TYTUŁ PROJEKTU	**Ustawa o zmianie ustawy o usługach zaufania oraz identyfikacji elektronicznej oraz niektórych innych ustaw (UC122)**
TYTUŁ WDRAŻANEGO AKTU PRAWNEGO / WDRAŻANYCH AKTÓW PRAWNYCH	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz. Urz. UE. L. 257 z 28.08.2014, str. 73, z późn. zm.) zmienione 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. Urz. UE. L 2024/1183 z 30.04.2024), zwane dalej „rozporządzeniem eIDAS”. Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. Urz. UE L 2024/2977 z 4.12.2024), zwane dalej „rozporządzeniem 2024/2977”. Rozporządzenie wykonawcze komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. Urz. UE L 2024/2979 z 4.12.2024), zwane dalej „rozporządzeniem 2024/2979”. Rozporządzenie wykonawcze Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. Urz. UE L 2025/846 z 7.05.2025), zwane dalej „rozporządzeniem 2025/846”. Rozporządzenie wykonawcze Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających europejskiego portfela tożsamości cyfrowej (Dz. Urz. UE L 2025/848 z 7.05.2025), zwane dalej „rozporządzeniem 2025/848”.

	Rozporządzenie wykonawcze Komisji (UE) 2025/1568 z dnia 29 lipca 2025 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do ustaleń proceduralnych dotyczących wzajemnych ocen systemów identyfikacji elektronicznej i współpracy w zakresie organizacji takich przeglądów w ramach grupy współpracy oraz uchylające decyzję wykonawczą Komisji (UE) 2015/296 (Dz. Urz. UE. L. 2025/1568 z 30.07.2025), zwane dalej „rozporządzeniem 2025/1568”. 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. Urz. UE. L. z 2025/1569 z 30.07.2025, z późn. zm.), zwane dalej „rozporządzeniem 2025/1569”.
WYJAŚNIENIE TERMINU WEJŚCIA W ŻYCIE PROJEKTU / PROJEKTÓW	Art. 12. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia, z wyjątkiem: 1) art. 1 pkt 2–11, które wchodzą w życie z dniem następującym po dniu ogłoszenia; 2) art. 1 pkt 15 w zakresie art. 22a i art. 2, które wchodzą w życie z dniem 31 grudnia 2027 r.; 3) art. 4 pkt 1, pkt 3 lit. b, pkt 4 lit. b oraz d, oraz pkt 6, które wchodzą w życie z dniem 30 czerwca 2028 r.; 4) art. 4 pkt 7 w zakresie art. 20u ust. 3 pkt 1 lit. k i l, lit. o tiret pierwsze, lit. s, w, x oraz y oraz pkt 2 i 3, art. 20w ust. 1 pkt 1 lit. g oraz h, lit. l w zakresie adresu poczty elektronicznej, pkt 3 lit. b oraz ust. 2, art. 20y ust. 1–9, art. 20z, art. 20za–20zc oraz art. 6 pkt 1 i 4, które wchodzą w życie po upływie 24 miesięcy od dnia ogłoszenia; 5) art. 7 pkt 4 w zakresie art. 14a ust. 3 i art. 14c, które wchodzą w życie z dniem 31 grudnia 2029 r.; 6) art. 7 pkt 4 w zakresie art. 14d i art.14h, które wchodzą w życie z dniem 24 grudnia 2027 r. Termin wejścia w życie projektu ustawy uwzględnia konieczność podjęcia niezbędnych działań celem dostosowania do zmian jakie zostały wprowadzone do eIDAS,

				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. Wynikający z ww. rozporządzenia termin na zapewnienie co najmniej jednego europejskiego portfela tożsamości cyfrowej jest zbieżny z terminem wejścia w życie projektu ustawy. Ponadto, część aktów wykonawczych mających znaczenie dla poprawnego funkcjonowania europejskiego portfela tożsamości cyfrowej i jego niezbędnego otoczenia (rejestr stron ufających, elektroniczne poświadczenia atrybutów) została wydana dopiero w 2025 r. następnie znowelizowana w 2026 r zakresie istotnych szczegółów funkcjonowania całego systemu portfela i trwają prace nad zmianą norm i specyfikacji technicznych Europejskiego Instytutu Norm Telekomunikacyjnych wskazanych w tych aktach wykonawczych..
Rozporządzenie eIDAS					
JEDN. RED.	**TREŚĆ PRZEPISU UE**	**KONIE-CZNOŚĆ WDROŻE-NIA TAK / NIE***	**JEDN. RED.**	**TREŚĆ PRZEPISU / PRZEPISÓW PROJEKTU**	**UZASADNIENIE**
Art. 1	**Przedmiot** Celem niniejszego rozporządzenia jest zapewnienie właściwego funkcjonowania rynku wewnętrznego oraz odpowiedniego poziomu bezpieczeństwa środków identyfikacji elektronicznej i usług zaufania wykorzystywanych w całej Unii, aby umożliwić i ułatwić osobom fizycznym i prawnym korzystanie z prawa do bezpiecznego uczestnictwa w społeczeństwie cyfrowym oraz dostępu do usług publicznych i prywatnych online w całej Unii. W tym celu niniejsze rozporządzenie: a) określa warunki, na jakich państwa członkowskie mają zapewniać i uznawać środki identyfikacji	TAK	Art. 1 pkt 1 (Art. 1 pkt 8-14 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), zwanej dalej „ustawą o	**Art. 1.** W ustawie 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) wprowadza się następujące zmiany: 1) w art. 1 w ust. 1 w pkt 7 kropkę zastępuje się średnikiem i dodaje się pkt 8-14 w brzmieniu: „8) zasady i sposób prowadzenia rejestru stron ufających europejskim portfelom tożsamości cyfrowej;	Przepis określa zakres przedmiotowy zmian w ustawie o usługach zaufania oraz identyfikacji elektronicznej, wynikających z rozporządzenia eIDAS.

	elektronicznej osób fizycznych i prawnych, które objęte są notyfikowanym systemem identyfikacji elektronicznej innego państwa członkowskiego, oraz zapewniać i uznawać europejskie portfele tożsamości cyfrowej; b) określa przepisy dotyczące usług zaufania, w szczególności na potrzeby transakcji elektronicznych; c) ustanawia ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego, usług certyfikacyjnych uwierzytelniania witryn internetowych, archiwizacji elektronicznej, elektronicznego poświadczenia atrybutów, urządzeń do składania podpisu elektronicznego, urządzeń do składania pieczęci elektronicznej, oraz rejestrów elektronicznych.		usługach zaufania oraz identyfikacji elektronicznej”	9) dopasowywanie tożsamości osób fizycznych używających notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej; 10) środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację tych atrybutów drogą elektroniczną, na żądanie użytkownika; 11) zasady wydawania elektronicznych poświadczeń atrybutów, w tym w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne; 12) zasady wnioskowania o włączenie atrybutów do katalogu atrybutów prowadzonego przez Komisję Europejską; 13) zasady wnioskowania o włączenie schematów poświadczania atrybutów do katalogu schematów poświadczania atrybutów prowadzonego przez Komisję Europejską lub o zmianę tych schematów;	

				14) zasady i sposób prowadzenia krajowego katalogu schematów poświadczania atrybutów.”;	
Art. 2 ust. 1 i 3	1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej notyfikowanych przez państwo członkowskie, do europejskich portfeli tożsamości cyfrowej zapewnianych przez państwo członkowskie oraz do dostawców usług zaufania mających siedzibę w Unii. (…..) 3. Niniejsze rozporządzenie nie ma wpływu na prawo Unii ani prawo krajowe dotyczące zawierania i ważności umów, innych obowiązków prawnych lub proceduralnych dotyczących ich formy, ani na wymogi sektorowe dotyczące ich formy.4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 (*).	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 3 pkt 1-5, 5a, 6, 16, 18, 21, 23a, 23b, 38, 41, 42-57	1) »identyfikacja elektroniczna« oznacza proces używania danych identyfikujących osobę, w postaci elektronicznej, niepowtarzalnie reprezentujących osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną; 2) »środek identyfikacji elektronicznej« oznacza materialną lub niematerialną jednostkę zawierającą dane identyfikujące osobę i używaną do celów uwierzytelniania dla usługi online lub, w stosownych przypadkach, dla usługi offline; 3) »dane identyfikujące osobę« oznaczają zestaw danych, który jest wydawany zgodnie z prawem	NIE/TAK	Art. 7 pkt 2 (Art. 2 pkt 8a ustawy o aplikacji mObywatel)	„8a) europejski portfel tożsamości cyfrowej - europejski portfel tożsamości cyfrowej, o którym mowa w art. 3 pkt 42 rozporządzenia 910/2014;”;	Przepis stosowany wprost, nie wymaga wdrożenia. W zakresie definicji wskazano na definicję europejskiego portfel tożsamości cyfrowej z rozporządzenia 910/2014.

	Unii lub prawem krajowym i który umożliwia ustalenie tożsamości osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną; 4) »system identyfikacji elektronicznej« oznacza system identyfikacji elektronicznej, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym lub prawnym, lub osobom fizycznym reprezentującym inne osoby fizyczne lub osoby prawne; 5) »uwierzytelnianie« oznacza proces elektroniczny, który umożliwia potwierdzenie identyfikacji elektronicznej osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia i integralności danych w postaci elektronicznej; 5a) »użytkownik« oznacza osobę fizyczną lub prawną, lub osobę fizyczną reprezentującą inną osobę fizyczną lub osobę prawną, korzystającą z usług zaufania lub środków identyfikacji elektronicznej świadczonych lub zapewnianych zgodnie z niniejszym rozporządzeniem; 6) »strona ufająca« oznacza osobę fizyczną lub prawną, która polega na identyfikacji elektronicznej, europejskich portfelach tożsamości cyfrowej lub innym środku identyfikacji elektronicznej, lub na usłudze zaufania; (…..) 16) »usługa zaufania« oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą którąkolwiek z następujących czynności:				

	a) wydawanie certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania; b) walidację certyfikatów podpisów elektronicznych, certyfikatów pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych lub certyfikatów do celów świadczenia innych usług zaufania; c) tworzenie podpisów elektronicznych lub pieczęci elektronicznych; d) walidację podpisów elektronicznych lub pieczęci elektronicznych; e) konserwację podpisów elektronicznych, pieczęci elektronicznych, certyfikatów podpisów elektronicznych lub certyfikatów pieczęci elektronicznych; f) zarządzanie urządzeniami do składania podpisu elektronicznego na odległość lub urządzeniami do składania pieczęci elektronicznej na odległość; g) wydawanie elektronicznych poświadczeń atrybutów; h) walidację elektronicznych poświadczeń atrybutów; i) tworzenie elektronicznych znaczników czasu; j) walidację elektronicznych znaczników czasu; k) świadczenie usług rejestrowanego doręczenia elektronicznego;				

	l) walidację danych przekazywanych za pośrednictwem usług rejestrowanego doręczenia elektronicznego i związanych z nimi dowodów; m) archiwizację elektroniczną danych elektronicznych i dokumentów elektronicznych; n) rejestrowanie danych elektronicznych w rejestrze elektronicznym; (…..) pkt 18 otrzymuje brzmienie: 18) »jednostka oceniająca zgodność« oznacza jednostkę oceniającą zgodność zdefiniowaną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania, lub jako właściwa do dokonywania certyfikacji europejskich portfeli tożsamości cyfrowej lub środków identyfikacji elektronicznej; (….) 21) »produkt« oznacza sprzęt lub oprogramowanie, lub odpowiednie komponenty sprzętu lub oprogramowania, które są przeznaczone do wykorzystywania w zapewnianiu usług identyfikacji elektronicznej i usług zaufania; (…….) 23a) »kwalifikowane urządzenie do składania podpisu elektronicznego na odległość« oznacza kwalifikowane urządzenie do składania podpisu elektronicznego, którym zarządza kwalifikowany				

	dostawca usług zaufania zgodnie z art. 29a w imieniu podpisującego; 23b) »kwalifikowane urządzenie do składania pieczęci elektronicznej na odległość« oznacza kwalifikowane urządzenie do składania pieczęci elektronicznej, którym zarządza kwalifikowany dostawca usług zaufania zgodnie z art. 39a w imieniu składającego pieczęć; (….) 38) »certyfikat uwierzytelniania witryn internetowych« oznacza poświadczenie elektroniczne, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat; (…..) 41) »walidacja« oznacza proces weryfikacji i potwierdzania, że dane w postaci elektronicznej są ważne zgodnie z niniejszym rozporządzeniem; 42) »europejski portfel tożsamości cyfrowej« oznacza środek identyfikacji elektronicznej, który umożliwia użytkownikowi bezpieczne przechowywanie i walidację danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz bezpieczne zarządzanie tymi danymi i poświadczeniami na potrzeby udostępniania ich stronom ufającym oraz innym użytkownikom europejskich portfeli tożsamości cyfrowej, i który umożliwia składanie kwalifikowanych podpisów elektronicznych lub kwalifikowanych pieczęci elektronicznych;				

