

## Nazwa dokumentu:

Projekt ustawy o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw UC122

Lp.	Organ wnoszący uwagi	Jednostka redakcyjna, do której wnoszone są uwagi	Treść uwagi	Propozycja zmian zapisu	Odniesienie do uwagi
1	RCL	Art. 1 pkt 13 w zakresie art. 22b ust. 17	Ponowić należy uwagę dotyczącą korekty wytycznych do upoważnienia zawartego w przepisie ust. 17, które w części nadal odnoszą się nie do opracowania wzoru, a do kwestii związanych ze „sprawnym przekazaniem danych” (wytyczne pozorne).	Korekta wytycznych	<b>Uwaga uwzględniona</b> Wytyczne zostaną zmodyfikowane zgodnie z uwagą.
2	RCL	Art. 1 pkt 14 w zakresie art. 23 pkt 16	Zgodnie z art. 5a ust. 9 rozporządzenia 910/2014 państwa członkowskie zapewniają, aby europejski portfel tożsamości cyfrowej mógł zostać unieważniony w następujących przypadkach: a) na wyraźne żądanie użytkownika; b) w przypadku bezpieczeństwa europejskiego portfela tożsamości cyfrowej zostało skompromitowane; c) po śmierci użytkownika lub zaprzestaniu działalności przez osobę prawną. Mając na uwadze powyższe, wyjaśnienia wymaga w jaki sposób minister właściwy do spraw informatyzacji będzie, zgodnie z projektowanym art. 23 pkt 16, zapewniał możliwość unieważniania europejskiego portfela tożsamości cyfrowej, a także - czy w tym zakresie nie należy wprowadzić szerszej regulacji uwzględniającej przypadki wskazane w art. 5a ust. 9 ww. rozporządzenia?		<b>Uwaga uwzględniona</b> Doprecyzowanie w zakresie lit. a i b znajdzie się w polityce certyfikacji, w zakresie lit. c w ustawie.
3	RCL	Art. 1 pkt 14 w zakresie art. 23 pkt 20	Mając na uwadze zadania ministra, o którym mowa w projektowanym art. 23 pkt 20 – <i>wykonywanie obowiązków, o których mowa w art. 48a rozporządzenia 910/2014 (m.in. wynikającego z ust. 3 tego artykułu obowiązku udostępniania danych statystycznych publicznie w otwartym i powszechnie używanym formacie nadającym się do odczytu maszynowego)</i> wyjaśnienia wymaga sposób lub miejsce udostępnienia przez ministra gromadzonych danych statystycznych dotyczących funkcjonowania europejskich portfeli tożsamości cyfrowej oraz kwalifikowanych usług zaufania dostarczanych lub świadczonych na terytorium RP.		<b>Uwaga uwzględniona</b> W uzasadnieniu, zostanie wskazane miejsce: danepubliczne.gov.pl
4	RCL	Art. 1 pkt 18 w zakresie art. 46a	Wskazany przepis ustanawiający podstawę nakładania administracyjnych kar pieniężnych wymaga	Uzupełnienie regulacji	<b>Uwaga uwzględniona</b>

			rozbudowania o wskazanie konkretnych przepisów lub obowiązków określonych w rozporządzeniu 910/2014, których naruszenie będzie powodowało powstanie odpowiedzialności administracyjnokarnej. Ogólne odesłanie w tym zakresie jedynie do naruszenia przepisów tego rozporządzenia nie realizuje w dostatecznym stopniu zasady określoności w odniesieniu do przepisów sankcyjnych.		Przepisy zostaną doprecyzowane zgodnie z uwagą.
5	RCL	Art. 4 pkt 7 w zakresie art. 20z ust. 2 pkt 1	Mając na uwadze katalog podmiotów publicznych zawarty w obecnie obowiązujących art. 2 ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz w art. 2 pkt 6 ustawy z dnia 18 listopada 2018 r. o doręczeniach elektronicznych, wyjaśnienia wymaga pozostawienie w projektowanym art. 20z ust. 2 pkt 1 regulacji wskazującej na dane <u>komornika sądowego</u> – jako podmiotu składającego wniosek o utworzenie konta.		<b>Uwaga uwzględniona</b> Regulacja dotycząca komornika sądowego zostanie wykreślona.
6	RCL	Art. 4 pkt 7 w zakresie art. 20zc pkt 2 i 3	Wskazany przepis przekazuje do uregulowania w akcie wykonawczym: 1) kwestię <u>szczegółowego sposobu utworzenia konta</u> podmiotu publicznego w Katalogu Podmiotów Publicznych przez ministra właściwego do spraw informatyzacji (art. 20zc pkt 2). Zauważyć jednak należy, że w projekcie brak regulacji ogólnych dotyczących sposobu tworzenia tego konta, które w przewidywanym akcie wykonawczym miałyby zostać uszczegółowione – proponowane przepisy przestają jedynie na wskazaniu przypadków, w których utworzenie konta nastąpi (proponowane art. 20y ust. 1 – na wniosek podmiotu publicznego, oraz art. 20y ust. 4 – z urzędu, jeżeli podmiot publiczny nie złoży w terminie wniosku o utworzenie konta); 2) <u>sposób zarządzania kontem administratora</u> podmiotu publicznego w Katalogu Podmiotów Publicznych – w tym przypadku projekt także nie zawiera regulacji dających podstawę do doprecyzowania sposobu zarządzania kontem administratora w rozporządzeniu – uregulowanie tej materii w akcie wykonawczym uzupełniałoby więc ustawę.	Uzupełnienie regulacji ustawowej o podstawowe unormowania spraw przekazanych do określenia w rozporządzeniu ministra właściwego do spraw informatyzacji.	<b>Uwaga uwzględniona</b> Po rozważeniu uwagi dotyczącej braku regulacji ogólnych w projekcie ustawy dotyczących sposobu tworzenia konta i sposobu zarządzania kontem administratora, należy uznać za niecelowe regulowanie szczegółowego sposobu utworzenia konta i zarządzania kontem w rozporządzeniu, tym samym zostanie skorygowany przepis upoważniający do wydania rozporządzenia tak, aby dotyczył jedynie kwestii określonych w ustawie.
7	RCL	Art. 7 pkt 4 w zakresie art. 14a ust. 6 pkt 1	Ponownie proponuje się doprecyzowanie przepisu w taki sposób, aby wskazywał (przez odesłanie do konkretnych przepisów), które dane osobowe użytkowników europejskiego portfela tożsamości cyfrowej będą przetwarzane przez ministra właściwego do spraw informatyzacji przez okres 20 lat od dnia unieważnienia	Uzupełnienie regulacji	<b>Uwaga uwzględniona</b> Dane zostaną wymienione.

			europejskiego portfela tożsamości cyfrowej – uwaga RCL nr 2.3.2 lit. a tiret siódme zgłoszona przy piśmie z dnia 3 kwietnia 2026 r.		
8	RCL	Art. 7 pkt 4 w zakresie art. 14c ust. 5 i 7	Podtrzymać należy uwagę w zakresie konieczności uzupełnienia ustawy o przepis ogólny dotyczący sposobu powiązania europejskiego portfela tożsamości cyfrowej osoby prawnej z europejskim portfelem tożsamości cyfrowej osoby fizycznej dysponującej tym portfelem, a także cofnięcia takiego powiązania. Proponowany nowy przepis ust. 5 nie powoduje uzupełnienia regulacji ustawowej w ww. zakresie – nie dotyczy „sposobu” powiązania, a jedynie stwierdza jego fakt – uwaga RCL nr 2.3.2 lit. c tiret drugie zgłoszona przy piśmie z dnia 3 kwietnia 2026 r.	Uzupełnienie regulacji o wskazanie ogólnego sposobu powiązania i cofnięcia powiązania.	<b>Uwaga uwzględniona</b> Ogólny sposób zostanie wskazany.
9	RCL	Art. 7 pkt 4 w zakresie art. 14e ust. 4	Zgodnie z projektowanym art. 14e ust. 4 minister wydaje decyzję, o której mowa w ust. 2 (wyrażenie zgody na świadczenie usługi umożliwiającej użytkownikom aplikacji mObywatel oraz europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych, zgodnie z art. 5a ust. 5 lit. g rozporządzenia 910/2014, w celach innych niż profesjonalne), po przeprowadzeniu testów integracyjnych zakończonych <u>pozytywnym wynikiem</u> , potwierdzających interoperacyjność świadczonej usługi z aplikacją mObywatel oraz europejskim portfelem tożsamości cyfrowej. W opinii RCL projektowaną regulację należy jednak uzupełnić o tryb postępowania i sposób rozstrzygnięcia w przypadku, gdy testy integracyjne zakończone zostaną wynikiem negatywnym. Nie jest jasne np. czy wydana zostanie w takim przypadku decyzja odmowna.	Uzupełnienie regulacji o tryb postępowania w przypadku negatywnego wyniku testu integracyjnego.	<b>Uwaga wyjaśniona</b> Projektodawca redagując przedmiotowy przepis nie zakładał takiej możliwości, że testy integracyjne zostaną zakończone po pierwszym uzyskaniu wyniku negatywnego. W opisanej procedurze wnioskodawcami będą profesjonalne, certyfikowane podmioty. Powyższe pozwala zatem przyjąć, że pozytywny wynik testu integracyjnego zostanie ostatecznie osiągnięty w ramach wzajemnej współpracy ministra z tymi podmiotami (testy integracyjne będą prowadzone aż do uzyskania skutku pozytywnego). Jednocześnie, przed zakończeniem testów integracyjnych minister nie będzie mógł wydać decyzji. Wartym odnotowania jest, że podobna sytuacja występuje obecnie w ramach procedury przyłączania systemu identyfikacji elektronicznej do węzła krajowego identyfikacji elektronicznej. Procedura ta również wymaga przeprowadzenia testów integracyjnych zakończonych wynikiem pozytywnym, o czym jest mowa w art. 21b ust. 1 pkt 2 zmienianej ustawy. W powyższym przypadku ustawodawca również nie przewidział przepisu dotyczącego trybu postępowania w przypadku negatywnego wyniku testu integracyjnego. Jednocześnie, dotychczasowe doświadczenie Ministerstwa Cyfryzacji, nabyte w ramach realizacji ww. przyłączeń, wskazuje, iż brak takiego przepisu nie stwarzał dotychczas żadnych problemów.

10	RCL	Art. 7 pkt 4 w zakresie art. 14e ust. 7	Mając na uwadze wyjaśnienia przedstawione przez Projektodawcę do uwagi RCL dotyczącej <i>ratio legis</i> wprowadzenia instytucji <u>wytycznych</u> ministra właściwego do spraw informatyzacji <u>do świadczenia usługi</u> umożliwiającej użytkownikom europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych w celach innych niż profesjonalne – <u>w drodze ich udostępnienia w BIP</u> (uwaga RCL nr 2.3.2 lit. e tiret drugie zgłoszona przy piśmie z dnia 3 kwietnia 2026 r.) oraz uwzględniając deklarację Projektodawcy o technicznym charakterze wytycznych, niezbędne jest wykazanie w uzasadnieniu, że treść wytycznych nie będzie <u>nakładała na dostawców usług nowych obowiązków świadczenia usług</u> – stanowić one będą, jak się wydaje, wskazówki bądź też rekomendacje w odniesieniu do określonych działań bądź też czynności.	Uzupełnienie uzasadnienia projektu.	<b>Uwaga uwzględniona</b> Uzasadnienie zostanie uzupełnione.
11	RCL	Art. 7 pkt 4 w zakresie art. 14e ust. 9 pkt 1	Przepisy projektu w dalszym ciągu należy uzupełnić o regulację ogólną dotyczącą „sposobu” świadczenia usługi, o której mowa w art. 14e ust. 1 – wyjaśnienia Wnioskodawcy wskazują, że odpowiednią regulacją ogólną przekazaną do uszczegółowienia w akcie wykonawczym, dla określenia „sposobu” świadczenia usługi, jest przepis art. 14e ust. 1, zgodnie jednakże stanowi jedynie, że minister właściwy do spraw informatyzacji <u>udostępnia usługę</u> , która umożliwia użytkownikom aplikacji mObywatel oraz europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 14 ust. 1, nieodpłatne składanie kwalifikowanych podpisów elektronicznych, zgodnie z art. 5a ust. 5 lit. g rozporządzenia 910/2014, w celach innych niż profesjonalne.	Proponuje się ponowne przeanalizowanie konieczności regulowania w akcie wykonawczym sposobu świadczenia usługi, o której mowa w art. 14e ust. 1, a w przypadku podtrzymania decyzji o dotychczasowym zakresie upoważnienia – rozbudowanie regulacji art. 14e o wskazanie ogólnego sposobu świadczenia tej usługi.	<b>Uwaga uwzględniona</b> Przepisy zostaną doprecyzowane.
12	MON	Art. 4 pkt 7 w zakresie dodania Rozdziału 3c	Zgodnie z projektowanym art. 20u ust. 3 pkt 1 lit. w i x ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne w Katalogu Podmiotów Publicznych przetwarza się dane podmiotów publicznych dotyczące szczegółowych informacji o wszystkich siedzibach podmiotu publicznego oraz komórkach organizacyjnych oraz dane dotyczące struktury organizacyjnej oraz jednostek obsługujących podmiot publiczny, zakresu nadrzędności i podrzędności podmiotów względem siebie. Proponowana zmiana ma na celu wyłączenie przetwarzania danych podmiotów podległych Ministrowi Obrony Narodowej w we wspomnianym zakresie w Katalogu Podmiotów	w projektowanym art. 20u ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne proponuje się dodać kolejny ustęp o treści: "Przepisów ust. 3 pkt 1 lit. w i x nie stosuje się do podmiotów podległych Ministrowi Obrony Narodowej."	<b>Uwaga uwzględniona</b> Przepis zostanie dodany.

