszonym do katalogu schematów poświadczeń atrybutów zapewnianego przez Komisję Europejską schematem) i z 22e ust. 1 (na podstawie atrybutu złożonego przez ministra do katalogu atrybutów). Zaprojektowano ogólne przepisy, z których wynika że minister jest zobowiązany zgłosić do Komisji Europejskiej atrybut, jakim jest wiek, do katalogu atrybutów i wskazać miejsce weryfikacji. Takie ogólne rozwiązania przewidziane w rozporządzeniu eIDAS (i projektowanej ustawie) są bardziej uniwersalne i nie wymagają uchwalania specjalnych przepisów w przypadku atrybutów, o których mowa w załączniku VI do rozporządzenia eIDAS. W odniesieniu do wskazywanego w pkt III zagrożenia ryzyka nadużycia dopasowywania tożsamości/PESEL w scenariuszu weryfikacji wieku wyjaśnienia wymaga, że zgodnie z definicją zawartą w art. 3 pkt 55 rozporządzenia eIDAS „dopasowywanie tożsamości" oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby. Z tej definicji, jak również z art. 11a ust. 1 rozporządzenia eIDAS oraz z rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającego zasady stosowania

			rejestru PESEL, oraz mechanizmy umożliwiające przekazanie danych identyfikujących i numeru PESEL stronie ufającej za zgodą użytkownika. Wnoszę o doprecyzowanie, że: w przypadku, gdy usługa online wymaga wyłącznie ustalenia spełnienia progu wiekowego, strona ufająca nie powinna uzależniać dostępu od dopasowania tożsamości do PESEL ani pozyskania numeru PESEL/danych identyfikujących; a właściwą ścieżką jest użycie poświadczenia atrybutu „age-only". Uzasadnienie: w przeciwnym razie rynek może pójść w kierunku „weryfikacji wieku przez pełną identyfikację", co byłoby sprzeczne z zasadami minimalizacji danych i niepotrzebnie zwiększałoby ryzyka prywatnościowe. IV. Logi historii użycia – doprecyzować minimalizację dla weryfikacji atrybutów (szczególnie w usługach wrażliwych) 3) Art. 21aa – dzienniki (logi) zawierają dane identyfikujące usługę online Projekt wprowadza usługę umożliwiającą użytkownikom zapoznanie się z historią użycia środków identyfikacji elektronicznej, w tym z danymi identyfikującymi usługę online oraz datą i czasem użycia. Co do zasady rozwiązanie to jest korzystne dla transparentności wobec użytkownika. Jednocześnie, dla scenariuszy wrażliwych (np. media społecznościowe / usługi treściowe) niesie ryzyko tworzenia wrażliwego śladu aktywności. Wnoszę o rozważenie doprecyzowania (w ustawie lub aktach/politykach wykonawczych), że w przypadku użycia poświadczeń atrybutów „age-only" możliwy jest tryb logowania zdarzeń z większą ochroną prywatności, np.: rejestrowanie faktu użycia poświadczenia atrybutu bez wskazywania nazwy konkretnej platformy (np. kategoria usługi lub pseudonim/identyfikator, który nie umożliwia łatwej identyfikacji podmiotu bez dodatkowych danych), albo inny mechanizm minimalizacji „identyfikacji usługi online" dla czynności polegających na weryfikacji pojedynczego atrybutu. Uzasadnienie: selective disclosure ma chronić użytkownika nie tylko przed ujawnieniem danych platformie, ale także przed powstawaniem wrażliwych metadanych w ekosystemie. V. Uproszczony profil integracji „age-check only" (żeby nie było to dostępne wyłącznie dla największych) 4) Rejestr stron ufających i certyfikaty – potrzebna „lekka" ścieżka dla age-only Projekt reguluje rejestr stron ufających i wymogi związane z certyfikatami dostępu/rejestracji oraz politykami krajowymi. W