	43) »atrybut« oznacza cechę charakterystyczną, właściwość, prawo lub zezwolenie osoby fizycznej lub prawnej lub przedmiotu; 44) »elektroniczne poświadczenie atrybutów« oznacza poświadczenie w postaci elektronicznej, które umożliwia uwierzytelnienie atrybutów; 45) »kwalifikowane elektroniczne poświadczenie atrybutów« oznacza elektroniczne poświadczenie atrybutów, które jest wydawane przez kwalifikowanego dostawcę usług zaufania oraz spełnia wymogi określone w załączniku V; 46) »elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu« oznacza elektroniczne poświadczenie atrybutu wydane przez podmiot sektora publicznego, który jest odpowiedzialny za źródło autentyczne, lub przez podmiot sektora publicznego, który jest wyznaczony przez państwo członkowskie do wydawania takich poświadczeń atrybutów w imieniu podmiotów sektora publicznego odpowiedzialnych za źródła autentyczne zgodnie z art. 45f oraz z załącznikiem VII; 47) »źródło autentyczne« oznacza repozytorium lub system, za prowadzenie którego odpowiedzialny jest podmiot sektora publicznego lub podmiot prywatny, które zawiera i udostępnia atrybuty dotyczące osoby fizycznej lub prawnej lub przedmiotu i które uważa się za podstawowe źródło tych informacji lub uznaje za autentyczne zgodnie z prawem Unii lub prawem krajowym, w tym z praktykami administracyjnymi;				

	48) »archiwizacja elektroniczna« oznacza usługę zapewniającą odbiór, przechowywanie, pobieranie i usuwanie danych elektronicznych i dokumentów elektronicznych w celu zapewnienia ich trwałości i czytelności, a także zachowywania ich integralności, poufności i dowodu pochodzenia przez cały okres ich przechowywania; 49) »kwalifikowana usługa archiwizacji elektronicznej« oznacza usługę archiwizacji elektronicznej, która jest świadczona przez kwalifikowanego dostawcę usług zaufania i która spełnia wymogi określone w art. 45j; 50) »unijny znak zaufania dla portfela tożsamości cyfrowej« oznacza weryfikowalne i rozpoznawalne wskazanie, które w jasny sposób informuje, że europejski portfel tożsamości cyfrowej zapewniono zgodnie z niniejszym rozporządzeniem; 51) »silne uwierzytelnienie użytkownika« oznacza uwierzytelnienie w oparciu o zastosowanie co najmniej dwóch składników uwierzytelniania należących do różnych kategorii: wiedza, czyli coś, co wie wyłącznie użytkownik, posiadanie, czyli coś, co posiada wyłącznie użytkownik, albo cecha użytkownika, czyli coś, czym jest użytkownik, niezależnych w tym znaczeniu, że naruszenie jednego z nich nie osłabia wiarygodności pozostałych, które to uwierzytelnienie jest zaprojektowane, tak aby zapewniać ochronę poufności danych uwierzytelniających; 52) »rejestr elektroniczny« oznacza sekwencję elektronicznych wpisów danych zapewniającą integralność tych wpisów i prawidłowość ich chronologicznego uporządkowania;				

	53) »kwalifikowany rejestr elektroniczny« oznacza rejestr elektroniczny, który jest zapewniany przez kwalifikowanego dostawcę usług zaufania i który spełnia wymogi określone w art. 45l; 54) »dane osobowe« oznaczają wszelkie informacje zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679; 55) »dopasowywanie tożsamości« oznacza proces, w którym dane identyfikujące osobę lub środki identyfikacji elektronicznej są dopasowywane lub przyporządkowywane do istniejącego konta należącego do tej samej osoby; 56) »wpis danych« oznacza dane elektroniczne zarejestrowane wraz z powiązanymi metadanymi wspierającymi przetwarzanie danych; 57) »tryb offline« oznacza – w odniesieniu do europejskich portfeli tożsamości cyfrowej – interakcję między użytkownikiem a stroną trzecią w fizycznej lokalizacji przy użyciu technologii zbliżeniowych, przy czym europejski portfel tożsamości cyfrowej nie musi mieć dostępu do systemów zdalnych za pośrednictwem sieci komunikacji elektronicznej do celów tej interakcji.				
Art. 5	**Pseudonimy w transakcji elektronicznej** Bez uszczerbku dla szczegółowych przepisów prawa Unii lub prawa krajowego wymagających od użytkowników, aby zidentyfikowali się, lub dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów wybranych przez użytkownika.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 5a ust. 1	SEKCJA 1 EUROPEJSKI PORTFEL TOŻSAMOŚCI CYFROWEJ **Europejskie portfele tożsamości cyfrowej** 1. W celu zapewnienia wszystkim osobom fizycznym i prawnym w Unii bezpiecznego, zaufanego i niezakłóconego transgranicznego dostępu do usług publicznych i prywatnych, przy jednoczesnym zachowaniu pełnej kontroli nad ich danymi, każde państwo członkowskie zapewnia co najmniej jeden europejski portfel tożsamości cyfrowej w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w ust. 23 niniejszego artykułu i art. 5c ust. 6.	TAK	Art. 7 pkt 4 (Art. 14a ust. 1 ustawy z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. z 2026 r. poz. 3), zwanej dalej „ustawą o aplikacji mObywatel”)	Art. 14a. 1. Minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, w tym: 1) oprogramowanie przeznaczone dla urządzeń mobilnych umożliwiające korzystanie przez użytkownika z tego portfela, zapewniające w szczególności instancję portfela, o której mowa w art. 2 pkt 10 rozporządzenia wykonawczego Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz. Urz. UE L 2024/2979 z 04.12.2024), zwanego dalej „rozporządzeniem 2024/2979”; 2) bezpieczną aplikację kryptograficzną portfela, o której mowa w art. 2 pkt 1 rozporządzenia 2024/2979; 3) bezpieczne urządzenie kryptograficzne portfela, o którym mowa w art. 2 pkt 12 rozporządzenia 2024/2979; 4) dane identyfikujące osobę, o których mowa w ust. 2 i powiązanie	Wskazanie ministra właściwego do spraw informatyzacji jako podmiotu zapewniającego europejski portfel tożsamości cyfrowej wynika z doświadczenia nabytego przez tego ministra przy zapewnianiu aplikacji mObywatel o podobnej funkcjonalności.

			Art. 7 pkt 4 (Art. 14b. ust. 1 i 2 ustawy o aplikacji mObywatel)	tych danych z europejskim portfelem tożsamości cyfrowej. Art. 14b. 1. Użytkownikiem europejskiego portfela tożsamości cyfrowej może zostać osoba fizyczna, która została uwierzytelniona w jeden z następujących sposobów: 1) za pomocą profilu osobistego, albo; 2) za pomocą wydawanego w Polsce środka identyfikacji elektronicznej, dla którego potwierdzono spełnienie wymagań dla średniego poziomu bezpieczeństwa, z dodatkową weryfikacją tożsamości spełniającą wymagania określone w rozporządzeniu wykonawczym Komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi	Wskazane trzy sposoby potwierdzania tożsamości użytkowników wynikają z potrzeby zapewnienia europejskiego portfela tożsamości cyfrowej wszystkim osobom fizycznym (w tym rezydentom) którzy nie mają możliwości potwierdzania tożsamości profilem osobistym, a potwierdzanie profilem zaufanym jest niewystarczające ze względu na wymaganie wysokiego poziomu bezpieczeństwa dla europejskiego portfela tożsamości cyfrowej w kontekście przepisów rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków

				procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi wysokiego poziomu bezpieczeństwa (Dz. Urz. UE L 2026/798 z 08.04.2026) określoną w przepisach wydanych na podstawie ust. 10, albo 3) w punkcie potwierdzającym tożsamość podczas obecności fizycznej osoby ubiegającej się o wydanie europejskiego portfela tożsamości cyfrowej po okazaniu dokumentu stwierdzającego tożsamość i obywatelstwo, który zawiera dowody identyfikacji fotograficznej lub biometrycznej, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235z 09.09.2015, z późn. zm.), zwanego dalej „rozporządzeniem	identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.Urz. UE L 235 z 09.09.2015, str. 7, z późn. zm.).

			Art. 7 pkt 4	2015/1502”, umożliwiające potwierdzenie deklarowanej tożsamości, w celu porównania co najmniej jednej cechy fizycznej osoby, której tożsamość jest weryfikowana, albo 4) z wykorzystaniem innej metody weryfikacji tożsamości, określonej w przepisach wydanych na podstawie ust. 11. 2. Funkcję punktu potwierdzającego tożsamość, o którym mowa w ust. 1 pkt 3: 1) pełni wojewoda; 2) może pełnić, za zgodą ministra właściwego do spraw informatyzacji: a) bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2026 r. poz. 38, z późn. zm.), b) organ gminy lub organ miasta na prawach powiatu. Art. 14c. 1. Użytkownikiem europejskiego portfela tożsamości cyfrowej osoby prawnej może zostać: 1) osoba fizyczna po uwierzytelnieniu za pomocą	Art. 5a ust. 1 rozporządzenia eIDAS wymaga zapewnienia europejskiego portfela tożsamości cyfrowej również dla osób prawnych, dlatego przewidziano rozwiązania w tym zakresie.

			(Art. 14c ust. 1 ustawy o aplikacji mObywatel)	europejskiego portfela tożsamości cyfrowej wydanego tej osobie oraz kwalifikowanego elektronicznego poświadczenia atrybutów poświadczającego pełnomocnictwo tej osoby do posługiwania się europejskim portfelem tożsamości cyfrowej osoby prawnej; 2) osoba fizyczna wskazana we wniosku osoby prawnej złożonym do ministra właściwego do spraw informatyzacji za pomocą usługi online udostępnianej przez tego ministra; 3) osoba fizyczna prowadząca działalność gospodarczą po uwierzytelnieniu za pomocą europejskiego portfela tożsamości cyfrowej.	
			Art. 7 pkt 4 (Art. 14h 1 ustawy o aplikacji mObywatel)	Art. 14h. Dostęp do aplikacji mObywatel i europejskiego portfela tożsamości cyfrowej w pełnym albo ograniczonym zakresie funkcjonalności, może być zapewniany przez ministra właściwego do spraw informatyzacji w ramach jednego rozwiązania techniczno-organizacyjnego 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.”;	

			Art. 7 pkt 6 (Art. 21 ustawy o aplikacji mObywatel)	6) w art. 21: a) w ust. 1: - po pkt 1 dodaje się pkt 1a w brzmieniu: „1a) regulamin korzystania z europejskiego portfela tożsamości cyfrowej;”, - pkt 3 otrzymuje brzmienie: „3) informacje w zakresie aplikacji mObywatel dotyczące: a) udostępnianych usług, b) usług czasowo zawieszonych, c) potwierdzania autentyczności, ważności, integralności oraz pochodzenia dokumentów mobilnych, w tym zabezpieczeń wizualnych tych dokumentów, d) udostępnianych metod unieważnienia certyfikatów użytkownika aplikacji mObywatel, e) ogólnych warunków świadczenia usług w aplikacji mObywatel, o których mowa w art. 15 ust. 3, oraz listy usług świadczonych na tej podstawie;”, - dodaje się pkt 4 w brzmieniu: „4) informacje w zakresie europejskiego portfela tożsamości cyfrowej dotyczące:	

				a) udostępnianych usług, b) usług czasowo zawieszonych.”; b) po ust. 3 dodaje się ust. 3a w brzmieniu: „3a. Regulamin korzystania z europejskiego portfela tożsamości cyfrowej określa co najmniej: 1) warunki bezpiecznego korzystania z tego portfela; 2) warunki licencyjne korzystania z tego portfela; 3) wymagania techniczne pozwalające na korzystanie z tego portfela, 4)_ politykę określającą warunki i ramy czasowe unieważniania poświadczeń jednostki portfela, o której mowa w art. 7 ust. 2 rozporządzenia 2024/2979; 5) politykę oraz warunki dostawcy portfela, które mają zastosowanie w zakresie portfela i korzystania z tego rozwiązania, o której mowa w ust. 2 pkt 1 lit g załącznika II do rozporządzenia wykonawczego Komisji (UE) 2024/2980 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do notyfikowania Komisji w związku z	

				ekosystemem europejskiego portfela tożsamości cyfrowej (Dz. Urz. UE L 2024/2980 z 04.12.2024), zwanego dalej „rozporządzeniem 2024/2980”; 6) politykę oraz warunki dostawcy danych identyfikujących osobę mające zastosowanie do dostarczania i wykorzystywania danych identyfikujących osobę, o której mowa w ust. 3 pkt 1 lit. g załącznika II do rozporządzenia 2024/2980; c) dodaje się ust. 6 w brzmieniu: „6. Użytkownik europejskiego portfela tożsamości cyfrowej w celu prawidłowego korzystania z tego portfela postępuje zgodnie z regulaminem korzystania z europejskiego portfela tożsamości cyfrowej.”;	
Art. 5a ust. 2	2. Europejskie portfele tożsamości cyfrowej muszą być zapewniane w co najmniej jeden z następujących sposobów: a) bezpośrednio przez państwo członkowskie; b) na podstawie upoważnienia od państwa członkowskiego; c) niezależnie od państwa członkowskiego, lecz uznawane przez to państwo członkowskie.	TAK	Art. 1 pkt 17 (Art. 24a ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 24a. 1. Wniosek o uznanie europejskiego portfela tożsamości cyfrowej wydawanego niezależnie od państwa członkowskiego Unii Europejskiej, o którym mowa w art. 5a ust. 2 lit. c rozporządzenia 910/2014, składa do ministra właściwego do spraw informatyzacji dostawca takiego portfela. 2. Do wniosku załącza się dokument potwierdzający	Ustalenie sposobu zapewnienia w Polsce innego europejskiego portfela tożsamości cyfrowej, niż wydawany przez ministra właściwego do spraw informatyzacji.

				certyfikację, o której mowa w art. 5c ust. 1 rozporządzenia 910/2014. 3. Minister właściwy do spraw informatyzacji rozpatrując wniosek bierze pod uwagę warunki kwalifikowania się systemu identyfikacji elektronicznej, w ramach którego zapewniany ma być europejski portfel tożsamości cyfrowej, do notyfikowania, wskazane w art. 7 rozporządzenia 910/2014, certyfikację, o której mowa w art. 12a ust. 1 tego rozporządzenia oraz politykę państwa w zakresie identyfikacji elektronicznej. 4. Po pozytywnym rozpatrzeniu wniosku minister właściwy do spraw informatyzacji wydaje decyzję o uznaniu europejskiego portfela tożsamości cyfrowej, o którym mowa w ust. 1, i informuje o tym Komisję Europejską i grupę współpracy oraz przekazuje Komisji Europejskiej informacje o których mowa w art. 5a ust. 18 rozporządzenia 910/2014. 5. Odmowa uwzględnienia wniosku, o którym mowa w ust. 1, następuje w drodze decyzji.	
			Art. 7 pkt 1	**Art. 7.** W ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz.	