			Publicznych. Dane dotyczące szczegółowych informacji o komórkach organizacyjnych oraz struktury organizacyjnej jednostek organizacyjnych podległych Ministrowi Obrony Narodowej (jednostki wojskowe wchodzące w skład Sił Zbrojnych RP) to dane wrażliwe i niecelowym jest ich przetwarzanie i agregacja w ramach Katalogu Podmiotów Publicznych.		
13	GUGiK	Art. 1 pkt 13 w zakresie art. 22b ust. 5, ust. 14 pkt 2 oraz ust. 17	GUGiK zwraca uwagę na potrzebę doprecyzowania zasad dokonywania wpisu do rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej w przypadku podmiotów publicznych prowadzących rozbudowane systemy teleinformatyczne, w ramach których udostępnianych jest wiele usług online o różnym charakterze, różnym celu przetwarzania danych oraz różnym zakresie danych lub atrybutów pozyskiwanych z europejskiego portfela tożsamości cyfrowej. Projektowany art. 22b wskazuje, że do rejestru wpisuje się strony ufające, natomiast jednocześnie przewiduje generowanie certyfikatów rejestracji strony ufającej portfelowi odpowiadających wpisom odnoszącym się do poszczególnych e-usług. W ocenie GUGiK zasadne jest jednoznaczne przesądzenie, czy wpis do rejestru powinien być dokonywany na poziomie podmiotu publicznego, systemu teleinformatycznego, czy konkretnej usługi online. Ma to szczególne znaczenie dla systemów portalowych o szerokim zakresie funkcjonalnym, takich jak Smart Geoportal, w których mogą być udostępniane zarówno usługi publiczne niewymagające identyfikacji użytkownika, jak i usługi wymagające uwierzytelnienia, dopasowania tożsamości albo pozyskania określonych atrybutów z europejskiego portfela tożsamości cyfrowej. Brak doprecyzowania może prowadzić do wątpliwości organizacyjnych i technicznych, w szczególności w zakresie sposobu wypełniania wniosku, liczby wymaganych wpisów, zakresu danych wskazywanych w rejestrze, aktualizacji wpisów oraz zapewnienia zgodności z zasadą minimalizacji danych. W ocenie GUGiK wpis do rejestru może dotyczyć podmiotu publicznego albo systemu teleinformatycznego, jednak zakres danych, cel ich wykorzystania oraz certyfikaty rejestracji powinny być określone na poziomie poszczególnych usług online lub przypadków użycia.	Dodanie w art. 22b ustępu 5a „5a. Jeżeli strona ufająca europejskiemu portfelowi tożsamości cyfrowej udostępnia w ramach jednego systemu teleinformatycznego więcej niż jedną e-usługę, wniosek, o którym mowa w ust. 3, wskazuje e-usługi, w których strona ufająca zamierza polegać na europejskim portfelu tożsamości cyfrowej, wraz z określeniem dla każdej z tych usług celu wykorzystania europejskiego portfela tożsamości cyfrowej oraz zakresu danych lub atrybutów pozyskiwanych od użytkownika. Dane te ujmuje się w rejestrze w sposób umożliwiający odrębne ustalenie zakresu danych lub atrybutów przetwarzanych w ramach poszczególnych usług online.”	<b>Uwaga wyjaśniona</b> Nie zachodzi potrzeba dodania ust. 5a do projektowanego art. 22b ustawy, gdyż kwestie podniesione w uwadze są uregulowane wprost w rozporządzeniu 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 uchylającym dyrektywę 1999/93/WE (Dz. U. UE. L. z 2014 r. Nr 257, str. 73, z późn. zm.) oraz 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). W uzasadnieniu do projektu ustawy projektodawca podkreślił, że obowiązkiem wynikającym z art. 5b rozporządzenia 910/2014 jest utworzenie rejestru podmiotów, które będą chciały świadczyć swoje usługi uwzględniające wykorzystanie europejskiego portfela tożsamości cyfrowej (rejestru stron ufających). „(...) Dlatego też zakłada się, że strony ufające będą mogły samodzielnie wpisywać się do rejestru i modyfikować swoje wpisy. Będą mogły w tym celu złożyć wniosek z wykorzystaniem formularza elektronicznego udostępnionego przez ministra właściwego do spraw informatyzacji. (...) Przewiduje się również zapewnienie możliwości składania wyżej wspomnianego wniosku, do ministra właściwego do spraw informatyzacji, za pośrednictwem kwalifikowanego dostawcy usług zaufania świadczącego usługę wydawania certyfikatów dostępu strony ufającej portfelowi lub certyfikatów rejestracji strony ufającej

				<p><i>portfelowi, o których mowa w rozporządzeniu 2025/848. Takie rozwiązanie umożliwi stronom ufającym załatwienie wszystkich formalności, niezbędnych do polegania na portfelu, (tj. wpisu do rejestru i uzyskania wyżej wspomnianych certyfikatów) w jednym miejscu”.</i></p> <p>Rejestr stron ufających stanowić będzie rejestr publiczny będący systemem teleinformatycznym, do którego strony ufające europejskiego portfela tożsamości cyfrowej będą wpisywać się (i dokonywać modyfikacje) samodzielnie (albo za pośrednictwem kwalifikowanego dostawcy usług) w oparciu o wniosek w postaci formularza elektronicznego udostępnionego przez ministra właściwego do spraw informatyzacji.</p> <p>Odnosząc się do pozostałej części uwagi, załącznik nr I do rozporządzenia wykonawczego 2025/848, stosuje liczbę mnoga i nakłada obowiązek na stronę ufającą europejskiemu portfelowi tożsamości cyfrowej by ta we wniosku o wpis do rejestru stron ufających, opisała rodzaje usług, które świadczy. Ponadto zgodnie z ust. 10 załącznika nr I rozporządzenia wykonawczego 2025/848, strona ufająca portfela musi dla każdego przypadku zamierzonego użycia - wskazać opis zamierzonego użycia danych, o które jako strona ufająca portfela zamierza występować do jednostek portfela.</p> <p>Jednocześnie w art. 5b ust. 2 lit. c rozporządzenia 910/2014 wskazano, że <i>“Proces rejestracji musi być efektywny kosztowo i proporcjonalny względem zagrożeń. Strona ufająca przekazuje co najmniej zamierzone używanie europejskich portfeli tożsamości cyfrowej, w tym wskazanie danych, o które strona ufająca będzie zwracać się do użytkowników”.</i></p> <p>Powyższy obowiązek obarczony jest przesłanką negatywną uregulowaną w art. 5b ust. 3 rozporządzenia 910/2014, zgodnie z którą: <i>“Strony ufające nie mogą zwracać się do użytkowników o udostępnienie jakichkolwiek danych innych niż te, które zostały wskazane zgodnie z ust. 2 lit. c”.</i></p>
--	--	--	--	--

14	GUGiK	Art. 1 pkt 13 w zakresie art. 22c	<p>Projektowany art. 22c ust. 1 nakłada na podmioty sektora publicznego odpowiedzialne za źródła autentyczne obowiązek zapewnienia kwalifikowanym dostawcom usług zaufania możliwości elektronicznej weryfikacji atrybutów. Przepis nie doprecyzowuje jednak, w jaki sposób należy ustalić, że dany podmiot publiczny jest odpowiedzialny za określone źródło autentyczne oraz za konkretny atrybut. W ocenie GUGiK samo prowadzenie rejestru publicznego, systemu teleinformatycznego lub repozytorium danych, jak również udostępnianie danych za pośrednictwem usług online, nie powinno automatycznie przesądzać o powstaniu obowiązków z art. 22c. Obowiązek ten powinien być każdorazowo powiązany z konkretnym źródłem autentycznym, konkretnym atrybutem oraz jednoznaczną podstawą prawną albo właściwym schematem poświadczania atrybutów.</p> <p>Doprecyzowanie ma szczególne znaczenie dla rejestrów, systemów teleinformatycznych i usług sieciowych z obszaru geodezji i kartografii, w tym systemów portalowych integrujących dostęp do różnych kategorii danych przestrzennych. Operator systemu udostępniającego dane lub integrującego usługi nie powinien być automatycznie utożsamiany z podmiotem odpowiedzialnym za źródło autentyczne dla każdego atrybutu, który może być pośrednio powiązany z danymi udostępnianymi przez ten system.</p> <p>Proponowana zmiana zwiększa pewność prawa, ogranicza ryzyko nadmiarowego rozszerzenia obowiązków technicznych i organizacyjnych po stronie podmiotów publicznych oraz wspiera zgodność projektowanych rozwiązań z zasadami legalizmu, przejrzystości, minimalizacji danych i rozliczalności.</p>	<p>W art. 22c ust. 1 otrzymuje brzmienie:</p> <p>„1. Podmioty sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014, odpowiedzialne na 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, o ile odpowiedzialność danego podmiotu za dane źródło autentyczne oraz zakres atrybutów podlegających weryfikacji wynikają z przepisów prawa Unii Europejskiej, przepisów prawa krajowego albo właściwego schematu poświadczania atrybutów.”</p> <p>Po ust. 2 dodaje się ust. 3 w brzmieniu:</p> <p>„3. Prowadzenie rejestru publicznego, systemu teleinformatycznego, repozytorium danych albo udostępnianie danych za pośrednictwem usług online nie przesądza o uznaniu podmiotu prowadzącego taki rejestr, system, repozytorium lub usługę za podmiot odpowiedzialny za źródło autentyczne w rozumieniu ust. 1 i 2, jeżeli</p>	<p><b>Uwaga wyjaśniona</b></p> <p>Nie zachodzi potrzeba zmiany brzmienia projektowanego art. 22c ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej. Przepis art. 3 pkt 7 rozporządzenia 910/2014 definiuje podmiot publiczny jako: <i>“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”</i>.</p> <p>Wykładnia językowa powyższego przepisu wyraźnie wskazuje, że jeśli podmiot sektora publicznego świadczy usługi o charakterze publicznych, posiada on z mocy rozporządzenia 910/2014 status podmiotu sektora publicznego. Podmioty sektora publicznego, w tym organy państwowe, regionalne czy lokalne np. jednostki samorządu terytorialnego, inne podmioty prawa publicznego lub podmioty (w tym podmioty prywatne) realizują zadania publiczne w oparciu o normę kompetencyjną wynikającą wprost z przepisu prawa powszechnie obowiązującego albo w drodze delegacji w postaci aktu powierzenia np. porozumienia czy umowy. Norma kompetencyjna wynikająca z konkretnego przepisu prawa powszechnie obowiązującego zobowiązuje jej adresata do realizowania ciążącego na nim obowiązku. Jeśli zaś norma ta zobowiązuje jej adresata do np. prowadzenia rejestru, będącego rejestrem publicznym, a tym samym do realizowania określonego, konkretnego zadania publicznego, to nie można stwierdzić, że podmiot ten nie może być zaliczony do podmiotu sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014.</p> <p>Jednocześnie warto dodać, że przepis art. 3 pkt 47 rozporządzenia 910/2014 nie precyzuje, jakie konkretnie repozytoria czy rejestry nie mogą</p>
----	-------	-----------------------------------	---	--	---

				odpowiedzialność ta nie wynika z przepisów prawa Unii Europejskiej, przepisów prawa krajowego albo właściwego schematu poświadczania atrybutów.”	stanowią podstawowych źródeł informacji o osobach fizycznych lub prawnych. W związku z powyższym, należy przyjmować, że z uwagi na brak na gruncie rozporządzenia 910/2014 przepisu wyłączającego w części jego stosowanie, poprzez źródła autentyczne trzeba rozumieć wszelkie repozytoria lub systemy, za prowadzenie których odpowiedzialne są podmioty sektora publicznego lub podmioty prywatne.
15	MSWiA	Art. 1 pkt 13 w zakresie art. 21a ust. 6a pkt 3	Zgodnie z projektowanym przepisem minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej, obejmujące: imiona rodziców osób oraz numer dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2. Pod rozważę poddaję się doprecyzowanie danych dotyczących dokumentu potwierdzającego tożsamość przez wskazanie rodzaju, serii i numeru tego dokumentu.		<b>Uwaga uwzględniona</b> Projektowany przepis zostanie uzupełniony o „rodzaj” dokumentu.
16	MSWiA	Art. 1 pkt 13 w zakresie art. 22a ust. 3 pkt 3	Zgodnie z projektowanym przepisem minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej, obejmujące: imiona rodziców osób oraz numer dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2. Pod rozważę poddaję się doprecyzowanie danych dotyczących dokumentu potwierdzającego tożsamość przez wskazanie rodzaju, serii i numeru tego dokumentu.		<b>Uwaga uwzględniona</b> Projektowany przepis zostanie uzupełniony o „rodzaj” dokumentu.
17	MSWiA	Uzasadnienie (str. 19-20)	W uzasadnieniu wskazano na zasadność włączenia do krajowego zestawu danych identyfikujących osobę numeru PESEL jako numeru jednoznacznie identyfikującego osobę fizyczną. Poruszono przy tym problem związany z negatywnymi skutkami polegania, w celu jednoznacznej identyfikacji osoby fizycznej, na zmiennych elementach, takich jak adres zamieszkania, adres email, czy nr telefonu komórkowego, które może spowodować uniemożliwienie ciągłego korzystania przez daną osobę z usług online po zmianie tych danych, a w szczególności uniemożliwienie dostępu do konta w systemie teleinformatycznym, w którym takie usługi są udostępniane. W ocenie projektodawcy rezygnacja z numeru PESEL, jako unikalnego identyfikatora osoby fizycznej, i poleganie w tym zakresie na elementach	W związku z powyższymi wyjaśnieniami zasadnym jest usunięcie z uzasadnienia (s. 20) zdania: „Innym dobrze ilustrującym przykładem konsekwencji polegania na zmiennych danych są problemy z dostępem do usług online, jakie mają osoby fizyczne po zmianie numeru PESEL.”	<b>Uwaga uwzględniona</b> Wskazane zdanie zostanie usunięte z uzasadnienia.