praktyce pełna ścieżka formalna może być zbyt obciążająca dla wielu mniejszych usług online, co paradoksalnie zwiększy liczbę praktyk niepożądanych (skany	rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846) wynika, że chodzi o obowiązek jednoznacznego zidentyfikowania osoby fizycznej. Jest to zatem proces w którym niedopuszczalne jest pominięcie danych identyfikujących osobę fizyczną w szczególności poleganie wyłącznie na weryfikacji wieku. Podobnie w przypadku historii użycia środków identyfikacji elektronicznej, o czym mowa w uwadze oznaczonej cyfrą IV – celem tej usługi jest ustalenie użycia środków identyfikacji elektronicznej w węźle krajowym identyfikacji elektronicznej, a nie elektronicznych poświadczeń atrybutów i co za tym idzie nie ma nic wspólnego z używaniem elektronicznego poświadczenia atrybutów potwierdzającego tylko wiek, gdyż w takim przypadku nie mamy do czynienia ze środkiem identyfikacji elektronicznej. W odniesieniu do uwagi oznaczonej cyfrą V – przepisy art. 5b rozporządzenia eIDAS oraz rozporządzenia wykonawczego Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. U. UE. L. z 2025 r. poz. 848) jednoznacznie wymagają, aby każda strona ufająca, która chce polegać na europejskim portfelu tożsamości cyfrowej zarejestrowała się w rejestrze stron ufających i po dokonaniu wpisu uzyskała certyfikat dostępu oraz, w zależności od przepisów krajowych, certyfikaty rejestracji dla każdej ze świadczonych usług. Przepisy krajowe ustanawiają w tym zakresie tylko kto prowadzi rejestr, w jaki sposób można się do niego wpisać oraz kto wydaje certyfikaty dostępu strony ufającej i certyfikaty rejestracji. Poleganie przez strony ufające na europejskich portfelach tożsamości cyfrowej w przypadku gdy strony te będą potrzebowały wyłącznie weryfikacji wieku zostanie odpowiednio wpisane do rejestru w taki sposób, że dla określonej usługi będzie potrzebne tylko

			dowodów, selfie, oświadczenia wieku). Wnoszę o wprowadzenie lub zapowiedź (w ustawie/politykach BIP) uproszczonego profilu integracji „age-check only”, obejmującego: ograniczony zakres formalny dla usług, które weryfikują wyłącznie atrybut wieku, obowiązek minimalizacji danych, zakaz żądania identyfikatorów (np. PESEL) jeżeli cel to tylko weryfikacja wieku, gotowe wytyczne/SDK/API ułatwiające integrację. VI. Priorytet: schemat poświadczenia „age_over_16” do katalogów UE 5) Wniosek o włączenie schematu „wiek 16+” do katalogów Komisji Europejskiej Projekt tworzy tryby wnioskowania o włączenie atrybutów i schematów poświadczeń do katalogów Komisji Europejskiej. Postuluję, aby schemat poświadczenia atrybutu „age_over_16” (lub ogólniej „age_over_X”) potraktować jako jeden z priorytetowych use-case’ów, docelowo interoperacyjny w UE. VII. Podsumowanie Projekt ustawy tworzy solidne podstawy prawne dla europejskiego portfela tożsamości cyfrowej i poświadczeń atrybutów. Wnoszę o doprecyzowania ukierunkowane na praktyczny i bezpieczny scenariusz „weryfikacja wieku jako atrybut”, tj.: ustanowienie profilu „age-only” bez tożsamości (selective disclosure), wyraźne rozdzielenie weryfikacji wieku od dopasowywania do PESEL, minimalizację wrażliwych metadanych (logi) przy weryfikacji atrybutów, uproszczony profil integracji „age-check only”, priorytet zgłoszenia schematu „age_over_16” do katalogów UE.	elektroniczne poświadczenie atrybutów potwierdzające wyłącznie wiek. Na