			(Art. 1 pkt 6 i 7 ustawy o aplikacji mObywatel)	U. z 2026 r. poz. 3) wprowadza się następujące zmiany: 1) w art. 1w pkt 5 kropkę zastępuje się średnikiem i dodaje się pkt 6-8 w brzmieniu: „6) sposób zapewnienia przez ministra właściwego do spraw informatyzacji europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 3 pkt 42 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73, z późn. zm.), zwanego dalej „rozporządzeniem 910/2014, oraz sposób jego funkcjonowania; 7) warunki i sposób pobierania przez użytkownika europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 3 pkt 42 rozporządzenia 910/2014, zapewnianego przez ministra właściwego do spraw informatyzacji, danych dotyczących tego użytkownika, pochodzących z rejestrów publicznych, rejestrów niepublicznych lub systemów teleinformatycznych podmiotów	

				publicznych lub podmiotów niepublicznych;	
Art. 5a ust. 3	3. Kod źródłowy komponentów oprogramowania użytkowego europejskich portfeli tożsamości cyfrowej musi być objęty licencją otwartego oprogramowania. Państwa członkowskie mogą postanowić, że z należycie uzasadnionych powodów nie ujawnia się kodu źródłowego poszczególnych komponentów innych niż zainstalowane na urządzeniach użytkownika.	TAK	Art. 1 pkt 14 (Art. 23 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 2) po uzyskaniu opinii CSIRT GOV, CSIRT MON i CSIRT NASK, o których mowa w art. 2 pkt 1 -3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej kod źródłowy poszczególnych komponentów oprogramowania europejskiego portfela tożsamości cyfrowej, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel z wyłączeniem informacji, których ujawnienie mogłoby zagrozić bezpieczeństwu portfela, bezpieczeństwu państwa lub ciągłości świadczenia usług, w szczególności danych konfiguracyjnych, mechanizmów ochrony przed nadużyciami oraz komponentów zawierających informacje niejawne;	Skoro minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, powinien on również udostępniać kod źródłowy. Z uwagi na rolę CSIRT GOV, CSIRT MON i CSIRT NASK zasadne jest uzyskanie opinii tych jednostek o uzasadnionej potrzebie nieudostępniania części kodu.
Art. 5a ust. 4 i 5 lit. a-f	4. Europejskie portfele tożsamości cyfrowej muszą umożliwiać użytkownikowi, w sposób przyjazny, przejrzysty i identyfikowalny dla użytkownika:	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	a) bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację – pod wyłączną kontrolą użytkownika – danych identyfikujących osobę oraz, w stosownych przypadkach, w połączeniu z elektronicznymi poświadczeniami atrybutów, uwierzytelnianie wobec stron ufających w trybie online oraz, w stosownych przypadkach, w trybie offline, w celu uzyskania dostępu do usług publicznych i prywatnych, przy jednoczesnym zapewnieniu możliwości selektywnego ujawniania danych; b) generowanie pseudonimów i przechowywanie ich w zaszyfrowanej formie i lokalnie w europejskim portfelu tożsamości cyfrowej; c) bezpieczne uwierzytelnianie europejskiego portfela tożsamości cyfrowej innej osoby oraz otrzymywanie i udostępnianie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów w bezpieczny sposób między dwoma europejskimi portfelami tożsamości cyfrowej; d) dostęp do rejestru wszystkich transakcji przeprowadzonych z wykorzystaniem europejskiego portfela tożsamości cyfrowej za pomocą wspólnego panelu zarządzania umożliwiającego użytkownikowi: (i) przeglądanie aktualnej listy stron ufających, z którymi użytkownik ustanowił połączenie, oraz, w stosownych przypadkach, wszystkich udostępnionych danych;				

	(ii) łatwe zażądanie od strony ufającej usunięcia danych osobowych zgodnie z art. 17 rozporządzenia (UE) 2016/679; (iii) łatwe zgłaszanie strony ufającej właściwemu krajowemu organowi ochrony danych, w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych; e) składanie kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych; f) pobieranie, w zakresie, w jakim jest to technicznie wykonalne, danych użytkownika, elektronicznych poświadczeń atrybutów i konfiguracji; g) korzystanie z praw użytkownika do przenoszenia danych. 5. Europejskie portfele tożsamości cyfrowej, w szczególności: a) muszą być zgodne ze wspólnymi protokołami i interfejsami: (i) do celów wydawania danych identyfikujących osobę, kwalifikowanych i niekwalifikowanych elektronicznych poświadczeń atrybutów lub kwalifikowanych i niekwalifikowanych certyfikatów do europejskiego portfela tożsamości cyfrowej; (ii) na potrzeby stron ufających do celów żądania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów oraz ich walidacji; (iii) na potrzeby udostępniania i prezentacji stronom ufającym danych identyfikujących osobę, elektronicznych poświadczeń atrybutów lub selektywnie ujawnionych powiązanych danych w				

	trybie online oraz, w stosownych przypadkach, w trybie offline; (iv) aby umożliwić użytkownikowi interakcję z europejskim portfelem tożsamości cyfrowej oraz wyświetlenie unijnego znaku zaufania dla portfela tożsamości cyfrowej; (v) na potrzeby bezpiecznej rejestracji użytkownika przy użyciu środka identyfikacji elektronicznej zgodnie z art. 5a ust. 24; (vi) na potrzeby interakcji między europejskimi portfelami tożsamości cyfrowej dwóch osób do celów otrzymywania, walidowania oraz udostępniania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów w bezpieczny sposób; (vii) na potrzeby uwierzytelnienia i identyfikacji stron ufających poprzez wdrożenie mechanizmów uwierzytelniania zgodnie z art. 5b; (viii) na potrzeby stron ufających do celów weryfikowania autentyczności i ważności europejskich portfeli tożsamości cyfrowej; (ix) na potrzeby zażądania od strony ufającej usunięcia danych osobowych zgodnie z art. 17 rozporządzenia (UE) 2016/679; (x) na potrzeby zgłoszenia strony ufającej właściwemu krajowemu organowi ochrony danych w przypadku otrzymania przypuszczalnie niezgodnego z prawem lub podejrzanego żądania udostępnienia danych; (xi) na potrzeby składania kwalifikowanych podpisów elektronicznych lub pieczęci				

	elektronicznych za pomocą kwalifikowanych urządzeń do składania podpisów elektronicznych lub pieczęci elektronicznych; b) nie mogą dostarczać dostawcom usług zaufania elektronicznych poświadczeń atrybutów jakichkolwiek informacji na temat wykorzystywania tych elektronicznych poświadczeń; c) muszą zapewniać możliwość uwierzytelnienia i identyfikacji stron ufających poprzez wdrożenie mechanizmów uwierzytelniania zgodnie z art. 5b; d) muszą spełniać wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa, w szczególności w zakresie wymogów dotyczących potwierdzania i weryfikacji tożsamości, zarządzania środkami identyfikacji elektronicznej oraz uwierzytelniania; e) w przypadku elektronicznego poświadczenia atrybutów z wbudowanymi regułami ujawniania – muszą wdrażać odpowiedni mechanizmu informowania użytkownika, że strona ufająca lub użytkownik europejskiego portfela tożsamości cyfrowej wnioskujący o udostępnienie tego elektronicznego poświadczenia atrybutów ma zezwolenie na dostęp do takiego poświadczenia; f) muszą zapewniać, aby dane identyfikujące osobę, które są dostępne w systemie identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej, niepowtarzalnie reprezentowały osobę fizyczną, osobę prawną, lub osobę fizyczną reprezentującą osobę fizyczną lub prawną, oraz były powiązane z tym europejskim portfelem tożsamości cyfrowej;				

Art. 5a ust. 5 lit. g	5. Europejskie portfele tożsamości cyfrowej, w szczególności: (…) g) muszą oferować wszystkim osobom fizycznym możliwości składania kwalifikowanych podpisów elektronicznych, domyślnie i nieodpłatnie. Niezależnie od akapitu pierwszego lit. g) państwa członkowskie mogą przewidzieć proporcjonalne środki w celu zapewnienia, aby nieodpłatne używanie kwalifikowanych podpisów elektronicznych przez osoby fizyczne było ograniczone do celów innych niż profesjonalne.	TAK (zapewnienie podpisu) NIE (ograniczenie do celów innych niż profesjonalne)	Art. 7 pkt 4 (Art.14e i 14f ustawy o aplikacji mObywatel)	Art. 14e. 1. Minister właściwy do spraw informatyzacji udostępnia usługę, która umożliwia 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. 2. W celu zapewnienia usługi, o której mowa w ust. 1, minister właściwy do spraw informatyzacji na wniosek kwalifikowanego dostawcy usług zaufania, wpisanego do rejestru, o którym mowa w art. 2 pkt 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, świadczącego kwalifikowane usługi zaufania w zakresie zarządzania urządzeniami do składania kwalifikowanego podpisu elektronicznego na odległość, może w drodze decyzji, wyrazić zgodę na świadczenie usługi, o której mowa w ust. 1. 3. Wniosek, o którym mowa w ust. 2, zawiera: 1) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer KRS, a w przypadku, gdy podmiot	Minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej powinien również zapewniać osobom fizycznym nieodpłatny kwalifikowany podpis elektroniczny. Mając na uwadze potencjalne koszty, jakie trzeba byłoby rekompensować kwalifikowanym dostawcom usług zaufania za świadczenie nieodpłatnych usług, gdyby możliwe byłoby składanie podpisów w każdym celu, ograniczono możliwość składania takich podpisów do celów nieprofesjonalnych. Zakłada się bowiem, że wspólne ponoszenie kosztów przez wszystkich podatników na kwalifikowane podpisy elektroniczne używane nie tylko w celach nieprofesjonalnych, ale

				nie posiada takiego numeru, numer identyfikacji podatkowej (NIP); 2) oświadczenie o zapewnieniu stosowania wytycznych, o których mowa w ust. 8. 4. Minister właściwy do spraw informatyzacji wydaje decyzję, o której mowa w ust. 2, po przeprowadzeniu testów integracyjnych zakończonych pozytywnym wynikiem, potwierdzających interoperacyjność świadczonej usługi z aplikacją mObywatel oraz europejskim portfelem tożsamości cyfrowej, o którym mowa w art. 14a ust. 1. 5. Kwalifikowanym dostawcom usług zaufania świadczącym nieodpłatną usługę, o której mowa w ust. 1, przysługuje rekompensata. 6. Rekompensata, o której mowa w ust. 5, przysługuje: 1) za każdy pełny miesiąc kalendarzowy świadczenia usługi, o której mowa w ust. 1, począwszy od następnego miesiąca, w którym dany dostawca rozpoczął świadczenie usługi; 2) w kwocie obliczonej zgodnie ze wzorem $KMW = SOG/12 + (LUP \times SOU/L$	również w celu prowadzenia działalności biznesowej przez przedsiębiorców, byłoby nieetyczne, z uwagi na to, że ilość podpisów, jakie potrzebuje złożyć osoba fizyczna w celach nieprofesjonalnych, jest znikoma wobec ilości podpisów, jakie potrzebuje złożyć firma lub osoba fizyczna prowadząca działalność gospodarczą w celach profesjonalnych. Ponadto, warto dodać, że przedsiębiorcy i podmioty publiczne w większości usług publicznych mogą już wykorzystać darmowy podpis zaufany.