			<p>zmiennych, takich jak opisane powyżej, wiązałoby się nie tylko z istotnymi problemami użytkowników w dostępie do ich danych zgromadzonych w rejestrach publicznych i systemach teleinformatycznych podmiotów publicznych, ale prowadziłoby również do konieczności kosztownej przebudowy większości usług publicznych, poprzedzonej zmianami przepisów prawa regulujących funkcjonowanie tych usług.</p> <p>Niespójne z powyższymi wyjaśnieniami jest zawarte w uzasadnieniu sformułowanie w brzmieniu „Innym dobrze ilustrującym przykładem konsekwencji polegania na zmiennych danych są problemy z dostępem do usług online, jakie mają osoby fizyczne po zmianie numeru PESEL”. Wskazać przy tym należy, że zgodnie z art. 19 ustawy o ewidencji ludności zmiana numeru PESEL możliwa jest wyłącznie w trzech przypadkach:</p> <ol style="list-style-type: none"> <li>1) sprostowania daty urodzenia;</li> <li>2) zmiany płci;</li> <li>3) nadania numeru PESEL na skutek omyłki organu administracji publicznej mającej wpływ na numer PESEL lub wprowadzenia w błąd organu administracji publicznej co do tożsamości osoby.</li> </ol> <p>Numer PESEL jest zatem, co do zasady, przypisany osobie fizycznej przez całą jej życie i tylko w wyjątkowych sytuacjach określonych przepisami prawa może ulec zmianie.</p>		
18	MSWiA	OSR	<p>Uzupełnienia OSR przez ujęcie Ministra Spraw Wewnętrznych i Administracji jako podmiotu, na który wpływa projektowana zmiana ustawy w obszarze Systemu Rejestracji Broni (SRB), a w konsekwencji zagwarantowanie dla MSWiA dodatkowych środków w szacowanej kwocie 2 mln PLN, w zakresie rozwoju SRB.</p> <p>Minister SWiA jest ustawowym Administratorem Sytemu Rejestracji Broni, uregulowanego w ustawie z dnia 13 czerwca 2019 r. o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym (Dz.U. z 2023 r. poz. 1743). System ten wpisuje się w usługi zaufania, z uwagi na jego przewidziane połączenie z systemem PESEL, jak również ewentualne udostępnienie usługi związanej z wydawaniem zaświadczeń dla posiadaczy broni w trybie elektronicznym w ramach planowanych usług</p>	<p>Uzupełnienie pkt 4 i 6 OSR poprzez uwzględnienie oddziaływania projektu na Ministra Spraw Wewnętrznych i Administracji w obszarze Systemu Rejestracji Broni (SRB) i zagwarantowania dla MSWiA dodatkowych środków w szacowanej kwocie 2 mln PLN, w zakresie rozwoju SRB.</p>	<p><b>Uwaga wyjaśniona</b></p> <p>Wskazana kwestia w zakresie, w jakim dotyczy udostępnienia usługi związanej z wydawaniem zaświadczeń dla posiadaczy broni w trybie elektronicznym – w ramach planowanych usług dostępnych w aplikacji mObywatel, pozostaje poza zakresem niniejszego aktu prawnego, gdyż projektowane przepisy nie zobowiązują do udostępnienia takiej usługi.</p> <p>Przepisy rozporządzenia 910/2014, nakładają na państwa członkowie obowiązek wyłącznie w zakresie zgłoszenia określonych rodzajów atrybutów polegających na publicznych źródłach autentycznych do katalogu Komisji Europejskiej, ze wskazaniem adresu elektronicznego, pod którym można zweryfikować te atrybuty oraz udostępnienia publicznych źródeł autentycznych kwalifikowanym dostawcom usług zaufania tak, aby mogli oni, na żądanie użytkownika portfela,</p>

			<p>dostępowych w aplikacji mObywatel. W związku z powyższym niezbędne jest zagwarantowanie dla MSWiA dodatkowych środków w szacowanej wartości 2 mln. PLN, które umożliwią realizację ww. usługi</p>		<p>potwierdzić atrybuty odnoszące się do tego użytkownika, o czym mowa w art. 45e rozporządzenia 910/2014.</p> <p>Udostępnienie konkretnej usługi odnoszącej się do np. Systemu Rejestracji Broni w ramach europejskiego portfela tożsamości cyfrowej ma wyłącznie fakultatywny charakter.</p> <p>Projektodawcy celowo nie wymienili katalogu rodzaju usług albo rejestrów publicznych, za które odpowiadają podmioty publiczne, gdyż może on w przyszłości ulec zmianie na skutek np. powstania nowych rejestrów. W związku z tym wskazywanie Systemu Rejestracji Broni w OSR jest niezasadne.</p>
--	--	--	--	--	---

19	MEN/CIE	<p>Art. 1 w zakresie art. 22c ust. 1 w zw. z art. 12 oraz art. 11 (ustawa zmieniana w art. 1; przepisy finansowe i przejściowe)</p>	<p><b>Luka implementacyjna: brak wskazania podmiotów odpowiedzialnych za atrybuty edukacyjne.</b></p> <p>Art. 22c ust. 1 nakłada obowiązek zapewnienia API weryfikacji atrybutów na „podmioty sektora publicznego odpowiedzialne na poziomie krajowym za źródła autentyczne, o których mowa w załączniku VI do rozporządzenia 910/2014”. Żaden przepis polskiego prawa nie wskazuje wprost, który organ jest podmiotem odpowiedzialnym za atrybuty edukacyjne (kwalifikacje, statusy uczniów i nauczycieli) wymienione w tym załączniku. Ustawa o systemie oświaty wskazuje ministra właściwego ds. oświaty jako prowadzącego SIO i SIOEO, jednak nie posługuje się pojęciem „podmiotu odpowiedzialnego za źródło autentyczne” w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014. Tworzy to lukę implementacyjną: nie wiadomo, kto jest adresatem obowiązku z art. 22c i kto odpowiada za jego wykonanie.</p> <p><b>Brak finansowania i nierealistyczny termin.</b></p> <p>Niezależnie od rozstrzygnięcia powyższej kwestii, wykonanie obowiązku z art. 22c przez MEN/CIE wymaga: budowy interfejsów API atrybutowych dla SIO i SIOEO, wdrożenia mechanizmów logowania i rozliczalności (RODO), uzyskania certyfikatów pieczęci elektronicznej oraz zapewnienia SLA. Są to działania infrastrukturalne wymagające co najmniej 12–18 miesięcy, a zatem niemożliwe do ukończenia do 24 grudnia 2026 r. Art. 9 przyznaje podmiotom publicznym czas do 31 grudnia 2027 r. na przyłączenie do systemu scentralizowanego, jednak obowiązek API atrybutów z art. 22c nie posiada analogicznego okresu przejściowego. Art. 11 określa limit wydatków wyłącznie dla ministra ds. informatyzacji. Koszty dostosowania SIO i SIOEO nie są ujęte w OSR ani w budżecie MEN na lata 2026–2027.</p>	<p><b>1)</b> Dodanie w projekcie ustawy lub w aktach wykonawczych przepisu wskazującego ministra właściwego ds. oświaty i wychowania jako podmiot odpowiedzialny za źródła autentyczne w zakresie atrybutów edukacyjnych z załącznika VI do rozporządzenia 910/2014, obejmujących co najmniej: dane uczniów i status edukacyjny (SIO) oraz zaświadczenia dot. wyników egzaminów państwowych (SIOEO).</p> <p><b>2)</b> Dodanie w przepisach przejściowych okresu przejściowego na uruchomienie API weryfikacji atrybutów przez podmioty sektorowe – do dnia 31 grudnia 2027 r., spójnie z terminem z art. 9 ust. 1.</p> <p><b>3)</b> Uzupełnienie OSR o analizę kosztów po stronie podmiotów sektorowych odpowiedzialnych za atrybuty z załącznika VI, przeprowadzoną we współpracy z właściwymi ministrami, oraz wskazanie mechanizmu finansowania tych kosztów – np. rezerwy celowej w ustawie budżetowej na rok 2027.</p>	<p><b>Ad 1. Uwaga wyjaśniona</b></p> <p>Nie ma potrzeby dodawania w projekcie ustawy przepisów wskazujących poszczególnych ministrów jako podmioty odpowiedzialne za określone źródła autentyczne, ponieważ wynika to łącznie z przepisów rozporządzenia 910/2014 i przepisów krajowych ustanawiających określone repozytoria lub systemy, za prowadzenie, których odpowiedzialne są określone podmioty.</p> <p>Jeżeli wskazane w przepisach krajowych repozytoria lub systemy zawierają atrybuty, o których mowa w załączniku VI do rozporządzenia 910/2014 i są prowadzone przez podmioty sektora publicznego w rozumieniu tego rozporządzenia - to znaczy, że te podmioty są zobowiązane. Nie ma tu zatem luki prawnej, ponieważ przepisy rozporządzeń parlamentu i rady stosuje się bezpośrednio.</p> <p><b>Ad. 2. Uwaga wyjaśniona</b></p> <p>Przepisy dotyczące udostępnienia źródeł autentycznych przez podmioty sektora publicznego odpowiedzialne za takie źródła są znane od kwietnia 2024 r., gdyż zostały wprowadzone rozporządzeniem 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 (Dz. U. UE. L. z 2024 r. poz. 1183). Szczegółowe kwestie w tym zakresie reguluje rozporządzenie wykonawcze 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.).</p> <p>Przykładowo w art. 7 ust. 3 wymaga się, aby państwa członkowskie składały wnioski</p>
----	---------	---	---	---	---

					<p>o włączenie atrybutów wymienionych w załączniku VI do rozporządzenia 910/2014 do katalogu atrybutów, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych do celów weryfikacji przez kwalifikowanych dostawców usług zaufania. Znaczy to że przepisy w tym zakresie nie są zaskoczeniem i co za tym idzie znacząco późniejsze dostosowania krajowych źródeł autentycznych do wymogów określonych w rozporządzeniu 910/2014 może nie być możliwe ze względów formalnych. Tym niemniej należy nadmienić, że należy się spodziewać, że przepisy europejskie w tym, zakresie będą z pewnością stosowane elastycznie, podobnie jak to było w przypadku pierwszej wersji rozporządzenia 910/2014. Należy jednak zauważyć, że Komisja Europejska zgodnie z art. 7 ust. 2 rozporządzenia 2025/1569 ocenia wnioski składane przy użyciu systemu, o którym mowa w ust. 1, o włączenie atrybutu do katalogu atrybutów lub o modyfikację atrybutu w katalogu atrybutów po uwzględnieniu wszelkich porad udzielonych przez grupę współpracy.</p> <p><b>Ad. 3. Uwaga wyjaśniona</b>  Rozporządzenie wykonawcze Komisji (UE) 2025/1569 z dnia 29 lipca 2025 nie przesądza sposobu weryfikacji atrybutów. Należy tu przytoczyć przepisy art. 7 ust.5 lit. h w kontekście przepisu art. 9 ust. 1. Przepis art. 9 ust. 1 przewiduje możliwość udostępnienia przez państwa członkowskie pojedynczych punktów weryfikacji atrybutów wymienionych w załączniku VI, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych w sektorze publicznym. Projekt ustawy nie przewiduje jednak utworzenia takiego punktu w uwagi na to, że Polsce nie funkcjonuje jeszcze podobne rozwiązanie na poziomie krajowym, umożliwiające integrację wszelkich autentycznych publicznych źródeł danych, które mogłoby być wykorzystane w celu o którym mowa w art. 45e rozporządzenia</p>
--	--	--	--	--	--

					<p>910/2014 oraz art. 9 ust. 1 rozporządzenia 2025/1569.</p> <p>W związku z tym zgodnie z przepisem art. 7 ust. 5 lit. h wymagającym aby wniosek o włączenie atrybutu do katalogu lub modyfikację atrybutu w zawierał informację o punkcie weryfikacji atrybutu na poziomie krajowym lub link do opisu sposobu składania wniosków o weryfikację, łącznie z projektowanym przepisem art. 22h ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej, to podmioty odpowiedzialne za źródła autentyczne zdecydują zgodnie z posiadaną wiedzą na temat źródeł, którymi zarządzają i spodziewanym zakresem wnioskowania o weryfikację atrybutów o sposobie składania wniosków o weryfikację oraz wskażą link do opisu tego sposobu.</p> <p>Tym samym, ujęcie w jednej ustawie wszelkich źródeł autentycznych mając na uwadze, że mogą one dotyczyć wszelkich atrybutów w rozumieniu art. 3 pkt 43 rozporządzenia 910/2014 nie jest możliwe, gdyż mogłaby się odnosić do każdej dziedziny życia. Ponadto, taka ustawa musiałaby być każdorazowo nowelizowana ilekroć pojawiłby się jakiegokolwiek przepisy sektorowe dotyczące repozytoriów publicznych lub systemów teleinformatycznych w których przetwarzane byłby dane w rozumieniu art. 3 pkt 43 rozporządzenia 910/2014.</p>
20	MEN/CIE	Art. 1 w zakresie art. 22d	<p><b>Brak terminu i procedury zgłaszania atrybutów edukacyjnych do katalogu Komisji Europejskiej.</b></p> <p>Art. 22d przewiduje, że podmiot odpowiedzialny za źródło autentyczne składa do ministra ds. informatyzacji wniosek o zgłoszenie atrybutów do katalogu KE. Przepis nie określa: terminu złożenia wniosku przez podmioty sektorowe; procedury koordynacji między ministerstwami sektorowymi a ministrem ds. informatyzacji; ani konsekwencji niezłożenia wniosku. Brak zgłoszenia atrybutów edukacyjnych do katalogu KE w odpowiednim czasie oznacza, że polscy uczniowie, absolwenci i nauczyciele nie będą mogli</p>	<p><b>1)</b> Dodanie w art. 22d ust. 4 (nowy) terminu składania wniosków przez podmioty sektorowe – proponowany termin: 6 miesięcy od dnia wejścia w życie ustawy lub od dnia formalnego wskazania podmiotu odpowiedzialnego.</p> <p><b>2)</b> Wskazanie w przepisach wykonawczych lub uzasadnieniu obowiązku wyznaczenia przez ministra ds. informatyzacji</p>	<p><b>Uwaga wyjaśniona</b></p> <p>Przepis celowo nie określa terminu składania wniosków.</p> <p>Przyjmuje się założenie, że wnioski zostaną złożone przez właściwe podmioty sektora publicznego w rozumieniu rozporządzenia 910/2014, gdy tylko odpowiednie rozwiązania przygotowane przez te podmioty będą gotowe. Warto zauważyć, że ze złożonej uwagi wynika Ministerstwo Edukacji Narodowej dostrzega nie tylko potrzebę zgłoszenia określonych źródeł autentycznych istotnych transgranicznie, ale</p>