podstawie wpisu zostanie wydany odpowiadający takiemu wymaganiu certyfikat rejestracji z które będzie wynikało, że w ramach danej usługi określona strona ufająca wymaga podania wieku. Taki certyfikat zostanie automatycznie rozpoznany przez na europejski portfel tożsamości cyfrowej co spowoduje że portfel wyświetli użytkownikowi informacje stronie ufającej oraz o zakresie danych jaki ta strona żąda. Z uwagi na to że: - rejestr stron ufających będzie publiczne dostępny, - użytkownicy europejskiego portfela tożsamości cyfrowej będą mogli korzystać z wbudowanego w każdy portfel panelu zarządzania umożliwiającego użytkownikowi we szczególności łatwe zgłaszanie strony ufającej właściwemu krajowemu organowi ochrony danych, w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych (zgodnie z art. 5a ust. 4 lit d tiret trzeci), nie ma potrzeby tworzenia dodatkowych regulacji w zakresie wersyfikacji wieku. Obecne przepisy rozporządzenia eIDAS wraz z planowanymi już przepisami krajowymi zmieniającymi ustawę o usługach zaufanie oraz identyfikacji elektronicznej zapewniają funkcjonowanie samoregulującego się systemu, gdyż żaden dostawca usług online nie zdecyduje się na żądanie większej ilości danych niż będzie mu to potrzebne do świadczenia usługi. Należy jednak nadmienić, że zgodnie z art. 5a ust. 15 rozporządzenia eIDAS używanie europejskich portfeli tożsamości cyfrowej musi być dobrowolne. Osobom fizycznym i prawnym, które nie korzystają z europejskich portfeli tożsamości cyfrowej, nie można w żaden sposób ograniczać ani utrudniać dostępu do usług publicznych i prywatnych, dostępu do rynku pracy i swobody prowadzenia działalności gospodarczej. Nadal musi być możliwy dostęp do usług publicznych i prywatnych za pomocą innych istniejących środków identyfikacji i uwierzytelniania.

				W odniesieniu do postulatu zawartego w pkt VI wyjaśniamy, że schemat elektronicznego poświadczenia atrybutów potwierdzającego wiek będzie jednym z priorytetów.
190.	Uwaga ogólna do zmian w przepisach prawa w zakresie powiazania dokumentów publicznych z atrybutami	PWPW S.A.	Wskazane zmiany w art. 16a ustawy o kierujących pojazdami oraz art. 75e ustawy – Prawo o ruchu drogowym wskazano jako preferowaną technikę legislacyjną na uwzględnienie uwagi dotyczącej powiązania w systemie prawnym konkretnych dokumentów publicznych z elektronicznymi oświadczeniami atrybutów. W celu zachowania jednolitości i spójności w systemie prawnym PWPW S.A. powinno zostać przyznane prawo wyłączne do wydawania i udostępnia elektronicznego poświadczenia atrybutów związanych z danymi zawartymi w dokumentach publicznych, do których wytwarzania, indywidualizacji i personalizacji prawo wyłączne przyznano PWPW S.A. na podstawie art. 17 ust. 1 ustawy z dnia 22 listopada 2018 r. o dokumentach publicznych (Dz. U. z 2024 r. poz. 1669, z późn. zm.), przepisów wydanych na podstawie art. 16a ust. 2 tej ustawy oraz przepisów ustaw szczególnych. PWPW S.A. dostrzega, że ze względu na systemowy charakter uwagi jej uwzględnienie będzie wymagało przeprowadzenia uprzednich uzgodnień z emitentami poszczególnych dokumentów publicznych. Wskazana uwaga nie stoi w sprzeczności z propozycją przepisu w ustawie o dokumentach publicznych wskazaną w poz. 2 tabeli.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów nie są dokumentami publicznymi w ramach reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim.