				- gdzie poszczególne symbole oznaczają następujące parametry: a) KMW – kwota miesięcznej rekompensaty dla kwalifikowanego dostawcy usług zaufania, wynikającą z nieodpłatnego świadczenia użytkownikom aplikacji mObywatel oraz europejskiego portfela tożsamości cyfrowej usługi składania kwalifikowanego podpisu elektronicznego, w celach innych niż profesjonalne, za pomocą urządzenia do składania kwalifikowanego podpisu elektronicznego na odległość, b) LUP – liczba osób fizycznych, które co najmniej raz skorzystały w okresie ostatnich 12 miesięcy z usługi, o której mowa w ust. 1, ustalana na ostatni dzień danego miesiąca, za który jest przyznawana rekompensata, z zastrzeżeniem, że w przypadku gdy parametr ten wyniesie więcej niż 10 000 000, przyjmuje się dla tego parametru wartość równą 10 000 000, c) SOU – stawka opłaty za każdą osobę fizyczną, która skorzystała w okresie ostatnich 12 miesięcy skorzystała z usługi, o której mowa w ust. 1, co najmniej raz ,	

				d) SOG – opłata za utrzymywanie gotowości do świadczenia usługi składania kwalifikowanego podpisu elektronicznego, w celach innych niż profesjonalne, e) LD – liczba dostawców usług zaufania, którzy świadczyli usługę w danym miesiącu. 7. Kwalifikowani dostawcy usług zaufania świadczą usługę, o której mowa w ust. 1, zgodnie z wytycznymi świadczenia tej usługi udostępnionymi przez ministra właściwego do spraw informatyzacji w Biuletynie Informacji Publicznej na jego stronie podmiotowej. 8. Wytyczne świadczenia usługi, o której mowa w ust. 1, określają: 1) sposób weryfikacji tożsamości użytkowników; 2) obsługiwane formaty podpisów; 3) szczególne wymagania dotyczące wydawanych certyfikatów kwalifikowanego podpisu elektronicznego; 4) sposób oznaczania podpisanych dokumentów elektronicznych informacją o opatrzeniu nieodpłatnym kwalifikowanym podpisem elektronicznym,	

				złożonym w celach innych niż profesjonalne. 9. Rekompensatę, o której mowa w ust. 5, wypłaca się na wniosek podmiotu uprawnionego, złożony do ministra właściwego do spraw informatyzacji do 25. dnia miesiąca następującego po miesiącu, za który przysługuje rekompensata. 10. Wniosek, o którym mowa w ust. 9, zawiera: 1) imię i nazwisko lub firmę (nazwę), adres siedziby i miejsca wykonywania działalności, numer KRS, a w przypadku gdy podmiot nie ma takiego numeru – numer identyfikacji podatkowej (NIP); 2) wskazanie przedmiotu wniosku;[MW1.1] 3) proponowaną kwotę rekompensaty; 4) oznaczenie miesiąca i roku, za który przysługuje rekompensata. 11. Minister właściwy do spraw informatyzacji weryfikuje wniosek o wypłatę rekompensaty pod względem prawidłowości dokonanych obliczeń i kompletności danych.	

				12. W przypadku pozytywnej weryfikacji wniosku o wypłatę rekompensaty minister właściwy do spraw informatyzacji zatwierdza wniosek i dokonuje wypłaty rekompensaty w terminie 14 dni od dnia otrzymania prawidłowo sporządzonego wniosku. 13. W przypadku, gdy wniosek o wypłatę rekompensaty zawiera braki formalne lub błędy obliczeniowe, minister właściwy do spraw informatyzacji, wzywa w terminie 7 dni od dnia otrzymania wniosku, podmiot uprawniony do usunięcia braków formalnych lub błędów obliczeniowych w terminie 7 dni od dnia otrzymania wezwania do ich usunięcia. 14. W przypadku nieusunięcia braków formalnych lub błędów obliczeniowych zawartych we wniosku o wypłatę rekompensaty w terminie 7 dni od dnia otrzymania wezwania do ich usunięcia minister właściwy do spraw informatyzacji odmawia zatwierdzenia wniosku, informując podmiot uprawniony o przyczynie tej odmowy. Odmowa zatwierdzenia wniosku o wypłatę rekompensaty nie wymaga wydania decyzji administracyjnej. 15. Odmowa, o której mowa w ust. 14, nie pozbawia podmiotu	

				uprawnionego możliwości ponownego złożenia wniosku o wypłatę rekompensaty. Przepisy ust. 9-13 stosuje się odpowiednio. 16. Minister właściwy do spraw informatyzacji określi w drodze rozporządzenia wysokość kwot SOG i SOU, o których mowa w ust. 6 mając na uwadze zapewnienie użytkownikom, o których mowa w ust. 1, nieprzerwanej usługi składania kwalifikowanego podpisu elektronicznego na odległość w celach innych niż profesjonalne, liczbę tych użytkowników i spodziewany zakres korzystania przez tych użytkowników z nieodpłatnej usługi składania kwalifikowanych podpisów elektronicznych. 17. Minister właściwy do spraw informatyzacji udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej dane będące podstawą do obliczenia rekompensaty, o których mowa w ust. 6 pkt 2 lit. b oraz e.[Art. 14f. 1. Przez cel składania kwalifikowanego podpisu elektronicznego inny niż profesjonalny rozumie się składanie tego podpisu w celu złożenia oświadczenia woli w swoim imieniu lub imieniu innej osoby fizycznej, w	

				celu załatwienia sprawy prywatnej, niezwiązanej z wykonywanym zawodem, prowadzoną działalnością gospodarczą lub działalnością osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, który składający to oświadczenia reprezentuje. 2. Dokumenty elektroniczne opatrzone nieodpłatnym kwalifikowanym podpisem elektronicznym, udostępnianym w ramach usługi, o której mowa w art. 14e ust. 1, w celu innym niż profesjonalny, oznacza się w sposób umożliwiający stwierdzenie użycia takiego podpisu.	
Art. 5a ust. 6	6. Państwa członkowskie bez zbędnej zwłoki informują użytkowników o wszelkich naruszeniach bezpieczeństwa, które mogłyby spowodować całkowite lub częściowe skompromitowanie ich europejskich portfeli tożsamości cyfrowej lub zawartości tych portfeli, w szczególności jeżeli ich europejski portfel tożsamości cyfrowej został zawieszony lub unieważniony zgodnie z art. 5e.	TAK	Art. 1 pkt 14 (Art. 23 pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 3) informuje użytkowników europejskich portfeli tożsamości cyfrowej o wszelkich naruszeniach bezpieczeństwa zgodnie z art. 5a ust. 6 rozporządzenia 910/2014;	Skoro minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, powinien on również informować o naruszeniach.
Art. 5a ust. 7	7. Bez uszczerbku dla art. 5f państwa członkowskie mogą przewidzieć, zgodnie z prawem krajowym, dodatkowe funkcje europejskich portfeli tożsamości cyfrowej, w tym interoperacyjność z istniejącymi krajowymi środkami identyfikacji elektronicznej. Te	TAK	Art. 7 pkt 1 (Art. 1 pkt 8 ustawy o aplikacji mObywatel)	Art. 1 (…) 8) warunki opracowywania, udostępniania i świadczenia usług w europejskim portfelu tożsamości	Projektowane przepisy mają na celu zapewnienie podstaw prawnych, które pozwolą na świadczenie w

	dodatkowe funkcje muszą być zgodne z niniejszym artykułem.			cyfrowej, o którym mowa w art. 3 pkt 42 rozporządzenia 910/2014, zapewnianym przez ministra właściwego do spraw informatyzacji.”; Art. 14g. 1. W europejskim portfelu tożsamości cyfrowej mogą być udostępniane usługi umożliwiające użytkownikowi tego portfela: 1) pobranie następujących danych pochodzących ze źródła autentycznego wskazanego w krajowym katalogu schematów poświadczania atrybutów, o którym mowa w art. 22g ust. 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej: a) danych osobowych tego użytkownika niezbędnych do realizacji usługi, b) danych dotyczących sytuacji prawnej tego użytkownika lub praw mu przysługujących, c) danych umożliwiających identyfikację rzeczy związanej z tym użytkownikiem, d) danych dotyczących sytuacji prawnej osoby niepełnoletniej lub	Art. 7 pkt 4 (Art. 14g ustawy o aplikacji mObywatel)	europejskim portfelu tożsamości szerokiej palety usług.

				praw przysługujących tej osobie, jeżeli użytkownik portfela jest: – rodzicem osoby niepełnoletniej, z wyłączeniem rodzica, którego sąd pozbawił władzy rodzicielskiej lub któremu sąd ograniczył władzę rodzicielską przez umieszczenie dziecka w pieczy zastępczej, albo – opiekunem prawnym osoby niepełnoletniej, z wyłączeniem rodzica zastępczego lub prowadzącego rodzinny dom dziecka, w przypadku gdy sąd orzekł o odebraniu mu dziecka z uwagi na niewłaściwe sprawowanie pieczy zastępczej; 2) uzyskanie elektronicznego poświadczenia atrybutów wystawionego przez ministra właściwego do spraw informatyzacji, zawierającego dane, o których mowa w pkt 1; 3) korzystanie z usług online, o których mowa w art. 19aa i art. 19ab ustawy z dnia 17 lutego 2005 r o informatyzacji działalności podmiotów realizujących zadania publiczne; 4) użycie urządzenia mobilnego w celu obsługi jednego z czynników uwierzytelniania profilu zaufanego, o którym mowa w art. 3 pkt 14 ustawy z dnia 17 lutego 2005 r.	

				o informatyzacji działalności podmiotów realizujących zadania publiczne; 5) otrzymywanie komunikatów dotyczących usług świadczonych w innych systemach teleinformatycznych na rzecz użytkownika europejskiego portfela tożsamości cyfrowej, o którym mowa w art. 14a ust. 1; 6) dokonywanie płatności elektronicznych związanych z usługami online świadczonymi na rzecz użytkownika europejskiego portfela tożsamości cyfrowej,; 7) opatrywanie dokumentu elektronicznego podpisem zaufanym, podpisem osobistym oraz kwalifikowanym podpisem elektronicznym, oraz weryfikację tych podpisów. 2. W europejskim portfelu tożsamości cyfrowej można udostępniać inne usługi, niż określone w ust. 1, świadczone przez podmioty publiczne lub podmioty niepubliczne prowadzące rejestry publiczne, rejestry niepubliczne lub systemy teleinformatyczne. 4) w art. 16:	

			Art. 7 pkt 5 (Art. 16 ust. 1, ust. 3 pkt 2 lit. b, ust. 7, 8 i 12 ustawy o aplikacji mObywatel)	a) ust. 1 otrzymuje brzmienie: „1. Podmiot zainteresowany świadczeniem nowej usługi w aplikacji mObywatel i w ramach europejskiego portfela tożsamości cyfrowej, może wystąpić do ministra właściwego do spraw informatyzacji z wnioskiem o opracowanie, udostępnienie oraz umożliwienie temu podmiotowi świadczenia takiej usługi.”, b) w ust 2 pkt 2 w lit. b po wyrazach „aplikacji mObywatel” dodaje się wyrazy „i użytkownika europejskiego portfela tożsamości cyfrowej”, c) w ust. 6: – we wprowadzeniu do wyliczenia po wyrazach „aplikacji mObywatel” dodaje się wyrazy „i europejskim portfelu tożsamości cyfrowej,”, – pkt 2 otrzymuje brzmienie: „2) bezpieczeństwo aplikacji mObywatel, systemu mObywatel i użytkowników aplikacji mObywatel oraz bezpieczeństwo europejskiego portfela tożsamości cyfrowej i jego użytkowników,”, d) w ust. 7 po wyrazach „aplikacji mObywatel” dodaje się wyrazy „i	

				europejskim portfelu tożsamości cyfrowej , e) w ust. 11 po wyrazach „aplikacji mObywatel” dodaje się wyrazy „i europejskim portfelu tożsamości cyfrowej”.	
Art. 5a ust. 8	8. Państwa członkowskie zapewniają mechanizmy walidacji nieodpłatnie, aby: a) zapewnić możliwość weryfikacji autentyczności i ważności europejskich portfeli tożsamości cyfrowej; b) umożliwić użytkownikom weryfikację autentyczności i ważności tożsamości stron ufających zarejestrowanych zgodnie z art. 5b.	TAK	Art. 1 pkt 14 (Art. 23 pkt 4 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji (…) 4) zapewnia nieodpłatne mechanizmy walidacji, o których mowa w art. 5a ust. 8 rozporządzenia 910/2014;	Skoro minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, powinien on również zapewniać możliwość weryfikacji jego autentyczności i ważności.
Art. 5a ust. 9-10	9. Państwa członkowskie zapewniają, aby europejski portfel tożsamości cyfrowej mógł zostać unieważniony w następujących przypadkach: a) na wyraźne żądanie użytkownika; b) w przypadku bezpieczeństwo europejskiego portfela tożsamości cyfrowej zostało skompromitowane; c) po śmierci użytkownika lub zaprzestaniu działalności przez osobę prawną. 10. Dostawcy europejskich portfeli tożsamości cyfrowej muszą zapewniać użytkownikom możliwość łatwego zwracania się o wsparcie techniczne oraz zgłaszania problemów technicznych lub wszelkich innych incydentów mających negatywny wpływ na używanie europejskiego portfela tożsamości cyfrowej.	TAK	Art. 7 pkt 4 (Art. 14a ust. 8 ustawy o aplikacji mObywatel)	8. Europejski portfel tożsamości cyfrowej może być unieważniony: 1) w przypadkach, o których mowa w art. 5a ust. 9 lit. a i b rozporządzenia 910/2014 – w sposób określony w krajowym programie certyfikacji, o którym mowa w art. 22j ust. 1 pkt 1 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej; 2) w przypadku o którym mowa w art. 5a ust. 9 lit. c rozporządzenia 910/2014 – automatycznie gdy: a) w rejestrze PESEL został odnotowany zgon osoby fizycznej będącej użytkownikiem	Niezbędne jest określenie sposobów unieważnienia europejskiego portfela tożsamości cyfrowej w określonych przypadkach.