			<p>potwierdzać swoich kwalifikacji i uprawnień w EUDI Wallet transgranicznie. Jest to szczególnie istotne w kontekście programu Erasmus.</p> <p>Atrybuty edukacyjne wymagające zgłoszenia obejmują co najmniej: mLegitymację szkolną (education_id) i status ucznia/nauczyciela z SIO, zaświadczenie wyników egzaminu E8, maturalnego, eksternistycznego.</p> <p>Uwaga zachowuje aktualność pod warunkiem uprzedniego formalnego wskazania MEN jako podmiotu odpowiedzialnego za atrybuty edukacyjne (zob. Uwaga 1 pkt 1).</p>	<p>koordynatora przyjmującego, opiniującego i przekazującego do KE wnioski ministerstw sektorowych.</p>	<p>również to, że jest podmiotem odpowiedzialnym za te źródła.</p> <p>Nie ma zatem potrzeby ustanawiania przepisów krajowych szczegółowo wskazujących, że określony rejestr/ system/ jest źródłem autentycznym w rozumieniu rozporządzenia 910/2014, a inny nie jest.</p> <p>Brak jest też na obecnym etapie wypracowanej praktyki na poziomie europejskim. Nie wiadomo, jak sprawnie będzie przebiegało zgłaszanie źródeł autentycznych do Komisji oraz, co również ma znaczenie dla wydawania ważnych w całej UE elektronicznych poświadczeń atrybutów, schematów poświadczania atrybutów na podstawie takich źródeł.</p>
21	MEN/CIE	<p>Art. 7 w zakresie</p> <p>Art. 14b ust. 1 oraz art. 14g ust. 1 lit. d</p>	<p><b>Dwie niezależne luki regulacyjne dotyczące dzieci: brak możliwości posiadania portfela poniżej 13. roku życia bez mechanizmu zastępczego oraz brak przepisów szczególnych dla użytkowników 13–18 lat.</b></p> <p><b><u>Problem 1. Dzieci poniżej 13. roku życia – wykluczenie z EUDI Wallet bez mechanizmu zastępczego.</u></b></p> <p>Art. 14b ust. 1 uzależnia możliwość posiadania EUDI Wallet od posiadania co najmniej ograniczonej zdolności do czynności prawnych, którą nabywa się z ukończeniem 13 lat (art. 15 k.c.). Dzieci poniżej 13. roku życia są tym samym z mocy prawa wykluczone z posiadania własnego portfela.</p> <p>Tymczasem mLegitymacja szkolna – jedno z kluczowych elektronicznych poświadczeń atrybutów planowanych do wdrożenia w EUDI Wallet – jest wydawana uczniom od klasy I szkoły podstawowej, tj. od ok. 7. roku życia. Systemy CIE (np. SIO) gromadzą dane uczniów od momentu objęcia ich obowiązkiem szkolnym. Projekt nie przewiduje żadnego mechanizmu umożliwiającego reprezentację atrybutów edukacyjnych dziecka poniżej 13 lat w EUDI Wallet – ani przez portfel dziecka (niemożliwy), ani przez portfel rodzica w roli cyfrowego nośnika tożsamości dziecka (art. 14g ust. 1 lit. d służy weryfikacji uprawnień rodzicielskich, nie reprezentacji tożsamości dziecka).</p>	<p><b>1)</b> Rozważenie wprowadzenia mechanizmu umożliwiającego reprezentację atrybutów edukacyjnych dzieci poniżej 13. roku życia w EUDI Wallet za pośrednictwem portfela rodzica/opiekuna jako ich przedstawiciela ustawowego – z wyraźnym rozróżnieniem tej roli od uprawnienia z art. 14g ust. 1 lit. d (weryfikacja uprawnień rodzicielskich). Alternatywnie: wskazanie innego mechanizmu cyfrowego potwierdzania tożsamości dzieci poniżej 13 lat w usługach publicznych, w tym w systemach oświatowych.</p> <p><b>2)</b> Dodanie w projekcie ustawy lub w aktach wykonawczych przepisów szczególnych dla użytkowników EUDI Wallet w wieku 13–18 lat, obejmujących co najmniej: zasady weryfikacji tożsamości bez dowodu osobistego; zakres zgody na przetwarzanie danych; katalog</p>	<p><b>Ad. 1. Uwaga wyjaśniona</b></p> <p>Zmienione w 2024 r. rozporządzenie 910/2014 przewiduje możliwość istnienia środków identyfikacji elektronicznej osoby fizycznej reprezentującej inną osobę fizyczną (zob. definicje w art. 3 pkt 1-3). Takie środki identyfikacji elektronicznej mogą zatem dotyczyć nie tylko relacji rodzice-dzieci, ale mogą być również bardzo przydatne w przypadku opiekunów osób starszych lub wykluczonych cyfrowo.</p> <p>Nie wymaga się jednak tworzenia takich środków. Art. 5a ust. 1 rozporządzenia 910/2014 wymaga jedynie zapewnienia europejskiego portfela tożsamości cyfrowej wszystkim osobom fizycznym i prawnym, Jak wynika za spotkań roboczych w ramach Europejskiej Grupy Współpracy ds. Tożsamości Cyfrowej<sup>1</sup> dla większości państw członkowskich UE wyzwaniem będzie zapewnienie w terminie rozwiązań wymaganych.</p> <p>Zagadnienia te z pewnością będą w przyszłości przedmiotem dalszych prac.</p> <p><b>Ad. 2. Uwaga wyjaśniona</b></p> <p>Nie ma potrzeby dodawania specjalnych przepisów potwierdzenia tożsamości dla osób w</p>

<sup>1</sup> Zob. <https://digital-strategy.ec.europa.eu/pl/policies/european-digital-identity-cooperation-group>

			<p><b><u>Problem 2. Dzieci w wieku 13–18 lat – brak przepisów szczególnych dla użytkowników portfela.</u></b></p> <p>Art. 14b ust. 1 dopuszcza posiadanie EUDI Wallet od 13. roku życia, jednak projekt nie zawiera przepisów szczególnych regulujących: zasad weryfikacji tożsamości małoletniego (brak dowodu osobistego przed 18. rokiem życia jako domyślnej metody); zakresu zgody na przetwarzanie danych (rodzic/opiekun vs. sam małoletni w świetle art. 8 RODO); katalogu atrybutów i usług dostępnych dla małoletniego bez zgody opiekuna. Ponadto art. 14g ust. 1 lit. d, uprawniający rodzica do pobierania z portfela danych o sytuacji prawnej dziecka, nie precyzuje: czy zakres obejmuje wrażliwe dane edukacyjne z SIO (orzeczenia o kształceniu specjalnym, opinie psychologiczno-pedagogiczne, dane o niepełnosprawności); jak rozstrzygnąć konflikt między uprawnieniem rodzica a wolą dziecka powyżej 13. roku życia posiadającego własny portfel; czy dane pobrane przez rodzica mogą być przechowywane w portfelu i udostępniane stronom trzecim. Obie luki są bezpośrednio istotne dla sektora edukacji: mLegitymacja szkolna obejmuje uczniów od 7 do 19 roku życia, a systemy ZPE i eDziennik obsługują zarówno rodziców dzieci poniżej 13 lat, jak i samodzielnych użytkowników w wieku 13–19 lat.</p>	<p>atrybutów i usług dostępnych bez zgody opiekuna.</p> <p><b>3)</b> Doprecyzowanie art. 14g ust. 1 lit. d przez wskazanie, że pobieranie danych dziecka przez rodzica odbywa się wyłącznie w zakresie i na zasadach określonych przepisami właściwymi dla danego rejestru źródłowego, z ich pierwszeństwem stosowania – w szczególności przepisów ustawy o systemie oświaty w zakresie wrażliwych danych uczniów.</p> <p><b>4)</b> Zasięgnięcie opinii ministra właściwego ds. oświaty i wychowania przy opracowywaniu przepisów i wytycznych dotyczących obu grup wiekowych.</p>	<p>wieku 13-18 lat bez dowodu osobistego (lub paszportu), jak również katalogu atrybutów i usług dostępnych bez zgody opiekuna. Już obecnie obywatelki i obywatele RP w wieku 13-18 lat mają prawo (za zgodą opiekunów) do uzyskania dowodu osobistego z warstwą elektroniczną, co znaczy, że otrzymają wraz z takim dowodem osobistym profil osobisty. Profil osobisty jest środkiem identyfikacji elektronicznej zgodnym z wysokim poziomem bezpieczeństwa. Mimo, że nie ma żadnych ustawowych ograniczeń dotyczących usług dla nieletnich posiadaczy profilu osobistego nie są nam znane żadne problemy z tego wynikające. Profil osobisty zawiera bowiem datę urodzenia, co pozwala w usługach online (jeżeli przepisy dotyczące tych usług takich ograniczeń wymagają) na odpowiednie działanie tych usług. Podobnie będzie w przypadku europejskiego portfela tożsamości cyfrowej.</p> <p><b>Ad 3. Uwaga wyjaśniona</b> Nie ma takiej potrzeby z uwagi na ogólną zasadę pierwszeństwa przepisów szczegółowych nad przepisami ogólnymi co potwierdza również art. 8 ust. 3 lit d, f i h rozporządzenia 2025/1569.</p> <p><b>Ad. 4. Uwaga wyjaśniona</b> Uzgodnienia projektów wszelkich przepisów z ministrami są prowadzone.</p>
22	MEN/CIE	Art. 1 w zakresie art. 22i ust. 2 w zw. z art. 22f–22h	<p><b>Brak obowiązku ministra ds. informatyzacji do powiadomienia podmiotów sektorowych o ścieżce art. 22i oraz o terminach działania.</b></p> <p>Art. 22i ust. 1 przewiduje, że podmioty odpowiedzialne za źródła autentyczne mogą wnioskować do ministra ds. informatyzacji o wydawanie przez niego EPoA w EUDI Wallet w imieniu tych podmiotów. Jest to kluczowy mechanizm umożliwiający m.in. wdrożenie cyfrowej mLegitymacji szkolnej i zaświadczeń egzaminacyjnych w EUDI Wallet.</p> <p>Przepis ma charakter wyłącznie fakultatywny ("mogą") po stronie inicjatywy podmiotów sektorowych. Żaden przepis nie zobowiązuje ministra ds. informatyzacji do powiadomienia ministrów sektorowych o istnieniu tej ścieżki, jej wymaganiach formalnych ani sugerowanych</p>	<p><b>1)</b> Dodanie w przepisach przejściowych lub w uzasadnieniu obowiązku ministra ds. informatyzacji do pisemnego powiadomienia ministrów sektorowych (w tym ministra właściwego ds. oświaty) o możliwości i wymaganiach złożenia wniosku z art. 22i, w terminie 30 dni od dnia wejścia w życie ustawy.</p> <p><b>2)</b> Wskazanie w uzasadnieniu lub w piśmie okólnym, że minister ds. oświaty i wychowania jest podmiotem</p>	<p><b>Ad. 1 i 2. Uwaga wyjaśniona</b> Minister Edukacji będzie mógł, na podstawie wskazanego przepisu, wnioskować do Ministra Cyfryzacji o wydawanie w jego imieniu elektronicznych poświadczeń atrybutów, jeżeli tylko będzie gotowy w zakresie określenia wymaganego w takim przypadku schematu poświadczania atrybutów i przygotowania źródła autentycznego danych odpowiednio do tego schematu.</p> <p>Nie ma powodu pisemnego powiadomienia ministrów sektorowych o możliwości złożenia wniosku.</p> <p>To w tym wniosku, zgodnie z przepisem art. 22i ust. 2 pkt 1 powinno znaleźć się wskazanie:</p>