191.	Uzupełnienie projektu ustawy o nowelizację art. 10 z dnia 6 sierpnia 2010 r. o dowodach osobistych	PWPW S.A.	W konsekwencji uwagi wskazanej w pkt 2 tabeli konieczne jest także dodanie odpowiedniej zmiany do ustawy o dowodach osobistych. W ustawie o dowodach osobistych wprowadza się następującą zmianę. Art. 10 otrzymuje brzmienie: „Art. 10. 1. Minister właściwy do spraw wewnętrznych personalizuje dowody osobiste. 2.Personalizacja dowodów osobistych jest realizowana w systemie teleinformatycznym utrzymywanym i rozwijanym przez ministra właściwego do spraw wewnętrznych lub jednostkę organizacyjną przez niego nadzorowaną. 3. Realizowanie zadań utrzymywania lub rozwijania systemu teleinformatycznego, o którym mowa w ust. 2, może zostać powierzone innemu podmiotowi. 4. Dane wskazane w art. 12 ust. 1 lub art. 12a ust. 1 pkt 1 przetwarzane w systemie teleinformatycznym wykorzystywanym do personalizacji dowodów, po dokonaniu personalizacji dowodu osobistego, są źródłem autentycznym dla elektronicznych poświadczeń atrybutów dotyczących osoby fizycznej wydawanych w europejskim portfelu tożsamości cyfrowej, w tym atrybutów, o których mowa w art. 45f 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	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów nie są dokumentami publicznymi w ramach reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim.

			uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z późn. zm.). 5. W przypadku powierzenia realizacji zadań, o których mowa w ust. 3, elektroniczne poświadczenia atrybutów, pochodzące ze źródła autentycznego, o którym mowa w ust. 4, wydaje oraz udostępnia podmiot, o którym mowa w ust. 2. W takim przypadku ten podmiot uzgadnia schemat wydawania elektronicznych poświadczeń atrybutów z ministrem właściwym do spraw wewnętrznych.”.	
192.	Uzupełnienie projektu ustawy o nowelizację art. 16a ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami	PWPW S.A.	Propozycja dodania wprost uprawnienia do wydawania atrybutów pochodzących z systemu, o którym mowa w art. 16a ust. 1 i 2 ustawy o kierujących pojazdami. Projekt powinien zostać uzupełniony o nowelizację art. 16a ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2025 r. poz. 1226, z późn. zm.), polegającą na dodaniu po ust. 2 ust. 2a i 2b w brzmieniu: „2a. Wytwórca praw jazdy, kart kwalifikacji kierowcy i pozwoleń na kierowanie tramwajem zapewniający system teleinformatyczny, o którym mowa w ust. 1, wydaje oraz udostępnia elektroniczne poświadczenia atrybutów, w tym elektroniczne poświadczenia atrybutów przechowywane i udostępniane europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, związane z danymi, które mają być zawarte w wytwarzanych dokumentach w imieniu podmiotów publicznych odpowiedzialnych za źródło autentyczne. 2b. Wytwórca, o którym mowa w art. 2a, uzgadnia schemat wydawania elektronicznych poświadczeń atrybutów z właściwym ze względu na rodzaj atrybutów ministrem.”.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów nie są dokumentami publicznymi w ramach reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim.
193.	Uzupełnienie projektu ustawy o nowelizację art. 75e ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym	PWPW S.A.	Propozycja dodania wprost uprawnienia do wydawania atrybutów pochodzących z systemu, o którym mowa w art. 75e ust. 1 i 2 ustawy - Prawo o ruchu drogowym. Projekt powinien zostać uzupełniony o nowelizację art. 75e ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251, z późn. zm.), polegającą na dodaniu po ust. 2 ust. 2a i 2b w brzmieniu: „2a. Wytwórca dowodów rejestracyjnych zapewniający system teleinformatyczny, o którym mowa w ust. 1, wydaje oraz udostępnia elektroniczne poświadczenia atrybutów, w tym elektroniczne poświadczenia atrybutów przechowywane i udostępniane w europejskim portfelu tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, związane z danymi, które mają być zawarte w wytwarzanych dokumentach w imieniu podmiotów publicznych odpowiedzialnych za źródło autentyczne. 2b. Wytwórca, o którym mowa w ust. 2a, uzgadnia schemat wydawania elektronicznych poświadczeń atrybutów z właściwym ze względu na rodzaj atrybutów ministrem.”.	**Uwaga wyjaśniona** Europejski portfel tożsamości cyfrowej, jak i elektroniczne poświadczenia atrybutów nie są dokumentami publicznymi w ramach reżimu organizacyjno-prawnego ustanowionego na poziomie europejskim.