				europejskiego portfela tożsamości cyfrowej , b) w Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w Krajowym Rejestrze Sądowym lub w Katalogu Podmiotów Publicznych zostało odnotowane zakończenie działalności podmiotu, któremu wydano europejski portfel tożsamości cyfrowej.	
Art. 5a ust. 11-16	11. Europejskie portfele tożsamości cyfrowej zapewnia się w ramach systemu identyfikacji elektronicznej, na wysokim poziomie bezpieczeństwa. 12. Europejskie portfele tożsamości cyfrowej muszą zapewniać uwzględnianie bezpieczeństwa na etapie projektowania. 13. Wydawanie wykorzystywanie i unieważnianie europejskich portfeli tożsamości cyfrowej musi być nieodpłatne dla wszystkich osób fizycznych. 14. Użytkownicy muszą mieć pełną kontrolę nad używaniem swojego europejskiego portfela tożsamości cyfrowej oraz znajdujących się w nim danych. Dostawca europejskiego portfela tożsamości cyfrowej nie może gromadzić informacji na temat używania europejskiego portfela tożsamości cyfrowej, które nie są niezbędne do świadczenia usług europejskiego portfela tożsamości cyfrowej, ani łączyć danych identyfikujących osobę lub jakichkolwiek innych danych osobowych przechowywanych lub związanych z używaniem europejskiego portfela	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	tożsamości cyfrowej z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez tego dostawcę lub z usług osób trzecich, które nie są niezbędne do świadczenia usług europejskiego portfela tożsamości cyfrowej, chyba że użytkownik wyraźnie tego zażąda. Dane osobowe związane z dostarczaniem europejskiego portfela tożsamości cyfrowej muszą być logicznie oddzielone od wszelkich innych danych będących w posiadaniu dostawcy danego europejskiego portfela tożsamości cyfrowej. Jeżeli europejski portfel tożsamości cyfrowej jest dostarczany przez podmioty prywatne zgodnie z ust. 2 lit. b) i c) niniejszego artykułu, przepisy art. 45h ust. 3 stosuje się odpowiednio. 15. Używanie europejskich portfeli tożsamości cyfrowej musi być dobrowolne. Osobom fizycznym i prawnym, które nie korzystają z europejskich portfeli tożsamości cyfrowej, nie można w żaden sposób ograniczać ani utrudniać dostępu do usług publicznych i prywatnych, dostępu do rynku pracy i swobody prowadzenia działalności gospodarczej. Nadal musi być możliwy dostęp do usług publicznych i prywatnych za pomocą innych istniejących środków identyfikacji i uwierzytelniania. 16. Ramy techniczne europejskiego portfela tożsamości cyfrowej: a) nie mogą zezwalać dostawcom elektronicznych poświadczeń atrybutów lub jakiejkolwiek innej stronie, po wydaniu poświadczenia atrybutów, na uzyskanie danych umożliwiających śledzenie, przyporządkowanie lub skorelowanie transakcji lub zachowań użytkowników, lub uzyskanie w inny sposób wiedzy na temat transakcji lub zachowań				

	użytkowników, chyba że użytkownik wyraźnie wyrazi na to zgodę; b) muszą umożliwiać stosowanie technik ochrony prywatności, które – w przypadku gdy poświadczenie atrybutów nie wymaga identyfikacji użytkownika – zapewniają uniemożliwienie powiązania tożsamości użytkownika z tym poświadczeniem.				
Art. 5a ust. 17	17. Wszelkie przetwarzanie danych osobowych przez państwa członkowskie lub w ich imieniu przez podmioty lub strony odpowiedzialne za dostarczenie europejskich portfeli tożsamości cyfrowej jako środka identyfikacji elektronicznej musi odbywać się zgodnie z odpowiednimi i skutecznymi środkami ochrony danych. Zgodność takiego przetwarzania z rozporządzeniem (UE) 2016/679 musi zostać wykazana. Państwa członkowskie mogą wprowadzić przepisy krajowe w celu doprecyzowania stosowania takich środków.	TAK	Art. 1 pkt 10 lit. c (Art. 21a ust. 6a ustawy o usługach zaufania oraz identyfikacji elektronicznej)	6a. Minister właściwy do spraw informatyzacji przetwarza dane osobowe osób, którym wydano środki identyfikacji elektronicznej, obejmujące: 1) dane identyfikujące osobę, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, z późn. zm.), zwanego dalej „rozporządzeniem 2015/1501”, 2) dane identyfikujące osobę, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28	Z uwagi na to, że wydawany przez ministra właściwego do spraw informatyzacji europejski portfel tożsamości cyfrowej w zakresie w jakim jest środkiem identyfikacji elektronicznej będzie przyłączony do węzła krajowego doprecyzowano zakres danych przetwarzanych na tym węźle.

				listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. Urz. UE L 2024/2977 z 04.12.2024), zwanego dalej „rozporządzeniem 2024/2977”, 3) imiona rodziców osoby, której dotyczą dane, o których mowa w pkt 1 i 2, oraz rodzaj, serię i numer dokumentu potwierdzającego tożsamość tej osoby, 4) identyfikator profilu zaufanego osoby fizycznej powiązanego z profilem zaufanym, o którym mowa w art. 20ad ust. 1b ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne – w celu uwierzytelnienia z wykorzystaniem węzła krajowego.	
Art. 5a ust. 18	18. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji informacje dotyczące: a) podmiotu odpowiedzialnego za sporządzenie i prowadzenie wykazu zarejestrowanych stron ufających, które polegają na europejskich portfelach	TAK	Art. 1 pkt 14 (Art. 23 pkt 5 ustawy o usługach zaufania oraz	Minister właściwy do spraw informatyzacji: (…) 5) przekazuje Komisji Europejskiej informacje, o których mowa w art.	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2025 r. poz. 1275 i 1846 oraz

	tożsamości cyfrowej zgodnie z art. 5b ust. 5, oraz informacje o miejscu dostępności tego wykazu; b) podmiotów odpowiedzialnych za dostarczenie europejskich portfeli tożsamości cyfrowej zgodnie z art. 5a ust. 1; c) podmiotów odpowiedzialnych za zapewnienie powiązania danych identyfikujących osobę z europejskim portfelem tożsamości cyfrowej zgodnie z art. 5a ust. 5 lit. f); d) mechanizmu umożliwiającego walidację danych identyfikujących osobę, o których mowa w art. 5a ust. 5 lit. f), oraz walidację tożsamości stron ufających; e) mechanizmu walidacji autentyczności i ważności europejskich portfeli tożsamości cyfrowej.		identyfikacji elektronicznej)	5a ust. 18 rozporządzenia 910/2014;	z 2026 r. poz. 160) obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 5a ust. 19-24	19. Bez uszczerbku dla ust. 22 niniejszego artykułu, art. 11 stosuje się odpowiednio do europejskiego portfela tożsamości cyfrowej. 20. Art. 24 ust. 2 lit. b) oraz lit. d) – h) stosuje się odpowiednio do dostawców europejskich portfeli tożsamości cyfrowej. 21. Europejskie portfele tożsamości cyfrowej udostępnia się do użytku osobom z niepełnosprawnościami na równi z innymi użytkownikami zgodnie z dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/882 (*). 22. Do celów zapewniania europejskich portfeli tożsamości cyfrowej, europejskie portfele tożsamości cyfrowej i systemy identyfikacji elektronicznej, w ramach których są one	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	zapewniane, nie podlegają wymogom określonym w art. 7, 9, 10, 12 i 12a. 23. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 4, 5, 8 i 18 niniejszego artykułu, dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 24. Komisja, w drodze aktów wykonawczych, sporządza wykaz norm referencyjnych oraz, w razie potrzeby, ustanawia specyfikacje i procedury w celu ułatwienia rejestracji użytkowników w europejskim portfelu tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych z wysokim poziomem bezpieczeństwa albo środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa, w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełniają wymogi dotyczące wysokiego poziomu bezpieczeństwa. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 5b ust. 1	**Strony ufające europejskich portfeli tożsamości cyfrowej** 1. W przypadku gdy strona ufająca zamierza polegać na europejskich portfelach tożsamości cyfrowej na potrzeby świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji, strona ufająca rejestruje się w państwie członkowskim, w którym ma siedzibę.	TAK	Art. 1 pkt 13 (Art. 22b ust. 1 i 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22b. 1. Minister właściwy do spraw informatyzacji prowadzi, przy użyciu systemu teleinformatycznego, rejestr stron ufających europejskiemu portfelowi tożsamości cyfrowej, o którym mowa w art. 3 ust. 1 rozporządzenia 2025/848, zwany	Rejestr stron ufających europejskiemu portfelowi tożsamości cyfrowej jest elementem niezbędnym dla funkcjonowania wszelkich europejskich portfeli tożsamości

				dalej „rejestrem stron ufających” oraz zapewnia utrzymanie i rozwój tego rejestru, w tym: 1) zapewnia ochronę przed nieuprawnionym dostępem do rejestru; 2) zapewnia integralność danych przetwarzanych w rejestrze; 3) zapewnia dostępność systemu teleinformatycznego, przy użyciu którego jest prowadzony rejestr; 4) przeciwdziała uszkodzeniom systemu teleinformatycznego, przy użyciu którego jest prowadzony rejestr; 5) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych; 6) określa zasady zgłaszania naruszenia ochrony danych osobowych; 7) zapewnia rozliczalność działań dokonywanych na danych w rejestrze; 8) zapewnia poprawność danych przetwarzanych w rejestrze. 2. Do rejestru wpisuje się strony ufające europejskiemu portfelowi tożsamości cyfrowej mające siedzibę w Polsce.	cyfrowej w Polsce (w tym wydawanych w innych państwach UE i portfela zapewnianego przez ministra właściwego do spraw informatyzacji). Mając na uwadze, że rejestr musi zapewniać dane niezbędne do potwierdzania tożsamości stron ufających (dostawców usług polegających na portfelu), zasadne jest, aby poprawne skoordynowanie europejskiego portfela tożsamości cyfrowej i rejestru było zapewniane przez ten sam podmiot.

Art. 5b ust. 2 zdanie pierwsze	2. Proces rejestracji musi być efektywny kosztowo i proporcjonalny względem zagrożeń.	TAK	Art. 1 pkt 13 (Art. 22b ust. 3,4, 6, 7 i ust. 10 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	3. Wpis do rejestru stron ufających i zmiany we wpisie następują na wniosek złożony w postaci elektronicznej do ministra właściwego do spraw informatyzacji: 1) z wykorzystaniem formularza elektronicznego udostępnionego przez ministra właściwego do spraw informatyzacji, po uwierzytelnieniu strony ufającej europejskiemu portfelowi tożsamości cyfrowej za pomocą: a) w przypadku osób fizycznych za pomocą: – środka identyfikacji elektronicznej osoby fizycznej zapewniającego wysoki poziom bezpieczeństwa, – danych weryfikowanych za pomocą kwalifikowanego podpisu elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online umożliwiającej wpis do rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej, b) w przypadku osób prawnych za pomocą: – środka identyfikacji elektronicznej osoby prawnej zapewniającego wysoki poziom bezpieczeństwa lub	Wskazane przepisy ustawy wychodzą naprzeciw wymaganiom efektywności. Zapewni to możliwość składania wniosków drogą elektroniczną bezpośrednio, jak i za pośrednictwem kwalifikowanych dostawców usług zaufania, którzy na podstawie wpisów do rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej będą wydawać tak zwane certyfikaty dostępu i certyfikaty rejestracji strony ufającej portfela. Możliwość korzystania z pośrednictwa pozwoli stronom ufającym na załatwienie wpisu i uzyskanie niezbędnych certyfikatów w jednym miejscu. Możliwość pozyskania danych dotyczących wpisywanego podmiotu do formularza dodatkowo ułatwi rejestrację. Ponadto zakłada się, że wpis do

				– zaawansowanej pieczęci elektronicznej weryfikowanej kwalifikowanym certyfikatem; 2) za pośrednictwem kwalifikowanego dostawcy usług zaufania świadczącego usługę wydawania certyfikatów dostępu strony ufającej portfelowi lub certyfikatów rejestracji strony ufającej portfelowi. 4. Wniosek, o którym mowa w ust. 3 pkt 2, opatruje się kwalifikowanym podpisem elektronicznym osoby fizycznej albo kwalifikowanym podpisem elektronicznym osoby fizycznej upoważnionej do reprezentowania osoby prawnej, w której imieniu ten wniosek jest składany, oraz zaawansowaną pieczęcią weryfikowaną kwalifikowanym certyfikatem kwalifikowanego dostawcy usług zaufania, za pośrednictwem którego jest składany. Przed opatrzeniem wniosku pieczęcią elektroniczną kwalifikowany dostawca usług zaufania weryfikuje uprawnienia osoby fizycznej do reprezentowania osoby prawnej w sposób zgodny z krajową polityką, o której mowa w ust. 15 pkt 2. (…)	rejestru będzie mógł nastąpić automatycznie w przypadku kompletności wniosku, co dodatkowo podniesie efektywność. Jednocześnie wymaga się celem uniknięcia zagrożeń potwierdzenia tożsamości osób fizycznych, osób fizycznych reprezentujących osoby prawne i osób prawnych odpowiednio bezpiecznych środków identyfikacji elektronicznej, pieczęci elektronicznych lub kwalifikowanych podpisów elektronicznych.