			terminach działania. W praktyce podmioty sektorowe mogą nie wiedzieć o konieczności podjęcia inicjatywy lub podjąć ją za późno, by atrybuty edukacyjne znalazły się w katalogu KE wraz z uruchomieniem portfela. Bez aktywnego działania MEN w trybie art. 22i Polska uruchomi EUDI Wallet 24 grudnia 2026 r. bez żadnych poświadczeń edukacyjnych, podczas gdy inne państwa UE (m.in. Estonia, Niemcy) aktywnie wdrażają odpowiedniki legitymacji szkolnych i zaświadczeń kwalifikacyjnych do swoich portfeli.	uprawnionym do złożenia wniosku z art. 22i w odniesieniu do mLegitymacji szkolnej i zaświadczeń egzaminacyjnych jako EPoA w EUDI Wallet.	- w przypadku poświadczenia atrybutów ważnego w całej UE - odpowiedniego schematu poświadczenia atrybutów w katalogu, o którym mowa w art. 8 rozporządzenia 2025/1569 (a takim schemacie, zgodnie z art. 8 ust. 3 lit d, musi się znaleźć odniesienie do konkretnych przepisów, norm lub wytycznych, w przypadku gdy wydanie, walidacja lub stosowanie elektronicznego poświadczenia atrybutów w ramach schematu podlega tym przepisom, normom lub wytycznym), - w przypadku poświadczenia atrybutów ważnego w kraju - odniesienie do przepisów, norm lub wytycznych, jeżeli mają zastosowanie. Nie ma potrzeby powtarzania przepisów sektorowych ustanawiających określone repozytoria i systemy teleinformatyczne do przechowywania określonych danych i informacji, oraz podmiotów odpowiedzialnych za te źródła w przepisach projektu ustawy.
23	MEN	Art. 4 pkt 7	W dodawanym art. 20u ust. 3 pkt 1 lit. v jest mowa, że w Katalogu Podmiotów Publicznych będzie przetwarzany numer szkoły lub placówki oświatowej, o którym mowa w art. 7 ust. 1 pkt 29 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2024 r. poz. 152, z późn. zm. ). Zgodnie z art. 7 ust. 1a pkt 10 ww. ustawy w Rejestrze Szkół i Placówek Oświatowych (RSPO) jest gromadzony także numer RSPO zespołu szkół i placówek oświatowych. Jeśli w Katalogu Podmiotów Publicznych będą funkcjonowały także zespoły szkół i placówek oświatowych, proponuje się uwzględnienie numeru zespołu w lit. v.	„v) numer szkoły lub placówki oświatowej oraz numer zespołu szkół i placówek oświatowych, o których mowa odpowiednio w art. 7 ust. 1 pkt 29 oraz ust. 1a pkt 10 ustawy z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej (Dz. U. z 2024 r. poz. 152, z późn. zm.),”	<b>Uwaga uwzględniona</b> Przepis zostanie zmodyfikowany zgodnie z uwagą.
24	MFiG	Art. 5 w zakresie art. 36 ust. 1 pkt 1 lit. d	Nowelizacja polega między innymi na dodaniu do art. 36 u.o.p.p.f.t. kolejnych rodzajów danych służących w ocenie projektodawcy <b>identyfikacji klienta</b> (obok serii i numeru dowodu stwierdzającego tożsamość). Dane te to zgodnie z projektem niepowtarzalny identyfikator, osobisty numer identyfikacyjny albo numer dokumentu – w każdym przypadku są to dane określone w Rozporządzeniu 910/2014 lub jego aktach wykonawczych. W tym miejscu należy jednak zwrócić uwagę na art. 22 Rozporządzenia 2024/1624 w sprawie <i>zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu</i> . Przepis ten wejdzie w życie 10 lipca 2027 r. Art. 22 ust. 1 tego	Proponujemy rozważenie zrezygnowania z nowelizacji u.o.p.p.p.f.t. ujętej w art. 5 projektu.	<b>Uwaga wyjaśniona</b> Zgodnie z istotą rozporządzenia 910/2014, wyrażoną w motywie 12 „jednym z celów niniejszego rozporządzenia jest zniesienie, przynajmniej w przypadku usług publicznych, istniejących barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich w celu uwierzytelniania. Celem niniejszego rozporządzenia nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich. Jego celem jest



			rozporządzenia wskazuje na katalog informacji, które mogą zostać wykorzystane właśnie do identyfikacji klienta – <b>a wśród nich nie znajdują się ww. dane objęte nowelizacją.</b> Tego rodzaju informacje służą natomiast zgodnie z art. 22 ust. 6 lit. b <b>weryfikacji tożsamości klienta.</b> Identyfikacja, a następnie weryfikacja danych stanowią wyróżnione prawnie procesy. W porządku krajowym odpowiada temu art. 36 i 37 u.o.p.p.p.f.t. Nadmienić należy, że art. 37 u.o.p.p.p.f.t. regulujący zasady weryfikacji tożsamości, zawiera już odesłanie do Rozporządzenia 910/2014. Powyższe twierdzenia zdaje się również potwierdzać konsultowany obecnie dokument <i>Draft Regulatory Technical Standards under Article 28(1) of Regulation (EU) 2024/1624</i> , który jasno opisuje źródła informacji wykorzystywane do weryfikacji danych. Odwołanie do Rozporządzenia 910/2014 pojawia się w tym dokumencie w części „ <i>Verification measures conducted on a non-face-to-face basis</i> ”.		zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania na potrzeby dostępu do transgranicznych usług online oferowanych przez państwa członkowskie”. Przepisy projektowanej ustawy mają na celu doprecyzowanie danych identyfikujących klienta w zakresie numeru identyfikacyjnego europejskiego środka identyfikacji elektronicznej, który będzie stanowił odpowiednik serii i numeru dokumentu tożsamości w procesach identyfikacji i weryfikacji tożsamości. Jednocześnie projektowany przepis stanowi odpowiedź na liczne postulaty wyrażone w trakcie procesu legislacyjnego, wyrażone przez podmioty reprezentujące sektor bankowy. Tym samym proponuje się pozostawić proponowany przepis w dotychczasowym brzmieniu.
25	MFiG	Art. 1 pkt 10 lit. c w zakresie art. 21a ust. 6a pkt 3	W dodawanym art. 6a pkt 3 proponujemy dodanie słowa „ważnego” do numeru dokumentu potwierdzającego tożsamość osób.	„3) imiona rodziców osób oraz serię i numer <b>ważnego</b> dokumentu potwierdzającego tożsamość osób, o których mowa w pkt 1 i 2,”	<b>Uwaga wyjaśniona</b> Należy podkreślić, że w celu dopasowania tożsamości może być podany numer dokumentu tożsamości, który już utracił ważność, choć był ważny w momencie, gdy seria i numer tego dokumenty były wpisywane do systemu teleinformatycznego. Na przykład w przypadku zagranicznego pacjenta, który korzystał z pomocy medycznej w polskim szpitalu i jego tożsamość została potwierdzona paszportem w roku 2022 (gdy paszport był ważny) i w roku 2027 będzie chciał uzyskać dostęp do swoich danych a paszport który okazał w roku 2022 będzie już nieważny. Tym samym proponuje się pozostawić przepis w dotychczasowym brzmieniu.
26	MFiG	Art. 1 pkt 10 lit. c oraz art. 1 pkt 13 w zakresie art. 21a ust. 6a oraz art. 22a-22k	Występuje niezgodność zakresu danych osobowych przetwarzanych w systemie scentralizowanym prowadzonym przez Ministra właściwego ds. informatyzacji określonych w art. 6a pkt 3 oraz art. 22a ust. 3 pkt 3 - w drugim przypadku wskazane jest dodatkowo przetwarzanie numeru PESEL osób fizycznych, o czym nie mam mowy w art. 6a pkt 3 wskazującym zakres przetwarzanych danych osobowych w systemie scentralizowanym.	Korekta projektu ustawy we wskazanym zakresie.	<b>Uwaga wyjaśniona</b> Nie występuje wskazana w uwadze niezgodność, ponieważ nr PESEL zawiera się w danych identyfikujących osobę, o których mowa w rozporządzeniach wykonawczych 1501/2015 i 2024/2977 w przypadku środków identyfikacji elektronicznej wydawanych w Polsce.

27	MFiG	OSR pkt 8	W OSR w pkt 8 w zdaniu: Należy podkreślić, że zgodnie z projektem ustawy, dodawany art. 10a, określa w ustawie z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, iż podmiotem zobowiązanym do prowadzenia w systemie teleinformatycznym, będącym rejestrem publicznym, Katalogu Podmiotów Publicznych, jest minister właściwy do spraw informatyzacji. Należy zauważyć, że nowa wersja projektu nie zawiera nowego/ dodawanego art. 10a.	Korekta OSR we wskazanym zakresie.	<b>Uwaga uwzględniona</b> Zostanie dokonana stosowna korekta w OSR.
28	MFiG	Uwaga ogólna	Brakuje przepisu stanowiącego, że czynność dokonana przy użyciu portfela tożsamości cyfrowej (UE) wywołuje skutki prawne przewidziane w ustawach materialnych. Może to prowadzić do sytuacji, w której np. na gruncie ustawy podatkowej portfel tożsamości cyfrowej nie będzie uznawany.	Dodać zapis, np.: 1. Identyfikacja elektroniczna osoby fizycznej lub prawnej dokonana przy użyciu portfela tożsamości cyfrowej, o którym mowa w niniejszej ustawie, wywołuje skutki prawne identyfikacji dokonanej przy użyciu środka identyfikacji elektronicznej o wysokim poziomie bezpieczeństwa. 2. Złożenie oświadczenia woli lub wiedzy przy użyciu portfela tożsamości cyfrowej, w tym przy użyciu kwalifikowanego podpisu elektronicznego albo kwalifikowanej pieczęci elektronicznej integrowanej z portfelem, wywołuje skutki prawne przewidziane w przepisach odrębnych, w szczególności w postępowaniach podatkowych, celnych i administracyjnych.	<b>Uwaga wyjaśniona</b> Nie zachodzi potrzeba dodania proponowanych przepisów, gdyż podniesione kwestie są już uregulowane przepisami rozporządzenia 910/2014, zaś art. 52 niniejszego rozporządzenia stanowi o jego bezpośrednim stosowaniu przez wszystkie państwa członkowskie.
29	MFiG	Uwaga ogólna	UC122 ma charakter ustawy ramowej i nie zawiera wdrożenia odpowiednich zmian, np. w Ordynacji podatkowej. W konsekwencji, mimo dostępności portfela, nie będzie on miał charakteru prawnie „obowiązkowego”.	Uzupełnić zapisy ustawy, np.: 1. Atrybut tożsamości lub poświadczenie elektroniczne wydane zgodnie z niniejszą ustawą zastępuje dokument urzędowy lub jego odpis, jeżeli przepisy odrębne wymagają przedłożenia dokumentu w celu potwierdzenia określonych danych lub statusu prawnego. 2. Organ administracji publicznej nie może odmówić	<b>Uwaga wyjaśniona</b> Nie zachodzi potrzeba dodatkowego uregulowania przedmiotowej kwestii z uwagi na treść przepisu art. 45b rozporządzenia 910/2014, który już normuje poruszone zagadnienia.

				przyjęcia atrybutu lub poświadczenia, o którym mowa w ust. 1, wyłącznie z powodu jego postaci elektronicznej.	
30	MFİG	Uwaga ogólna	W projekcie UC122 brak sprecyzowanego trybu offline, co może powodować ryzyko podważenia czynności kontrolnych realizowanych w ramach kontroli skarbowych.	<p>Uzupełnić zapisy ustawy np.:</p> <ol style="list-style-type: none"> <li>1. W przypadku braku dostępu do sieci telekomunikacyjnej dopuszcza się weryfikację atrybutów tożsamości w trybie offline, w zakresie określonym w przepisach wykonawczych.</li> <li>2. Weryfikacja offline, o której mowa w ust. 1, wywołuje skutki prawne w zakresie czynności kontrolnych i sprawdzających, w szczególności wykonywanych przez organy Krajowej Administracji Skarbowej.</li> <li>3. Minister właściwy do spraw informatyzacji określi, w porozumieniu z ministrem właściwym do spraw finansów publicznych, szczegółowy zakres i tryb weryfikacji offline.</li> </ol>	<p><b>Uwaga wyjaśniona</b></p> <p>Zgodnie z motywem 2 rozporządzenia 910/2014, celem przedmiotowego rozporządzenia jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi. W związku z tym, w przypadku wskazanym w uwadze, gdy strona ufająca nie może ustalić ważności europejskiego portfela tożsamości cyfrowej za pomocą technologii kryptograficznej, z uwagi na tryb offline, czynność weryfikacji europejskiego portfela tożsamości cyfrowej nie powinna być możliwa i nie powinna wywoływać określonych skutków prawnych. Europejski portfel tożsamości cyfrowej nie posiada zabezpieczeń fizycznych, jakie mają dokumenty tożsamości np. mikrotekst czy tłoczenia.</p> <p>Z uwagi na powyższe oraz art. 3 pkt 2 rozporządzenia 910/2014, zgodnie z którym poprzez środek identyfikacji elektronicznej należy rozumieć materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online lub, w stosownych przypadkach, dla usługi offline, należy przyjmować, że stosowanie w warunkach offline z europejskiego portfela tożsamości cyfrowej nie ma charakteru absolutnego - bezwzględnie obowiązującego. Dlatego też, w przypadku spełnienia się przesłanek negatywnych, weryfikacja tożsamości powinna nastąpić w oparciu o dokument tożsamości.</p>
31	MFİG	Uwaga ogólna	Brak zapewnienia interoperacyjności z prawem podatkowym.	<p>Dodać przepisy końcowe, np.:</p> <p>W ustawie z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa identyfikacja podatnika oraz składanie oświadczeń woli przy</p>	<p><b>Uwaga wyjaśniona</b></p> <p>Skutek prawny środków identyfikacji elektronicznej oraz usług zaufania, jak również brak możliwości zaprzeczania tego typu dowodom w postaci elektronicznej uregulowany</p>

				użyciu portfela tożsamości cyfrowej uznaje się za równoważne z identyfikacją oraz oświadczeniami dokonywanymi przy użyciu środków określonych w przepisach odrębnych.	jest przepisami rozporządzenia 910/2014. W związku z tym nie zachodzi na gruncie przepisów krajowych potrzeba powielania określonego skutku, w tym poszczególnych ustawach materialnych.
32	MFiG	Art. 1 (zakres przedmiotowy ustawy)	Rozszerzenie zakresu ustawy o funkcjonowanie portfela tożsamości cyfrowej oraz rejestru stron ufających nie zawiera odniesienia do zasad ochrony danych osobowych, w szczególności zasad minimalizacji i ograniczenia celu.	Proponuje się uzupełnienie przepisu o ustęp: „Realizacja zadań, o których mowa w pkt 8–14, odbywa się z uwzględnieniem zasad przetwarzania danych osobowych określonych w art. 5 rozporządzenia 2016/679, w szczególności zasady minimalizacji danych oraz ograniczenia celu.”	<b>Uwaga wyjaśniona</b> Nie jest koniecznym uzupełnienie przedmiotowego przepisu w zaproponowanym brzmieniu, z uwagi na to, że wszelkie zadania związane z przetwarzaniem danych osobowych w związku z funkcjonowaniem europejskiego portfela tożsamości cyfrowej oraz rejestr strony ufających, muszą być realizowane zgodnie z rozporządzeniem 2016/679, na co wskazuje m.in. przepis ogólny art. 2 ust. 4 rozporządzenia nr 910/2014 („ <i>niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679</i> ”), a także przepisy szczególne rozporządzenia 910/2014 - np. 5a ust. 17.
33	MFiG	Art. 1 (przepisy dot. dopasowania tożsamości (implementacja art. 11a eIDAS)	Projekt nie określa jednoznacznie zakresu danych wykorzystywanych w procesie dopasowania tożsamości ani zasad ich ograniczenia.	Proponuje się uzupełnienie: „Dopasowanie tożsamości odbywa się wyłącznie w zakresie danych niezbędnych do jednoznacznej identyfikacji osoby, przy zastosowaniu środków minimalizujących zakres przetwarzanych danych oraz z wyłączeniem tworzenia dodatkowych profili użytkowników.”	<b>Uwaga wyjaśniona</b> Przepis ogólny art. 2 ust. 4 rozporządzenia 910/2014 stanowi „niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679”. W związku z powyższym, realizacja ciężących na państwach członkowskich obowiązków wynikających z art. 11a odbywać się będzie z poszanowaniem przepisów rozporządzenia 2016/679. Zatem nie zachodzi konieczność dodania proponowanego przepisu do projektu ustawy.
34	MFiG	Art. 1 pkt 13 w zakresie art. 22i	Połączenie funkcji wydawania poświadczeń oraz nadzoru może prowadzić do konfliktu ról.	Proponuje się uzupełnienie: „Zapewnia się organizacyjną i funkcjonalną rozdzielność zadań związanych z wydawaniem poświadczeń oraz nadzorem nad dostawcami usług zaufania.”	<b>Uwaga wyjaśniona</b> Stosowne rozdzielanie zadań związanych z pełnieniem przez ministra właściwego do spraw informatyzacji roli dostawcy portfela, usług zaufania i pełnienia roli organu nadzoru zapewniają projektowane przepisy art. 23a (art. 1 pkt 15 projektu ustawy) i 22k (art. 1 pkt 13 projektu ustawy).