				6. Formularz elektroniczny, o którym mowa w ust. 3 pkt 1, umożliwia, po uwierzytelnieniu strony ufającej europejskiemu portfelowi tożsamości cyfrowej, pobranie danych z rejestrów, o których mowa w ust. 7, w celu wstępnego automatycznego uzupełnienia wniosku. 7. Minister właściwy do spraw informatyzacji weryfikuje zgodność danych zawartych we wniosku z danymi wpisanymi: 1) do Centralnej Ewidencji i Informacji o Działalności Gospodarczej; 2) do Krajowego Rejestru Sądowego; 3) do Katalogu Podmiotów Publicznych; 4) na zaufaną listę, o której mowa w art. 2 pkt 2; 5) do rejestru PESEL - w przypadku, gdy wniosek o wpis składa osoba fizyczna nieprowadząca działalności gospodarczej. (…) 10. Wpis do rejestru stanowi czynność materialno-techniczną i następuje po zweryfikowaniu	

				kompletności danych zawartych we wniosku zgodnie z ust. 7-9, o czym strona ufająca jest powiadamiana na niezwłocznie adres poczty elektronicznej, o którym mowa w pkt 7 lit. c załącznika I do rozporządzenia 2025/848.	
Art. 5b ust. 2 zdanie drugie, ust. 3-4 i ust. 6	Strona ufająca przekazuje co najmniej: a) informacje niezbędne do uwierzytelnienia w europejskich portfelach tożsamości cyfrowej, które obejmują co najmniej: (i) państwo członkowskie, w którym strona ufająca ma siedzibę; oraz (ii) nazwę strony ufającej oraz, w stosownych przypadkach, jej numer rejestrowy podany zgodnie z oficjalnym rejestrem wraz z danymi identyfikacyjnymi zawartymi w tym oficjalnym rejestrze; b) dane kontaktowe strony ufającej; c) zamierzone używanie europejskich portfeli tożsamości cyfrowej, w tym wskazanie danych, o które strona ufająca będzie zwracać się do użytkowników. 3. Strony ufające nie mogą zwracać się do użytkowników o udostępnienie jakichkolwiek danych innych niż te, które zostały wskazane zgodnie z ust. 2 lit. c). 4. Ust. 1 i 2 pozostają bez uszczerbku dla prawa Unii lub prawa krajowego mającego zastosowanie do świadczenia określonych usług.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	(…..) 6. Strony ufające zarejestrowane zgodnie z niniejszym artykułem niezwłocznie informują państwa członkowskie o wszelkich zmianach w informacjach przekazanych w ramach rejestracji zgodnie z ust. 2.				
Art. 5b ust. 5 i ust. 7	5. Państwa członkowskie udostępniają publicznie informacje, o których mowa w ust. 2, online, w postaci pozwalającej na automatyczne przetwarzanie, elektronicznie podpisane lub opatrzone pieczęcią elektroniczną. 7. Państwa członkowskie zapewniają wspólny mechanizm umożliwiający identyfikację i uwierzytelnianie stron ufających, o którym mowa w art. 5a ust. 5 lit. c).	TAK	Art. 1 pkt 14 (Art. 23 pkt. 6 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 6) udostępnia publicznie informacje, o których mowa w art. 5b ust. 2 rozporządzenia 910/2014, w postaci elektronicznej i umożliwiającej ich automatyczne przetwarzanie, elektroniczne podpisanie lub opatrzenie pieczęcią elektroniczną, oraz zapewnia mechanizm umożliwiający identyfikację i uwierzytelnianie strony ufającej europejskiemu portfelowi tożsamości cyfrowej, o którym mowa w art. 5b ust. 7 rozporządzenia 910/2014;	Skoro minister właściwy do spraw informatyzacji zapewni rejestr stron ufających europejskiemu portfelowi tożsamości cyfrowej, to powinien zapewnić również spełnienie wskazanych wymagań.
Art. 5b ust. 8-11	8. W przypadku gdy strony ufające zamierzają polegać na europejskich portfelach tożsamości cyfrowej, muszą potwierdzić swoją tożsamość wobec użytkownika. 9. Strony ufające odpowiedzialne są za przeprowadzenie procedury uwierzytelniania i walidacji danych identyfikujących osobę oraz elektronicznego poświadczenia atrybutów żądanych z europejskich portfeli tożsamości cyfrowej. Strony	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	ufające nie mogą odmówić używania pseudonimów, w przypadkach gdy identyfikacja użytkownika nie jest wymagana na podstawie prawa Unii lub prawa krajowego. 10. Pośrednicy działający w imieniu stron ufających uznawani są za strony ufające i nie mogą przechowywać danych na temat treści transakcji. 11. Do dnia 21 listopada 2024 r. Komisja ustanowi specyfikacje techniczne i procedury w odniesieniu do wymogów, o których mowa w ust. 2, 5 i 6–9 niniejszego artykułu, w drodze aktów wykonawczych dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5a ust. 23. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 5c ust. 1 i ust. 7 zdanie pierwsze	**Certyfikacja europejskich portfeli tożsamości cyfrowej** 1. Zgodność europejskich portfeli tożsamości cyfrowej i systemu identyfikacji elektronicznej, w ramach którego są one zapewniane, z wymogami określonymi w art. 5a ust. 4, 5 i 8, z wymogiem dotyczącym logicznego oddzielenia określonym w art. 5a ust. 14 oraz, w stosownych przypadkach, z normami i specyfikacjami technicznymi, o których mowa w art. 5a ust. 24, musi być certyfikowana przez jednostki oceniające zgodność wyznaczone przez państwa członkowskie. (…) 7. Państwa członkowskie przekazują Komisji nazwy i adresy jednostek oceniających zgodność, o których mowa w ust. 1.	TAK	Art. 1 pkt 14 (Art. 23 pkt 7 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 7) wyznacza właściwe jednostki oceniające zgodność europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5c ust. 1 rozporządzenia 910/2014, oraz przekazuje Komisji Europejskiej ich nazwy i adresy , zgodnie z art. 5c ust. 7 rozporządzenia 910/2014;	Obecnie minister właściwy do spraw informatyzacji pełni rolę organu nadzoru nad dostawcami usług zaufania oraz nad krajowym schematem identyfikacji elektronicznej i zgodnie z nowym art. 22j pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej ma pełnić również rolę organu nadzoru nad ramami dla europejskiego

					portfela tożsamości cyfrowej. W związku z tym doświadczeniem zasadne jest, aby to również ten organ wyznaczał jednostki oceniające zgodność.
Art. 5c ust. 2-8	2. Certyfikację zgodności europejskich portfeli tożsamości cyfrowej lub ich części z wymogami, o których mowa w ust. 1 niniejszego artykułu, które są związane z cyberbezpieczeństwem, przeprowadza się zgodnie z europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 (**) oraz wymienionymi w aktach wykonawczych, o których mowa w ust. 6 niniejszego artykułu. 3. W odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu, które nie są związane z cyberbezpieczeństwem, oraz w odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu, które są związane z cyberbezpieczeństwem, w zakresie, w jakim programy certyfikacji cyberbezpieczeństwa, o których mowa w ust. 2 niniejszego artykułu, nie obejmują tych wymogów dotyczących cyberbezpieczeństwa lub obejmują je tylko częściowo, również w odniesieniu do tych wymogów, państwa członkowskie ustanawiają krajowe programy certyfikacji zgodnie z wymogami określonymi w aktach wykonawczych, o których mowa w ust. 6 niniejszego artykułu. Państwa członkowskie przekazują swoje projekty krajowych programów certyfikacji Grupie Współpracy na rzecz	TAK	Art. 1 pkt 13 i pkt 14 (Art. 22j oraz art. 23 pkt 7 i 8 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22j. 1. Minister właściwy do spraw informatyzacji: 1) opracowuje, utrzymuje i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej krajowy program certyfikacji, o którym mowa art. 3 rozporządzenia wykonawczego Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej, , (Dz. Urz. UE L 2024/2981 z 04.12.2024), zwanego dalej „rozporządzeniem 2024/2981”, w szczególności sporządza i utrzymuje program certyfikacji europejskiego portfela tożsamości cyfrowej, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel; 2) wyznacza jednostką certyfikującą, o której mowa w art. 2 pkt 9 rozporządzenia 2024/2981;	Wskazanie rozwiązań zapewniających certyfikację europejskiego portfela tożsamości cyfrowej.

	Europejskiej Tożsamości Cyfrowej ustanowionej na podstawie art. 46e ust. 1 (zwanej dalej »grupą współpracy«). Grupa współpracy może wydawać opinie i zalecenia. 4. Certyfikacja zgodna z ust. 1 ważna jest przez okres do pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostanie stwierdzona podatność na zagrożenia i nie zostanie ona terminowo wyeliminowana, certyfikacja zostaje odwołana. 5. Spełnienie wymogów określonych w art. 5a niniejszego rozporządzenia związanych z operacjami przetwarzania danych osobowych może zostać certyfikowane na podstawie rozporządzenia (UE) 2016/679. 6. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów certyfikacji europejskich portfeli tożsamości cyfrowej, o której mowa w ust. 1, 2 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 7. Państwa członkowskie przekazują Komisji nazwy i adresy jednostek oceniających zgodność, o których mowa w ust. 1. Komisja udostępnia te informacje wszystkim państwom członkowskim. 8. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, ustanawiających szczególne kryteria, które mają spełniać wyznaczone jednostki oceniające zgodność, o których mowa w ust. 1 niniejszego artykułu.			3) jest organem nadzoru, o którym mowa w art. 46a ust. 1 rozporządzenia 910/2014, oraz przekazuje Komisji Europejskiej odpowiednie informacje w tym zakresie. 2. Polskie Centrum Akredytacji udziela akredytacji jednostce oceniającej zgodność, o której mowa w art. 3 pkt 18 rozporządzenia 910/2014. 3. Do akredytacji jednostki oceniającej zgodność stosuje się odpowiednio przepisy rozdziału 4 ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2025 r. poz. 568). 4. Polskie Centrum Akredytacji uzgadnia z ministrem właściwym do spraw informatyzacji program akredytacji określający zasady i procesy akredytacji jednostek oceniających zgodność. 5. Minister właściwy do spraw informatyzacji i Polskie Centrum Akredytacji mogą zawrzeć porozumienie o współpracy w zakresie monitorowania działalności jednostek oceniających zgodność oraz o wzajemnym przekazywaniu informacji dotyczących tych jednostek.	

				Art. 23. Minister właściwy do spraw informatyzacji: (…..) 7) wyznacza właściwe jednostki oceniające zgodność europejskich portfeli tożsamości cyfrowej, o których mowa w art. 5c ust. 1 rozporządzenia 910/2014, oraz przekazuje Komisji Europejskiej ich nazwy i adresy , zgodnie z art. 5c ust. 7 rozporządzenia 910/2014; 8) przekazuje projekt krajowego programu certyfikacji, o którym mowa w art. 22j ust. pkt 1, Grupie Współpracy na rzecz Europejskiej Tożsamości Cyfrowej, o której mowa w art. 46e ust. 1 rozporządzenia 910/2014, zwanej dalej „grupą współpracy”;	
Art. 5d ust. 1	**Publikacja wykazu certyfikowanych europejskich portfeli tożsamości cyfrowej** 1. Państwa członkowskie bez zbędnej zwłoki informują Komisję oraz grupę współpracy ustanowioną na podstawie art. 46e ust. 1 o europejskich portfelach tożsamości cyfrowej, które zostały zapewnione zgodnie z art. 5a i certyfikowane przez jednostki oceniające zgodność, o których mowa w art. 5c ust. 1. Państwa członkowskie informują Komisję oraz grupę współpracy ustanowioną na podstawie art. 46e ust.	TAK	Art. 1 pkt 14 (Art. 23 pkt 9 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (….) 9) informuje Komisję Europejską oraz grupę współpracy o wszelkich zmianach związanych z europejskimi portfelami tożsamości cyfrowej, o których mowa a art. 5d ust. 1 rozporządzenia 910/2014;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i