35	MFiG	Art. 7 pkt 4 w zakresie. art. 14a ust. 6 pkt 1	Okres 20 lat przechowywania danych może być nieproporcjonalny względem celu.	Proponuje się uzupełnienie: „Okres przechowywania danych podlega okresowej ocenie adekwatności, nie rzadziej niż co 5 lat, z możliwością jego skrócenia w przypadku ustania celu przetwarzania.”	<b>Uwaga wyjaśniona</b> Okres dwudziestu lat przechowywania tego typu informacji był już uregulowany w przepisie art. 13 ust. 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (tekst jedn. Dz. U. z 2013 r., poz. 262 ze zm.), celem zapewnienia dowodów w zakresie uznania dokumentów podpisanych elektronicznie. Przyjęcie przedmiotowego terminu w projektowanej ustawie stanowi wyraz kontynuacji sprawdzonego (stabilnego) rozwiązania legislacyjnego, a jednocześnie realizacji zasady pewności prawa. Jednocześnie przyjęcie tak długiego terminu spowodowane jest okresem przedawnienia uregulowanym w art. 442 <sup>1</sup> § 2 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2025 r. poz. 1071, z późn. zm.), wynoszącym dwadzieścia lat, licząc od dnia popełnienia przestępstwa (bez względu na to, kiedy poszkodowany dowiedział się o szkodzie i osobie obowiązanej do jej naprawienia).
36	MFiG	Art. 1 pkt 20 lit. b w zakresie art. 47 ust. 1a	Do art. 1 pkt 20 lit. b (zmieniającego art. 47 ustawy o usługach zaufania oraz identyfikacji elektronicznej): nie jest możliwe określanie wysokości kar pieniężnych w euro. Kary pieniężne, o których mowa w projektowanym art. 47 ust. 1a pkt 1 i 2, powinny być określone w decyzji w złotych – tak jak w obowiązującym art. 47 ust. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej. W przeciwnym razie nie będzie możliwe wystawienie tytułów wykonawczych na te należności. W tytułach wykonawczych należności pieniężne są wykazywane w złotych.	Korekta projektu ustawy we wskazanym zakresie.	<b>Uwaga uwzględniona</b> Przepisy projektu ustawy zostaną uzupełnione w tym zakresie.
37	MFiG	Art. 7 pkt 4 w zakresie art. 14e ust. 6	Do art. 7 pkt 4 (zmieniającego ustawę o aplikacji mObywatel) wprowadzającego rekompensatę za świadczenie nieodpłatnej usługi umożliwiającej użytkownikom aplikacji mObywatel oraz europejskiego portfela tożsamości cyfrowej nieodpłatne składanie kwalifikowanych podpisów elektronicznych (projektowany art. 14e ust. 6). Z zaproponowanych przepisów nie wynika, jaki podmiot, na podstawie jakiego dokumentu (wniosku dostawcy usług zaufania?) i na jakich zasadach będzie tę rekompensatę wypłacał. Nie wiadomo zatem, czy ewentualny wniosek dostawcy	Uzupełnienie projektu ustawy we wskazanym zakresie.	<b>Uwaga uwzględniona</b> Przepisy projektu ustawy zostaną uzupełnione w tym zakresie.

			usług zaufania będzie weryfikowany przed wypłatą i w jakim trybie, czy rekompensata może zostać nadpłacona i jaki byłby tryb odzyskiwania rekompensaty wypłaconej w nadmiernej wysokości. Czy w takiej sytuacji wydawana byłaby decyzja i w jakim trybie? Sam sposób wyliczania opłaty nie wydaje się wystarczający.		
38	MFiG	OSR	Przedmiotowy projekt ustawy zakłada uregulowanie kwestii dotyczących nakładania kar pieniężnych przez ministra właściwego do spraw informatyzacji na dostawców usług naruszających przepisy rozporządzenia 910/2014 (art. 46a i art. 47 zmienianej w art. 1 projektu ustawy o usługach zaufania oraz identyfikacji elektronicznej). W związku z powyższym w OSR konieczne jest wskazanie szacunkowej wysokości dochodów z przedmiotowych kar pieniężnych (tj. rząd wielkości), które powinny być ujęte w odpowiedniej poz. w tabeli. W dodatkowych informacjach należałoby odnieść się do przyjętych założeń dotyczących metodyki obliczenia tych dochodów w podziale na poszczególne lata.	Uzupełnienie OSR we wskazanym zakresie.	<b>Uwaga wyjaśniona</b> Zakłada się, że nie będzie zachodziła konieczność nakładania kar pieniężnych, gdyż ich obowiązywanie na gruncie projektowanej ustawy będzie realizować przypisywane im cele, tj. odstraszający oraz prewencyjny. Nie jest możliwe oszacowanie zgodnie z uwagą wysokości dochodów z przedmiotowych kar pieniężnych, gdyż zakłada się, iż adresaci projektowanych przepisów będą ich przestrzegać. Jeżeli zaś będą pojawiać się sytuacje, na skutek których koniecznym będzie nałożenie kary pieniężnej na jej adresata, to będzie to miało marginalny charakter z uwagi na ich znikome występowanie. W związku z tym nie zachodzi konieczność wskazania w OSR szacunkowej wysokości dochodów z przedmiotowych kar pieniężnych.
39	MFiG	OSR pkt 6	W pkt 6 OSR wskazano, iż kwoty wydatków wynikają ze wskazanych w projekcie ustawy limitów wydatków z budżetu państwa, o które będzie zwiększona część budżetowa ministra właściwego do spraw informatyzacji. Powyższe nie może zyskać akceptacji. Przyjęcie rozwiązań powodujących dodatkowe skutki dla budżetu państwa powinno zostać poprzedzone analizą obszarów, w których można dokonać oszczędności, tak aby możliwe było sfinansowanie wskazanych kosztów w ramach dotychczas ustalonych limitów wydatków dla części 27 – Informatyzacja. Należy zwrócić uwagę, że budżet państwa podlega stabilizującej regule wydatkowej (SRW) i jego wydatki objęte są limitem wydatków, o którym mowa w art. 112aa ust. 3 ustawy o finansach publicznych. Należy również wyraźnie podkreślić, że każde zwiększenie wydatków w stosunku do przepisów obecnie obowiązujących zmniejsza przestrzeń wydatkową na realizację kontynuowanych zadań budżetowych. Zgodnie z procedurami przyjętymi	Korekta OSR we wskazanym zakresie.	<b>Uwaga wyjaśniona</b> Kwota wydatków wynikająca ze wskazanych w projekcie ustawy limitów wydatków z budżetu państwa, o które będzie zwiększona część budżetowa ministra właściwego do spraw informatyzacji, spowodowana jest realizacją zadań wynikających z implementacji przepisów unijnych.

			przez Polskę w związku z obostrzeniami wynikającymi z prawa krajowego i unijnego, co do możliwego poziomu wydatków budżetu państwa oraz średniookresowego planu budżetowo strukturalnego na lata 2025-2028, Polska zobowiązała się w ramach przyjętej ścieżki wydatków do ograniczenia deficytu nominalnego do poniżej 3% PKB w 2028 roku. W związku z powyższym OSR należy uzupełnić o informację jednoznacznie wskazującą, iż skutki finansowe wynikające z wejścia w życie przedmiotowej ustawy dla części 27 – Informatyzacja zostaną sfinansowane w ramach limitów wydatków i nie będą stanowić podstawy do ubiegania się o dodatkowe środki z budżetu państwa na ten cel w roku wejścia w życie ustawy oraz w latach kolejnych.		
40	MFiG	OSR	Należy wskazać, że w art. 11 przedmiotowego projektu ustawy określono maksymalny limit wydatków z budżetu państwa będących skutkiem wejścia w życie niniejszej ustawy, a jako organ właściwy do wykorzystania maksymalnego limitu wydatków wskazano ministra właściwego do spraw informatyzacji. Kwoty zapisane w przedmiotowym artykule są tożsame z kwotami wydatków ogółem ujętymi w pkt 6 OSR, na które składają się zarówno wydatki budżetu państwa (cz. 27 – Informatyzacja) jak i wydatki pozostałych jednostek (Polskie Centrum Akredytacji). Powyższe nie jest jasne, w szczególności mając na uwadze informację z OSR, zgodnie z którą PCA nie otrzymuje środków z budżetu państwa i prowadzi samodzielną gospodarkę finansową.	Korekta OSR we wskazanym zakresie.	<b>Uwaga uwzględniona</b> OSR zostanie zmieniona.
41	MFiG	Art. 11, OSR	Budżet państwa objęty jest stabilizującą regułą wydatkową (SRW) oraz limitem wydatków, o których mowa w art. 112aa ust. 3 ustawy o finansach publicznych. W związku z tym planowane wydatki na realizację zadań Polskiego Centrum Akredytacji wynikające z wejścia w życie ww. ustawy powinny zostać pokryte w ramach dostępnych środków w planie finansowym jednostki, bez konieczności zwiększania łącznych wydatków. Mając powyższe na uwadze, należy wykreślić z art. 11 projektu ustawy maksymalny limit wydatków będących skutkiem wejścia w życie ustawy dla Polskiego Centrum Akredytacji, a także usunąć z tabeli w pkt 6 OSR skutki finansowe przewidziane dla tej jednostki.	Korekta projektu ustawy i OSR we wskazanym zakresie.	<b>Uwaga uwzględniona</b> OSR zostanie zmieniona. Przepis art. 11 projektu ustawy zostanie zmieniony we wskazanym zakresie.

42	MFİG	Art. 11 ust. 2	„W przypadku przekroczenia lub zagrożenia przekroczeniem przyjętego na dany rok budżetowy maksymalnego limitu wydatków określonego w ust. 1, stosuje się mechanizm korygujący polegający na ograniczeniu kosztów związanych z realizacją zadań wynikających z ustawy.” Powstaje wątpliwość, w jaki sposób ma być stosowany wskazany w tym przepisie mechanizm korygujący. W obecnym brzmieniu przepis ma charakter blankietowy i pozostaje na dużym stopniu ogólności. Przepis nie wskazuje zasad stosowania mechanizmu korygującego, co może utrudniać jego praktyczne zastosowanie. Nie jest jasne bowiem, jakie dokładnie koszty ujęto w projektowanym art. 11 i OSR (czy tylko na budowę RCT). Wymaga to wyjaśnienia i doprecyzowania. Podkreślenia wymaga, że co do zasady mechanizm korygujący konstruowany przez projektodawcę ustawy winien polegać na obniżeniu kosztów realizacji wyznaczonych zadań, tj. powinien w sposób dokładny i konkretny określać zakres wprowadzanego ograniczenia, tak aby mógł on doprowadzić do redukcji kosztów do maksymalnego limitu wydatków przyjętego na dany rok budżetowy, w przypadku zagrożenia przekroczenia tego limitu.	Należy skonkretyzować, o koszty których zadań chodzi (czy tylko budowę RCT) i koszty których zadań miałyby być ograniczane przy zastosowaniu mechanizmu korygującego opisanego w art. 11 ust. 2.	<b>Uwaga wyjaśniona</b> Na skutek uwzględnienia uwag, nie zachodzi potrzeba skonkretyzowania kosztów, w tym kosztów tych zadań, które miałyby być ograniczone przy zastosowaniu mechanizmu korygującego - opisanego w art. 11 ust. 2 projektu ustawy, gdyż z projektowanych przepisów wynika, iż dotyczą one wyłącznie budowy RCT.
43	MFİG	OSR pkt 6	W Tabeli, w wierszu odnoszącym się do wydatków pozostałych jednostek, nie ujęto o jaką jednostkę chodzi.	Należy wskazać o jaką jednostkę tutaj chodzi.	<b>Uwaga uwzględniona</b> W tabeli OSR w części pt. “Wpływ na sektor finansów publicznych” zostaną wprowadzone stosowne zmiany.
44	MFİG	OSR pkt 6	W tabeli w poz. „Źródła finansowania” zawarto stwierdzenie, że „Na kwotę wydatków w poszczególnych latach składają się następujące czynniki: - liczba zespołów x miesięczny koszt zespołu x liczba miesięcy; - koszt darmowych kwalifikowanych podpisów elektronicznych; - uwzględniająca 3% inflację rocznie; - uwzględniająca 20% pozostałych kosztów; - uwzględniająca 10% kwotę ryzyka.”.	Należy rozbudować ww. wyjaśnienia – czym są „zespoły”.	<b>Uwaga wyjaśniona</b> OSR zostanie stosownie uzupełniona w związku z przedmiotową uwagą. Przez wyrażenie “zespoły” należy rozumieć zespoły realizujące nałożone na nie zadania związane z budową, rozwojem i utrzymaniem odpowiednich systemów teleinformatycznych zapewniających funkcjonowanie europejskiego portfela tożsamości cyfrowej i jego niezbędnego otoczenia.
45	MFİG	OSR pkt 6	W poz. „Dodatkowe informacje” – tabela dot. wydatków budżetu państwa na RCT, wymaga szczegółowych informacji w opisie.	Pod tabelą należałoby bardziej szczegółowo opisać jakie składniki kosztów składają się na ujęte w tej tabeli kwoty, w podziale na: Utrzymanie, Budowa i Rozwój RCT.	<b>Uwaga wyjaśniona</b> Na tym etapie nie jest możliwe szczegółowe określenie składników kosztów w podziale na: utrzymanie, budowa i rozwój RCT, gdyż nie da się przewidzieć i wyliczyć kosztów poszczególnych zadań.