	1 bez zbędnej zwłoki o odwołaniu certyfikacji oraz podają przyczyny odwołania.				telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 5d ust. 2-7	2. Bez uszczerbku dla art. 5a ust. 18 informacje przekazywane przez państwa członkowskie zgodnie z ust. 1 niniejszego artykułu obejmują co najmniej: a) certyfikat i sprawozdanie z oceny certyfikacji certyfikowanego europejskiego portfela tożsamości cyfrowej; b) opis systemu identyfikacji elektronicznej, w ramach którego zapewniany jest europejski portfel tożsamości cyfrowej; c) mający zastosowanie system nadzoru oraz informacje na temat systemu odpowiedzialności w odniesieniu do strony dostarczającej europejski portfel tożsamości cyfrowej; d) organ lub organy odpowiedzialne za system identyfikacji elektronicznej; e) ustalenia dotyczące zawieszania lub unieważniania systemu identyfikacji elektronicznej lub uwierzytelnienia lub ich skompromitowanych części. 3. Na podstawie informacji otrzymanych zgodnie z ust. 1 Komisja ustanawia, publikuje w *Dzienniku Urzędowym Unii Europejskiej* oraz prowadzi w formie nadającej się do odczytu maszynowego	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	wykaz certyfikowanych europejskich portfeli tożsamości cyfrowej. 4. Państwo członkowskie może przedłożyć Komisji wniosek o usunięcie z wykazu, o którym mowa w ust. 3, europejskiego portfela tożsamości cyfrowej i systemu identyfikacji elektronicznej, w ramach którego portfel ten jest zapewniany. 5. W przypadku zmian w informacjach przekazanych zgodnie z ust. 1 państwo członkowskie przekazuje Komisji zaktualizowane informacje. 6. Komisja aktualizuje wykaz, o którym mowa w ust. 3, publikując w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie w terminie miesiąca od otrzymania wniosku zgodnie z ust. 4 lub zaktualizowanych informacji zgodnie z ust. 5. 7. Do dnia 21 listopada 2024 r. Komisja ustanowi formaty i procedury mające zastosowanie do celów ust. 1, 4 i 5 niniejszego artykułu, w drodze aktów wykonawczych dotyczących wdrożenia europejskich portfeli tożsamości cyfrowej, o którym mowa w art. 5a ust. 23. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 5e ust. 1-3	**Naruszenie bezpieczeństwa europejskich portfeli tożsamości cyfrowej** 1. W przypadku naruszenia lub częściowej kompromitacji europejskich portfeli tożsamości cyfrowej zapewnianych zgodnie z art. 5a, mechanizmów walidacji, o których mowa w art. 5a ust. 8, lub systemu identyfikacji elektronicznej, w	TAK	Art. 1 pkt 14 (Art. 23 pkt 17 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23 Minister właściwy do spraw informatyzacji: (…)	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych

	ramach którego te europejskie portfele tożsamości cyfrowej są zapewniane, w sposób, który wpływa na ich wiarygodność lub na wiarygodność innych europejskich portfeli tożsamości cyfrowej, państwo członkowskie, które zapewniło dane europejskie portfele tożsamości cyfrowej, bez zbędnej zwłoki zawiesza zapewnianie i używanie europejskich portfeli tożsamości cyfrowej. W przypadku gdy jest to uzasadnione wagą naruszenia bezpieczeństwa lub kompromitacji, o których mowa w akapicie pierwszym, państwo członkowskie bez zbędnej zwłoki wycofuje europejskie portfele tożsamości cyfrowej. Państwo członkowskie informuje użytkowników, których to dotyczy, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1, strony ufające oraz Komisję. 2. Jeżeli naruszenie bezpieczeństwa lub kompromitacja, o których mowa w ust. 1 akapit pierwszy niniejszego artykułu, nie zostaną wyeliminowane w terminie trzech miesięcy od zawieszenia, państwo członkowskie, które zapewniło europejskie portfele tożsamości cyfrowej, wycofuje europejskie portfele tożsamości cyfrowej i je unieważnia. Państwo członkowskie informuje o tym wycofaniu użytkowników, których to dotyczy, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1, strony ufające oraz Komisję. 3. W przypadku gdy naruszenie bezpieczeństwa lub kompromitacja, o których mowa w akapicie pierwszym niniejszego artykułu, zostaną wyeliminowane, zapewniające państwo			17) wykonuje zadania, o których mowa w art. 5e ust. 1-3 rozporządzenia 910/2014.	Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.

	członkowskie przywraca zapewnianie i używanie europejskich portfeli tożsamości cyfrowej oraz informuje o tym bez zbędnej zwłoki użytkowników, których to dotyczy, strony ufające, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1 oraz Komisję.				
Art. 5e ust. 4-5	4. Komisja bez zbędnej zwłoki publikuje w *Dzienniku Urzędowym Unii Europejskiej* odpowiednie zmiany w wykazie, o którym mowa w art. 5d. 5. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów środków, o których mowa w ust. 1, 2 i 3 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 5f	**Transgraniczne poleganie na europejskich portfelach tożsamości cyfrowej** 1. W przypadku gdy państwa członkowskie wymagają identyfikacji elektronicznej oraz uwierzytelnienia w celu dostępu do usługi online świadczonej przez podmiot sektora publicznego, akceptują również europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem. 2. W przypadku gdy prywatne strony ufające, które świadczą usługi – z wyjątkiem mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE (***)– zobowiązane są na podstawie prawa Unii lub prawa	NIE/TAK	Art. 5. ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu	Art. 5. W ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644, 1669 oraz z 2026 r. poz. 875 i 1206) w art. 36 w ust. 1 w pkt 1 lit d. otrzymuje brzmienie: „d) serii i numeru dokumentu stwierdzającego tożsamość osoby lub niepowtarzalnego identyfikatora nadanego przez jedno z państw członkowskich Unii Europejskiej dla celów transgranicznej identyfikacji, o którym mowa w rozporządzeniu wykonawczym	Przepis stosowany wprost, poza ust. 2, w którym wymaga się uznawania europejskiego portfela tożsamości cyfrowej m.in. w obszarach bankowości i usługach finansowych. Z uwagi na to, że zestaw danych identyfikujących osobę, znajdujący się w europejskim portfelu tożsamości cyfrowej nie zawiera w sobie serii i

	krajowego do stosowania silnego uwierzytelnienia użytkownika do celów identyfikacji elektronicznej lub w przypadku gdy silne uwierzytelnienie użytkownika do celów identyfikacji elektronicznej wymagane jest na podstawie zobowiązania umownego, w tym w obszarach transportu, energii, bankowości, usług finansowych, zabezpieczenia społecznego, zdrowia, wody pitnej, usług pocztowych, infrastruktury cyfrowej, edukacji lub telekomunikacji, te prywatne strony ufające, nie później niż 36 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, oraz wyłącznie na dobrowolny wniosek użytkownika, również akceptują europejskie portfele tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem. 3. W przypadku gdy dostawcy bardzo dużych platform internetowych, o których mowa w art. 33 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 (****), wymagają uwierzytelniania użytkownika do celów dostępu do usług online, akceptują i ułatwiają oni również używanie europejskich portfeli tożsamości cyfrowej, które są zapewniane zgodnie z niniejszym rozporządzeniem, do celów uwierzytelnienia użytkownika, wyłącznie na dobrowolny wniosek użytkownika oraz w odniesieniu do minimalnych danych niezbędnych do celów konkretnej usługi online, która wymaga uwierzytelnienia użytkownika. 4. We współpracy z państwami członkowskimi Komisja ułatwia opracowywanie kodeksów postępowania, w ścisłej współpracy ze wszystkimi odpowiednimi zainteresowanymi stronami, w tym ze			Komisji (UE) 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235 z 09.09.2015, str. 1, z późn. zm.),, albo osobistego numeru identyfikacyjnego, o którym mowa w tabeli 2 załącznika do rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. Urz. UE L 2024/2977 z 04.12.2024), albo numeru dokumentu, o którym mowa w tabeli 5 załącznika do tego rozporządzenia,”.	numeru dokumentu stwierdzającego tożsamość, należało umożliwić weryfikowanie tożsamości również w oparciu o te dane.

	społeczeństwem obywatelskim, aby przyczynić się do szerokiej dostępności i użyteczności europejskich portfeli tożsamości cyfrowej objętych zakresem stosowania niniejszego rozporządzenia, oraz zachęcać dostawców usług do ukończenia opracowywania kodeksów postępowania. 5. W terminie 24 miesięcy po wprowadzeniu europejskich portfeli tożsamości cyfrowej Komisja dokonuje oceny popytu na europejskie portfele tożsamości cyfrowej oraz ich dostępności i użyteczność, biorąc pod uwagę kryteria takie jak rozpowszechnienie wśród użytkowników, transgraniczna obecność dostawców usług, rozwój technologiczny, zmiany sposobów użytkowania oraz popyt ze strony konsumentów.				
Przed art. 6	SEKCJA 2 SYSTEMY IDENTYFIKACJI ELEKTRONICZNEJ	NIE			Przepis stosowany wprost, nie wymaga wdrożenia
Art. 7 lit. g	g) co najmniej sześć miesięcy przed notyfikacją na podstawie art. 9 ust. 1 notyfikujące państwo członkowskie przekazuje pozostałym państwom członkowskim, do celów art. 12 ust. 5, opis tego systemu zgodnie z warunkami proceduralnymi ustanowionymi w aktach wykonawczych przyjętych zgodnie z art. 12 ust. 6;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia
Art. 8 ust. 3	3. Do dnia 18 września 2015 r., uwzględniając odpowiednie normy międzynarodowe oraz z zastrzeżeniem ust. 2, Komisja określi, w drodze aktów wykonawczych, minimalne techniczne specyfikacje, normy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki	NIE			Przepis stosowany wprost, nie wymaga wdrożenia

	poziom bezpieczeństwa dla środka identyfikacji elektronicznej.				
Art. 9 ust. 2 i 3	2. Komisja bez zbędnej zwłoki publikuje w Dzienniku Urzędowym Unii Europejskiej wykaz systemów identyfikacji elektronicznej, które zostały notyfikowane zgodnie z ust. 1, wraz z podstawowymi informacjami na temat tych systemów. 3. Komisja publikuje w Dzienniku Urzędowym Unii Europejskiej zmiany w wykazie, o którym mowa w ust. 2, w terminie miesiąca od dnia otrzymania notyfikacji.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia
Tytuł art. 10	Naruszenie bezpieczeństwa systemów identyfikacji elektronicznej	NIE			Przepis stosowany wprost, nie wymaga wdrożenia
Art. 11a ust. 1	**Transgraniczne dopasowywanie tożsamości** 1. Działając jako strony ufające w odniesieniu do usług transgranicznych, państwa członkowskie zapewniają jednoznaczne dopasowywanie tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej.	TAK	Art. 1 pkt 13 (Art. 22a ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej) Art. 9	Art. 22a. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie systemu scentralizowanego, o którym mowa w rozporządzeniu 2025/846umożliwiającego dopasowywanie tożsamości, o którym mowa w art. 11a rozporządzenia 910/2014. Art. 9. System teleinformatyczny podmiotu publicznego zapewnia możliwość dopasowywania tożsamości osób fizycznych z użyciem notyfikowanych środków identyfikacji elektronicznej lub europejskich portfeli tożsamości cyfrowej, o którym mowa w art. 11a	Minister właściwy do spraw informatyzacji zapewnia obecnie funkcjonowanie krajowego węzła identyfikacji elektronicznej oraz węzła transgranicznego umożliwiające uwierzytelnianie transgraniczne. Przepis przejściowy dający czas na dostosowanie usług publicznych do wymagań związanych z

				ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, z wykorzystaniem systemu scentralizowanego, o którym mowa w art. 22a ust. 1 pkt 2 lit. c ustawy zmienianej w art. 1, najpóźniej od dnia 31 grudnia 2028 r.	dopasowaniem tożsamości.
Art. 11a ust. 2 i 3	2. Państwa członkowskie określają środki techniczne i organizacyjne w celu zapewnienia wysokiego poziomu ochrony danych osobowych wykorzystywanych do dopasowywania tożsamości oraz w celu zapobiegania profilowaniu użytkowników. 3. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 12 tytuł	**Interoperacyjność**	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 12 ust. 3 lit. c	c) ułatwiają wdrożenie zasad prywatności i bezpieczeństwa na etapie projektowania;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 12 ust. 4 lit. d	d) odniesienie do minimalnego zbioru danych identyfikujących osobę niezbędnych do niepowtarzalnego reprezentowania osoby fizycznej lub prawnej, lub osoby fizycznej reprezentującej inną osobę fizyczną lub osobę prawną, które jest dostępne w ramach systemów identyfikacji elektronicznej;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 12 ust. 5	"5. Państwa członkowskie przeprowadzają wzajemne oceny systemów identyfikacji elektronicznej, które objęte są zakresem stosowania niniejszego rozporządzenia, i które mają być notyfikowane zgodnie z art. 9 ust. 1 lit. a).	TAK	Art. 1 pkt 16 lit. b (Art. 24 ust. 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	3. Minister właściwy do spraw informatyzacji może zgłosić system identyfikacji elektronicznej do przeprowadzenia wzajemnej oceny, o której mowa w art. 12 ust. 5 rozporządzenia 910/2014, oraz do notyfikacji, o której mowa w art. 9 rozporządzenia 910/2014, po pozytywnym zweryfikowaniu wniosku, o którym mowa w ust. 1, biorąc pod uwagę warunki kwalifikowania się systemu do notyfikowania wskazane w art. 7 tego rozporządzenia oraz politykę państwa w zakresie identyfikacji elektronicznej.	Minister jest już obecnie wyznaczony do realizacji tego zadania. Dotychczas wymóg przeprowadzenia wzajemnej oceny znajdował się w przepisach wykonawczych wydanych na podstawie art. 12 ust. 7. Obecnie wymóg wzajemnej oceny wynika wprost z art. 12 ust. 5. Zmieniono brzmienie przepisu dostosowując do ww. zmian w rozporządzeniu eIDAS.
Art. 12 ust 6-8	6. Do dnia 18 marca 2025 r. Komisja ustanowi, w drodze aktów wykonawczych, niezbędne warunki proceduralne wzajemnych ocen, o których mowa w ust. 5 niniejszego artykułu, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa,	NIE			Przepis stosowany wprost ,nie wymaga wdrożenia.