46	PUODO	OSR pkt 4	Prowadzenie postępowań w sprawie naruszenia przepisów dotyczących przetwarzania danych nie jest uregulowane w art. 2 i 3 rozporządzenia 2016/679. Art. 33 rozporządzenia 2016/679 określa zasady zgłaszania naruszenia ochrony danych osobowych organowi nadzorcemu, zaś postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych jest uregulowane w rozdziale 7 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.		<b>Uwaga uwzględniona</b> OSR zostanie zmieniona we wskazanym zakresie.
47	PUODO	Uwaga ogólna	Sposób ukształtowania uprawnienia ministra właściwego do spraw informatyzacji, w zakresie dodawania nowych usług w aplikacji mObywatel – art. 15 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2024 r. poz. 1275, z późn. zm.), tj. na podstawie uznaniowej decyzji administracyjnej, która nie ma później odzwierciedlenia w prawie powszechnie obowiązującym, nie wyklucza możliwości dodania takiej usługi w przyszłości, nawet pomimo niewskazania tego faktu w uzasadnieniu do projektu ustawy. Jest to problem systemowy, sygnalizowany już przez organ nadzorczy przy procedowaniu ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. Dlatego wprowadzenie nowych usług w aplikacji mObywatel, dotyczących kompetencji organu nadzorczego, musi odbywać się w ścisłym porozumieniu z organem nadzorczym. Prezes UODO jest organem nadzorczym w rozumieniu rozporządzenia 2016/679. Jest niezależny w ramach wykonywania przez siebie zadań, zaś gwarancje jego niezależności wynikają bezpośrednio z rozporządzenia 2016/679, nie wchodzi on również w skład administracji rządowej. Nakładanie na Prezesa UODO nowych zadań, o ile jest to zgodne z rozporządzaniem 2016/679 i innymi aktami prawa UE, musi się również zawsze wiązać z zapewnieniem organowi nadzorcemu adekwatnych środków i finansowania dla prawidłowego wykonywania jego uprawnień.		<b>Uwaga wyjaśniona</b> Art. 15 dotyczy tzw. usług standardowych, które są opracowane/udostępniane przez ministra właściwego do spraw informatyzacji, ale świadczone przez wiele podmiotów. Projektowane przepisy nie nakładają na Prezesa UODO nowych zadań.
48	PUODO	Uwaga ogólna	Pomimo deklaracji projektodawcy odnośnie przeprowadzenia testu prywatności i oceny skutków dla ochrony danych w rozumieniu art. 25 ust. 1 i art. 35 rozporządzenia 2016/679 (w szczególności ust. 1 i ust. 10), projektowana ustawa nie uległa zasadniczym zmianom, które mogłyby wskazywać, że analiza w tym zakresie miała pogłębiony i systemowy charakter.		<b>Uwaga wyjaśniona</b> Dokonano oceny skutków dla ochrony danych. Należy nadmienić, że procedowana ustawa co do zasady realizuje przepisy europejskie ustanawiające wspólne ramy tożsamości cyfrowej w całej Unii Europejskiej, które już zostały przeanalizowane i zaopiniowane przez Europejskiego Inspektora Ochrony Danych.

					Opinie Europejskiego Inspektora Ochrony Danych dotyczące projektu rozporządzenia zmieniającego rozporządzenia 910/2014, wprowadzającego europejskie portfele tożsamości, elektroniczne poświadczenia atrybutów, rejestry stron ufających, obowiązek dopasowywania tożsamości i inne zmiany w zakresie ram tożsamości cyfrowej, oraz projektów aktów wykonawczych związanych, z tą nowelizacją są dostępne pod adresem <a href="https://www.edps.europa.eu/search_en?search=910">https://www.edps.europa.eu/search_en?search=910</a>
49	PUODO	Art. 1 pkt 10w zakresie art. 21a	Organ nadzorczy podtrzymuje uwagę do art. 1 pkt 10 projektu ustawy w zakresie zmian w art. 21a ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. z 2024 r. poz. 1725 oraz z 2026 r. poz. 252). Niepodjęcie przez projektodawcę próby stworzenia katalogu danych przetwarzanych w systemie scentralizowanym, o jak najbardziej zamkniętym charakterze, oprócz kwestii związanych z zasadą legalności i przejrzystością przetwarzania, które były wskazywane we wcześniejszych uwagach organu nadzorczego, może doprowadzić do przetwarzania całego szeregu danych nadmiarowych przez ministra właściwego do spraw informatyzacji. Jak wskazano w wyjaśnieniach projektodawcy: „Nawet jeżeli system scentralizowany nie będzie potrzebował w zakresie danych identyfikujących osobę oznaczenia płci określonego zgodnie z szerokimi możliwościami określonymi w rozporządzeniu 2024/2977 albo numeru telefonu komórkowego, ale użytkownik portfela zagranicznego mimo to będzie usiłował przekazać takie dane w zestawie danych identyfikujących osobę, to nawet odrzucenie takich danych będzie oznaczało ich przetwarzanie.”. Czym innym jest czynność przetwarzania w postaci odrzucenia danych, a czym innym przetwarzanie niedookreślonego katalogu danych przez organ publiczny w rejestrze publicznym o takim znaczeniu jak system scentralizowany. To właśnie brak zamkniętego katalogu danych powoduje, że obywatele nie będą mieli odpowiednich gwarancji, dotyczących tego jak ich dane będą przetwarzane docelowo w rejestrze publicznym, które zaś zostaną uznane za zbędne i tym samym odrzucone. Stworzy to w		<p><b>Uwaga wyjaśniona</b></p> <p>Zakres przetwarzanych danych z systemie scentralizowanym i sposób postępowania z nimi jest ściśle określony w projektowanym oraz art. 22a.</p> <p>System scentralizowany będzie stosowany wyłącznie w przypadku transgranicznego uwierzytelniania, zatem przetwarzania imion rodziców nie będzie dotyczyło wszystkich polskich obywateli, tylko osób którym nadano numer PESEL posługujących się notyfikowanym środkiem identyfikacji elektronicznej lub europejskim portfel tożsamości cyfrowej wydanym w innym kraju. Będzie to miało zatem miejsce sporadycznie, będzie dotyczyło osób fizycznych, których tożsamość została już bez wątpliwości zidentyfikowana, ale zgodnie z przepisami art. 11a rozporządzenia eIDAS musi być dopasowana do danych tej osoby zapisanych w systemie/ rejestrze innego państwa członkowskiego. Ponadto użytkownik środka identyfikacji elektronicznej nie będzie musiał podawać takich dodatkowych danych, ale wtedy dopasowanie nie będzie możliwe. Jakikolwiek przekazywanie danych z systemu scentralizowanego do strony ufającej będzie następowało wyłącznie za zgodą użytkownika. Ponadto należy mieć na uwadze, że dopasowywanie tożsamości będzie musiało być również zgodne przepisami rozporządzenia wykonawczego Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i</p>

			<p>przyszłości szereg problemów dla administratora danych – ministra właściwego do spraw informatyzacji. Dotyczyć to będzie w szczególności realizacji praw osób, których dane dotyczą, na podstawie rozporządzenia 2016/679.</p> <p>W zakresie uwagi organu nadzorczego dotyczącej celowości przetwarzania imion rodziców w ramach systemu scentralizowanego projektodawca wyjaśnia: „Odnosząc się do uwagi dotyczącej adekwatności i celowości przetwarzania imion rodziców należy wyjaśnić, że jest to wyłącznie dodatkowa identyfikacja celem dopasowania do danych w rejestrze PESEL i dotyczy danych osoby, której tożsamość już została zidentyfikowana, ale nie ma pewności, czy jest to ta sama osoba, której dane zostały wpisane do ewidencji ludności. Rezygnacja z tej opcji może utrudnić lub nawet uniemożliwić licznym przedstawicielom Polonii skorzystanie z usług online w Polsce, którzy zapomnieli przez lata spędzone poza ojczyzną, jaki mieli nadany nr PESEL.”, i dalej: „Podanie imienia rodzica nie służy zatem identyfikacji osoby fizycznej, gdyż ta została już dokonana, ale wyłącznie do dopasowania do danych w ewidencji ludności, w której imiona rodziców to dane obowiązkowo przechowywane.”. W ocenie organu nadzorczego nie jest to argument wystarczający do rozszerzenia katalogu danych osobowych poza zakres wymagany w rozporządzeniu 2024/2977. Rozszerzenie katalogu danych będzie przecież dotyczyło wszystkich polskich obywateli. Jeżeli problem korzystania przez przedstawicieli Polonii, którzy zapomnieli swojego numeru PESEL, z usług online jest na tyle szeroki i ma charakter systemowy, to rozwiązanie go powinno mieć miejsce w odrębnym dedykowanym akcie prawnym.</p>		<p>Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. U. UE. L. z 2025 r. poz. 846).</p> <p>Aby dopasować dane, jakie mogą być przekazane w ramach zestawów danych identyfikujących osobę, o których mowa w rozporządzeniach Komisji 2024/2977 oraz 1501/2015 do danych rejestrze PESEL niezbędne jest podanie dodatkowych danych, jakie w tym rejestrze się znajdują. Należy pamiętać, że celem tych przepisów jest zapewnienie użytkownikom dopasowania tożsamości, co wymaga przetwarzania dodatkowych danych osobowych, ponieważ nie jest bez tego logicznie możliwe dopasowanie do siebie zbiorów danych przesyłanych za pomocą zagranicznych środków identyfikacji elektronicznej z danymi w rejestrze PESEL. Rezygnacja z możliwości podania imienia rodzica celem jednoznacznego wstępnie dopasowanej tożsamości byłaby znaczącym utrudnieniem dla użytkowników usług. Należy przypomnieć że już na wstępnym etapie prac nad zmianą rozporządzenia 910/2014 zrezygnowano z możliwości uzyskiwania przez użytkowników, którzy tego by sobie życzyli europejskiego identyfikatora osoby fizycznych, który by jednoznacznie identyfikował ich w usługach transgranicznych w dowolnym kraju UE. Konsekwencją tego jest konieczność dopasowywania tożsamości wymagająca każdorazowo przetwarzania większego zakresu danych.</p>
50	PUODO	Art. 1 pkt 13 w zakresie art. 22a ust 4 pkt 1 i 2	<p>Organ nadzorczy podtrzymuje uwagę zgłoszoną do art. 1 pkt 13 projektu ustawy w zakresie art. 22a ust. 4 pkt 1 i 2 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Uwaga organu nadzorczego dotycząca oparcia systemu scentralizowanego na numerze PESEL, wiąże się bezpośrednio z problemem nieprzyjęcia przez projektodawcę rozwiązania w postaci wprowadzenia unikalnego numeru identyfikacyjnego powiązanego z europejskim portfelem tożsamości cyfrowej. Kwestia ta jest rozwinięta szerzej w dalszej części niniejszego pisma.</p>		<p><b>Uwaga wyjaśniona</b></p> <p>Ponownie należy wyjaśnić, że nie można w tym przypadku zrezygnować z przetwarzania numeru PESEL, gdyż to ten numer jest unikatowym wyróżnikiem w ewidencji ludności i ten numer jest wymagany elementem wszystkich usług online świadczonych w systemach teleinformatycznych przyłączonych do węzła krajowego identyfikacji elektronicznej. Nie można się opierać o unikatowy numer identyfikacyjny powiązany z europejskim portfelem tożsamości cyfrowej, ponieważ:</p>

					<p>1) przekazywanie takiego numeru do dostawcy usługi online byłoby całkowicie nieużyteczne;</p> <p>2) numer ten nie jest elementem obowiązkowym wymienionym w rozporządzeniu 2024/2977;</p> <p>3) dopasowywanie tożsamości jest wymagane nie tylko dla europejskich portfeli tożsamości cyfrowej, ale również dla notyfikowanych środków identyfikacji elektronicznej.</p>
51	PUODO	Art. 1 pkt 13 w zakresie art. 22b ust. 1 pkt 5 i 6	Organ nadzorczy podtrzymuje uwagę zgłoszoną do art. 1 pkt 13 projektu ustawy w zakresie art. 22b ust. 1 pkt 5 i 6 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Zarówno zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych jak i zasady zgłaszania naruszenia ochrony danych osobowych, powinny być określone na poziomie aktów prawa powszechnie obowiązującego. Jak wskazano na wstępie niniejszego pisma, problem ten był już wcześniej sygnalizowany i jak pokazuje proces legislacyjny projektowanej ustawy, może on przełożyć się na realne rozwiązania faktyczne, takie jak planowane wcześniej wdrożenie usługi „zgłaszania naruszeń organowi nadzorcemu”. Model ten nie dość że jest nieprzejrzysty to powoduje jeszcze, że na blankietowe i zdecydowanie niewyczerpujące przepisy ustawy nakładane są uprawnienia do kształtowania celów i sposobów przetwarzania w drodze uznaniowej i opartej na uznaniu decyzji ministra właściwego do spraw informatyzacji.		<p><b>Uwaga wyjaśniona</b> Określona funkcjonalność portfela wynika wprost z art. 5a ust. 4 lit d tiret III rozporządzenia 910/2014 i musi zostać zrealizowana.</p> <p>Celowo nie proponuje się ustalenia na poziomie ustawy w jaki sposób realizowane będzie opisane w tym przepisie „łatwe zgłaszanie strony ufającej właściwemu krajowemu organowi ochrony danych, w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych” (p.. czy portfel będzie wysyłał zgłoszenie na adres do doręczeń elektronicznych UODO AE:PL-67085-31860-RWFHC-35, jak obecnie sugeruje to PUODO na swojej stronie internetowej, lub w inny sposób) dlatego, że jest to zupełnie nowy przepis nie ma jeszcze żadnych odniesień do dobrej praktyki w tym zakresie.</p> <p>Mając na uwadze, że taka dobra praktyka powinna zostać wypracowana wspólnie z PUODO i odpowiednio modyfikowana w zależności od nabierania doświadczeń w tym zakresie wydaje się, że przesądzanie w ustawie o tej praktyce jest niezasadne.</p>
52	PUODO	Art. 1 pkt 13 w zakresie art. 22c	Organ nadzorczy podtrzymuje uwagę zgłoszoną do art. 1 pkt 13 projektu ustawy w zakresie art. 22c ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. Jak wyjaśnia projektodawca „Podmioty publiczne celowo nie są wymieniane wprost w projektowanych przepisach, z uwagi na to, że stale postępująca informatyzacja zadań publicznych powoduje tworzenie kolejnych publicznych źródeł autentycznych, które wcześniej nie istniały. Zakłada się,		<p><b>Uwaga wyjaśniona</b> Projektodawca podtrzymuje dotychczasowe wyjaśnienia w tej sprawie.</p> <p>Wprowadzanie wszelkich źródeł autentycznych do ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji jest niecelowe i prowadziło do niepotrzebnego dublowania przepisów. Rozporządzenie 910/2014 i rozporządzenie wykonawcze 2025/1569</p>

			<p>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.”. Organ nadzorczy zwraca uwagę, że chociażby pkt 4 OSR projektu ustawy „Podmioty, na które oddziałuje projekt”, wymienia organy administracji publicznej odpowiedzialne za źródła autentyczne. W ocenie organu nadzorczego źródła autentyczne zapewniane przez podmioty publiczne muszą być oparte na rejestrach publicznych rozumieniu art. 3 pkt 5 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703, z późn. zm.). Utworzenie rejestru publicznego zawsze wiąże się z koniecznością wprowadzenia zmian ustawowych. Dlatego nie ma formalnych ani faktycznych przeszkód aby w tym zakresie za każdym razem wprowadzić odpowiednie zmiany w przepisach ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej w zakresie źródeł autentycznych. Tym samym organ nadzorczy podtrzymuje swoją uwagę, również w zakresie konieczności wprowadzenia w projekcie ustawy odpowiednich zmian sektorowych.</p>		<p>określają w jaki sposób źródła autentyczne mają być zgłaszane i katalogowane aby stanowiły podstawę do wydawanie elektronicznych poświadczeń atrybutów. Podobne rozwiązanie (krajowy katalog schematów poświadczania atrybutów) zaproponowano na poziomie krajowym uwzględniając uwagi zgłoszone podczas uzgodnień, opiniowania i konsultacji publicznych projektu ustawy.</p>
53	PUODO	Art. 4 pkt 3 projektu ustawy – w zakresie art. 22ac	<p>Organ nadzorczy podtrzymuje uwagę zgłoszoną do art. 4 pkt 3 projektu ustawy w zakresie art. 22ac ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703 oraz z 2026 r. poz. 160). Jak wyjaśnia projektodawca „Zgodnie z minimalnymi wymaganiami dla systemów teleinformatycznych, szerzej opisanymi w dalszej części niniejszego stanowiska, podmioty publiczne mają obowiązek stosowania numeru PESEL jako identyfikatora osoby fizycznej w prowadzonych przez siebie rejestrach publicznych. W kontekście powyższego należy wskazać, że numer PESEL jest najbardziej powszechnym i skutecznym identyfikatorem, który poza unikalną identyfikacją osoby fizycznej pozwala także na powiązanie identyfikowanej osoby z szeregiem dotyczących jej dokumentów oraz opisujących tę osobę danych, które przetwarzane są w rejestrach publicznych.”. Abstrahując od powyższych wyjaśnień, organ nadzorczy wskazuje, że w żaden sposób nie uzasadnia to przetwarzania</p>		<p><b>Uwaga wyjaśniona</b> Nr PESEL w przypadkach wskazanych w uwadze będzie przetwarzany wyłącznie celu powiązania środków identyfikacji elektronicznej osób fizycznych ze środkami osoby prawnej i nie będzie przekazywany do strony ufającej. Takie powiązanie zapewniając kontrolę upoważnionej osoby fizycznej nad środkiem osoby prawnej i kontrolę osoby prawnej nad tym powiązaniem zapewni jednocześnie bezpieczeństwo obu tych interesariuszy oraz możliwość efektywnego zarządzania środkiem przez osobę prawną.</p>

			numeru PESEL osoby reprezentującej podmiot publiczny oraz osoby pełniące funkcję administratora profilu zaufanego, gdyż osoby te w ramach danego podmiotu publicznego w sposób jednoznaczny identyfikowane są poprzez imię, nazwisko, pełnioną funkcję oraz nazwę reprezentowanego podmiotu. Tym samym uwaga organu nadzorczego pozostaje aktualna.		
54	PUODO	Art. 7 pkt 4 w zakresie art. 14a ust. 2	<p>Organ nadzorczy podtrzymuje uwagę zgłoszoną do art. 7 pkt 4 projektu ustawy w zakresie art. 14a ust. 2 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel. Jak wyjaśnia projektodawca: „Nadmienić należy, że inicjatywa zastąpienia numeru PESEL innym numerem administracyjnym w identyfikacji elektronicznej w usługach online 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.”</p> <p>Istnieje potrzeba pogłębionej dyskusji w zakresie ewentualnego zastąpienia numeru PESEL innym numerem administracyjnym w ramach identyfikacji elektronicznej. Kwestia ta dotyczy jednak nie tylko tej sfery, ale całego mechanizmu funkcjonowania systemu rejestrów państwowych, w których numer PESEL jest numerem referencyjnym. Organ nadzorczy uważa jednak, że wprowadzenie numeru przypisanego użytkownikowi portfela (niepowiązanego z jego cechami charakterystycznymi jak wiek czy płeć jak ma to miejsce w przypadku numeru PESEL) na poziomie funkcjonującego w ramach aplikacji mObywatel europejskiego portfela tożsamości cyfrowej, nie musi się wiązać automatycznie ze zmianami w narzędziach takich jak podpis zaufany czy podpis osobisty. Należy ponownie wskazać, że kwalifikowane podpisy elektroniczne nie muszą zawierać numeru PESEL w certyfikacie. Dlatego też odstępienie od obligatoryjnego użycia numeru PESEL w kwalifikowanym podpisie elektronicznym, który zostanie udostępniony w ramach aplikacji mObywatel, nie zmienia ogólnych zasad funkcjonowania środków identyfikacji elektronicznej. Rozwiązanie to nie będzie możliwe bez wprowadzenia numeru przypisanego użytkownikowi portfela tj. personal administrative number, w rozumieniu tabeli 2</p>		<p><b>Uwaga wyjaśniona</b> Obecnie nie jest możliwa rezygnacja z nr PESEL w krajowych środkach identyfikacji elektronicznej.</p>

			rozporządzenia 2024/2977. Dlatego też organ nadzorczy podtrzymuje uwagę, jednocześnie dziękując za zauważanie przez projektodawcę konieczności przeprowadzenia pogłębionej dyskusji w zakresie użycia numer PESEL w funkcjonującym w Polsce systemie identyfikacji elektronicznej.		
55	PUODO	Art. 7 pkt 4 w zakresie art. 14b ust. 3	Organ nadzorczy dziękuje za wyjaśnienia do uwagi zgłoszonej do art. 7 pkt 4 projektu ustawy w zakresie art. 14b ust. 3 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel – w zakresie wymogów dotyczących dodatkowej weryfikacji tożsamości na podstawie rozporządzenia 2026/798. Tym niemniej, stosowanie przez administratorów metod takich jak weryfikacja biometryczna, w ramach zdalnej weryfikacji tożsamości, będzie niosło za sobą wysokie ryzyko naruszenia praw i wolności osób fizycznych. Konieczne będzie więc przeprowadzenie przez ministra właściwego do spraw informatyzacji szerokiej akcji informacyjnej w tym zakresie.		<b>Uwaga wyjaśniona</b> Ministerstwo Cyfryzacji prowadzi na bieżąco działania o charakterze infomacyjnym.
56	PUODO	Art. 7 pkt 4 w zakresie art. 14h	Projektowany przepis w wersji ustawowej skierowanej do opiniowania brzmiał w następujący sposób: „Rada Ministrów określi, w drodze rozporządzenia, zakres danych i wykaz rejestrów publicznych oraz systemów teleinformatycznych, z których użytkownik europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, może pobrać dane, oraz podmiotów publicznych prowadzących te rejestry publiczne i systemy teleinformatyczne, mając na uwadze adekwatność zakresu tych danych do potrzeb związanych z usługami świadczonymi w ramach europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 5a ust. 2 lit. a rozporządzenia 910/2014, oraz uwarunkowania pozwalające na zapewnienie możliwości pobierania tych danych.”. W wersji skierowanej na posiedzenie Komitetu do spraw Cyfryzacji brzmi on zaś następująco: „Dostęp do aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 14a ust. 1, w pełnym albo ograniczonym zakresie funkcjonalności, może być zapewniany przez ministra właściwego do spraw informatyzacji w ramach jednego rozwiązania techniczno-organizacyjnego po uwierzytelnieniu osoby fizycznej, w sposób, o którym mowa w art. 14b ust. 1, lub osoby prawnej w sposób, o którym mowa w art. 14c ust. 1.”.		<b>Uwaga wyjaśniona</b> Zakres danych identyfikujących osobę jest określony i wynika z rozporządzenia 2024/2977. Natomiast katalog danych w elektronicznych poświadczeniach atrybutów nie może być określony, ponieważ użytkownicy mogą uzyskiwać dowolne elektroniczne poświadczenie atrybutów zdefiniowane w katalogu schematów poświadczania atrybutów, o którym mowa w rozporządzeniu 2025/1569. Odpowiednio i na wzór tego katalogu będzie funkcjonował krajowy katalog schematów poświadczania atrybutów. Wymienienie w jednym akcie prawnych wszelkich danych, jakie mogą się znaleźć w elektronicznych poświadczeniach atrybutów nie jest możliwe, gdyż dotyczyć one mogą tak wielu dziedzin życia, że wymagałoby to nieustannych zmian przepisów. Elektroniczne poświadczenia atrybutów mają bowiem co do zasady zastąpić istniejące w obiegu wszelkie poświadczenia w postaci papierowej, co wynika z przepisów rozporządzenia 910/2014. Skoro nie ma w jednej ustawie przepisów dotyczących zakresu danych przetwarzanych we wszelkich poświadczeniach

			<p>Weześniejsze uwagi organu nadzorczego do art. 14h odnosiły się do problemu regulowania aktem wykonawczym materii, która powinna znaleźć się w ustawie. Zarówno zakres danych, jak i wykaz rejestrów powiązanych z europejskim portfelem tożsamości cyfrowej, zapewnianym przez ministra właściwego do spraw informatyzacji nie powinny być ustalane rozporządzeniem.</p> <p>W obecnej wersji projektowanej ustawy, odstąpiono w ogóle od regulowania tej materii w akcie prawa powszechnie obowiązującego. Tym samym w miejsce niedoskonałego – blankietowego rozwiązania, projektodawca celowo decyduje się na wprowadzenie luki prawnej.</p> <p>kontekście systemowym wyłania się więc obraz projektowanej ustawy jako regulacji o dużym stopniu elastyczności, która jednak w wyniku tego nabiera charakteru blankietowego, w stopniu który głęboko godzi zarówno w zasady określone w rozporządzeniu 2016/679 jak i zasady konstytucyjne. Projektodawca decyduje się na stworzenie otwartych katalogów danych dotyczących użytkowników europejskiego portfela tożsamości cyfrowej, nie określa podmiotów odpowiedzialnych za źródła autentyczne oraz nie decyduje się na wprowadzenie od dawna postulowanych zmian systemowych w zakresie użycia numeru PESEL w systemach identyfikacji elektronicznej. Całościowo daje to ministrowi właściwemu do spraw informatyzacji instrument prawny do szybkiego wdrożenia europejskiego portfela tożsamości cyfrowej, powoduje jednak, że wszystkie ryzyka, na które wskazuje organ nadzorczy będą się na siebie nakładać i w konsekwencji mogą prowadzić do naruszenia gwarantowanych konstytucyjnie – prawa do prywatności (art. 47 Konstytucji RP) i prawa do autonomii informacyjnej (art. 51 Konstytucji RP). Demokratyczne państwo prawne nie może wykraczać poza poziom niezbędny, w zakresie gromadzenia i udostępniania informacji o obywatelach. Granice zaś tej niezbędności musi wyznaczać spójny i kompleksowy akt prawny rangi ustawowej.</p> <p>Dlatego też konieczne jest wprowadzenie zmian w projektowanej ustawie, tak aby odpowiadała konstytucyjnej zasadzie legalizmu. Przetwarzanie danych osobowych przez podmioty publiczne musi</p>		<p>w postaci papierowej analogicznie nie jest zasadne wprowadzanie takich przepisów dla poświadczeń elektronicznych.</p>
--	--	--	--	--	--



			<p>odbywać się na podstawie i w granicach przepisów prawa (art. 7 Konstytucji RP). Rolą projektodawcy jest natomiast precyzyjne wskazanie wykonawcom norm, jakie dane mają być przetwarzane, w jakim celu, w jaki sposób, przez jaki okres czasu oraz kto będzie za to przetwarzanie odpowiadał (art. 5 ust. 1 lit. a, b, c, e w zw. z art. 5 ust. 2 w zw. z art. 6 ust. 3 rozporządzenia 2016/679).</p>		
--	--	--	--	--	--