	stosownie do poziomu ryzyka. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. uchyla się ust. 7; 8. Do dnia 18 września 2025 r., w celu określenia jednolitych warunków wdrożenia wymogu, o którym mowa w ust. 1 niniejszego artykułu, z zastrzeżeniem kryteriów określonych w ust. 3 niniejszego artykułu oraz z uwzględnieniem rezultatów współpracy między państwami członkowskimi, Komisja przyjmie akty wykonawcze dotyczące ram interoperacyjności określonych w ust. 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 12a ust. 1	**Certyfikacja systemów identyfikacji elektronicznej** 1. Zgodność systemów identyfikacji elektronicznej, które mają być notyfikowane, z wymogami dotyczącymi cyberbezpieczeństwa określonymi w niniejszym rozporządzeniu, w tym zgodność z wymogami związanymi z cyberbezpieczeństwem określonymi w art. 8 ust. 2 dotyczącymi poziomów bezpieczeństwa systemów identyfikacji elektronicznej, certyfikują jednostki oceniające zgodność wyznaczone przez państwa członkowskie.	TAK	Art. 1 pkt 14 i 16 (Art. 23 pkt 10 i art. 24 ust. 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 10) wyznacza właściwe jednostki oceniające zgodność systemów identyfikacji elektronicznej, o których mowa w art. 12a ust. 1 rozporządzenia 910/2014 oraz przekazuje Komisji Europejskiej ich nazwy i adresy , zgodnie z art. 12a ust. 6 rozporządzenia 910/2014; w art. 24: a) w ust. 2 po wyrazach „rozporządzenia 910/2014”dodaje się wyrazy „oraz dokument potwierdzający certyfikację, o której	Obecnie minister właściwy do spraw informatyzacji pełni rolę organu nadzoru nad krajowym schematem identyfikacji elektronicznej. W związku z tym zasadne jest, aby to również ten organ wyznaczał jednostki oceniające zgodność.

				mowa w art. 12a ust. 1 tego rozporządzenia.”,	
Art. 12a ust. 2-3	2. Certyfikację zgodnie z ust. 1 niniejszego artykułu przeprowadza się w ramach odpowiedniego programu certyfikacji cyberbezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 lub jego części, w zakresie, w jakim certyfikat cyberbezpieczeństwa lub jego części obejmują te wymogi w zakresie cyberbezpieczeństwa. 3. Certyfikacja na podstawie ust. 1 jest ważna przez okres do pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostanie stwierdzona podatność na zagrożenia i nie zostanie ona wyeliminowana w terminie trzech miesięcy od takiego stwierdzenia, certyfikacja zostaje odwołana.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 12a ust. 4	4. Niezależnie od ust. 2 państwa członkowskie, zgodnie z tym ustępem, mogą zwrócić się do notyfikującego państwa członkowskiego o dodatkowe informacje na temat systemów identyfikacji elektronicznej lub ich części.	TAK	Art. 1 pkt 14 (Art. 23 pkt 11 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 11) uzyskuje dodatkowe informacje na temat systemów identyfikacji elektronicznej, o których mowa w art. 12a ust. 4 rozporządzenia 910/2014;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister

					właściwy do spraw informatyzacji.
Art. 12a ust. 5	5. Wzajemna ocena systemów identyfikacji elektronicznej, o której mowa w art. 12 ust. 5, nie ma zastosowania do systemów identyfikacji elektronicznej certyfikowanych zgodnie z ust. 1 niniejszego artykułu ani do części takich systemów. Państwa członkowskie mogą wykorzystać certyfikat lub deklarację zgodności, wydane zgodnie z odpowiednim programem certyfikacji lub częściami takich programów, z wymogami niezwiązanymi z cyberbezpieczeństwem określonymi w art. 8 ust. 2 w zakresie poziomu bezpieczeństwa systemów identyfikacji elektronicznej.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 12a ust. 6	6 . Państwa członkowskie przekazują Komisji nazwy i adresy jednostek oceniających zgodność, o których mowa w ust. 1. Komisja udostępnia te informacje wszystkim państwom członkowskim.	TAK	Art. 1 pkt 14 (Art. 23 pkt 10 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 10) wyznacza właściwe jednostki oceniające zgodność systemów identyfikacji elektronicznej, o których mowa w art. 12a ust. 1 rozporządzenia 910/2014 oraz przekazuje Komisji Europejskiej ich nazwy i adresy , zgodnie z art. 12a ust. 6 rozporządzenia 910/2014;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.

Art. 12b	**Dostęp do funkcji sprzętu i oprogramowania** W przypadku gdy dostawcy europejskich portfeli tożsamości cyfrowej i wydawcy notyfikowanych środków identyfikacji elektronicznej działający w celach handlowych lub zawodowych oraz korzystający z podstawowych usług platformowych zdefiniowanych w art. 2 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/1925 (*) do celów świadczenia użytkownikom końcowym usług europejskiego portfela tożsamości cyfrowej i środków identyfikacji elektronicznej lub w trakcie świadczenia takich usług i środków są użytkownikami biznesowymi zgodnie z definicją w art. 2 pkt 21 tego rozporządzenia, strażnicy dostępu umożliwiają im w szczególności skuteczną interoperacyjność z tym samym systemem operacyjnym oraz funkcjami sprzętu lub oprogramowania oraz dostęp do tego systemu operacyjnego i tych funkcji na potrzeby interoperacyjności. Taką skuteczną interoperacyjność i dostęp zapewnia się nieodpłatnie oraz niezależnie od tego, czy funkcje sprzętu lub oprogramowania stanowią część systemu operacyjnego, są dostępne dla tego strażnika dostępu lub wykorzystywane przez niego podczas świadczenia takich usług w rozumieniu art. 6 ust. 7 rozporządzenia (UE) 2022/1925. Niniejszy artykuł pozostaje bez uszczerbku dla art. 5a ust. 14 niniejszego rozporządzenia.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 13 ust. 1	1. Niezależnie od ust. 2 niniejszego artykułu oraz bez uszczerbku dla rozporządzenia (UE) 2016/679, dostawcy usług zaufania są odpowiedzialni za szkody wyrządzone w sposób zamierzony lub w wyniku niedbalstwa osobie fizycznej lub prawnej z	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	powodu nieprzestrzegania obowiązków określonych w niniejszym rozporządzeniu. Każda osoba fizyczna lub prawna, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia przez dostawcę usług zaufania, ma prawo dochodzić odszkodowania zgodnie z prawem Unii i krajowym. Ciężar dowiedzenia zamiaru lub niedbalstwa po stronie niekwalifikowanego dostawcy usług zaufania spoczywa na osobie fizycznej lub prawnej zgłaszającej szkodę, o której mowa w akapicie pierwszym. Domniemywa się zamiar lub niedbalstwo kwalifikowanego dostawcy usług zaufania, chyba że kwalifikowany dostawca usług zaufania udowodni, że szkoda, o której mowa w akapicie pierwszym, nie nastąpiła w wyniku zamiaru lub niedbalstwa.				
Art. 14	**Aspekty międzynarodowe** Art. 14.1. Usługi zaufania świadczone przez dostawców usług zaufania mających siedzibę w państwie trzecim lub przez organizację międzynarodową uznaje się za prawnie równoważne kwalifikowanym usługom zaufania świadczonym przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii, w przypadku gdy usługi zaufania pochodzące z państwa trzeciego lub organizacji międzynarodowej są uznawane w drodze aktów wykonawczych lub umowy zawartej między Unią a danym państwem trzecim lub organizacją międzynarodową zgodnie z art. 218 TFUE.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	Akty wykonawcze, o których mowa w akapicie pierwszym, przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 2. Akty wykonawcze i umowa, o których mowa w ust. 1, zapewniają, aby wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania mających siedzibę w Unii oraz do świadczonych przez nich kwalifikowanych usług zaufania były spełniane przez dostawców usług zaufania w danym państwie trzecim lub przez organizację międzynarodową oraz przez świadczone przez nich usługi zaufania. Państwa trzecie i organizacje międzynarodowe w szczególności ustanawiają, prowadzą i publikują zaufaną listę uznawanych dostawców usług zaufania. 3. Umowa, o której mowa w ust. 1, zapewnia, aby kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania mających siedzibę w Unii były uznawane za prawnie równoważne usługom zaufania świadczonym przez dostawców usług zaufania w danym państwie trzecim lub przez organizację międzynarodową, z którymi zawarta została dana umowa.				
Art. 15	Art. 15. **Dostępność dla osób z niepełnosprawnościami i osób o specjalnych potrzebach** Zapewniane środki identyfikacji elektronicznej, usługi zaufania oraz produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług udostępnia się w prostym i zrozumiałym języku, zgodnie z Konwencją Narodów	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	Zjednoczonych o prawach osób niepełnosprawnych oraz zgodnie z wymogami dostępności określonymi dyrektywie (UE) 2019/882, przynosząc w ten sposób korzyści również osobom z ograniczeniami funkcjonalnymi, takim jak osoby starsze, oraz osobom z ograniczonym dostępem do technologii cyfrowych.				
Art. 16 ust. 1-2	**Kary** 1. Bez uszczerbku dla art. 31 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 * państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia. Kary te muszą być skuteczne, proporcjonalne i odstraszające. 2. Państwa członkowskie zapewniają, aby naruszenia niniejszego rozporządzenia przez kwalifikowanych i niekwalifikowanych dostawców usług zaufania podlegały administracyjnej karze pieniężnej w maksymalnej wysokości co najmniej: a) 5 000 000 EUR - w przypadku gdy dostawca usług zaufania jest osobą fizyczną; lub b) w przypadku gdy dostawca usług zaufania jest osobą prawną - 5 000 000 EUR lub 1 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należał dostawca usług zaufania, w roku obrotowym poprzedzającym rok, w którym miało miejsce naruszenie, w zależności od tego, która z tych wartości jest wyższa.	TAK	Art. 1 pkt 19-22 (Art. 46, 46a, 47 i 48 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	**Art. 1.** W ustawie 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) wprowadza się następujące zmiany: (…) 19) w art. 46 uchyla się pkt 1; 20) po art. 46 dodaje się art. 46a w brzmieniu: „Art. 46a. Kwalifikowany lub niekwalifikowany dostawca usług zaufania, który narusza przepisy rozporządzenia 910/2014, podlega karze pieniężnej.”; 21) w art. 47: a) ust. 1 otrzymuje brzmienie: „1. Kary pieniężne, o których mowa w art. 46, art. 46a, art. 47a i art. 47b, nakłada, w drodze decyzji, minister właściwy do spraw informatyzacji.”,	Niezbędne jest dostosowanie przepisów dotyczących kar.

				b) po ust. 1 dodaje się ust. 1a – 1b w brzmieniu: „1a. Wysokość kary pieniężnej, o której mowa w art. 46a wynosi nie więcej niż: 1) w przypadku, gdy dostawca usług zaufania jest osobą fizyczną – równowartość w złotych nie przekraczającą 5 000 000 euro, lub 2) w przypadku, gdy dostawca usług zaufania jest osobą prawną – równowartość w złotych nie przekraczającą 5 000 000 euro lub 1 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należał dostawca usług zaufania, w roku obrotowym poprzedzającym rok, w którym miało miejsce naruszenie, w zależności od tego, która z tych wartości jest wyższa. 1b. Przeliczenia kwot wyrażonych w ustawie w euro dokonuje się według średniego kursu waluty ogłoszonego przez Narodowy Bank Polski obowiązującego w dniu wydania decyzji o nałożeniu kary pieniężnej.”, c) w ust. 2 pkt 1 otrzymuje brzmienie: „1) pkt 2-9 i 12, wynosi do 50 000 zł;”;	

				22) art. 48 otrzymuje brzmienie: „Art. 48. Przy ustalaniu wysokości kary pieniężnej, o której mowa w art. 46 i art. 46a, minister właściwy do spraw informatyzacji uwzględnia zakres, czas trwania i skutki naruszenia wymagań, o których mowa w przepisach o usługach zaufania.”.	
Art. 16 ust. 3	3. W zależności od systemu prawnego państw członkowskich przepisy dotyczące administracyjnych kar pieniężnych można stosować w taki sposób, że o zastosowanie kary pieniężnej wnosi właściwy organ nadzorczy, a nakładają ją właściwe sądy krajowe. Zastosowanie takich przepisów w tych państwach członkowskich musi zapewniać, aby te środki prawne były skuteczne i miały skutek administracyjny równoważny karom pieniężnym nakładanym bezpośrednio przez organy nadzorcze.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Rozdział III tytuł sekcji 2	w rozdziale III tytuł sekcji 2 otrzymuje brzmienie: „Niekwalifikowani dostawcy usług zaufania”.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia
Art. 17 i art. 18	uchyla się art. 17 i 18;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 19a	**Wymogi dla niekwalifikowanych dostawców usług zaufania** 1. Niekwalifikowany dostawca usług zaufania świadczący niekwalifikowane usługi zaufania:	TAK	Art. 1 pkt 4 lit. b oraz pkt 5 (Art. 4 ust. 4 oraz art. 6 ust. 1 pkt 2, ust. 3,	b) ust. 4 otrzymuje brzmienie: „4. Do wniosku o wpis, o którym mowa w ust. 1, dołącza się, w postaci elektronicznej:	Przepisy dostosowujące ustawę o usługach zaufania oraz identyfikacji elektronicznej do zmian dotyczących

	a) musi posiadać odpowiednie polityki i wprowadzać odpowiednie środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla świadczenia niekwalifikowanej usługi zaufania, które – niezależnie od art. 21 dyrektywy (UE) 2022/2555 – obejmują co najmniej środki związane z: (i) procedurami rejestracji i wdrażania w odniesieniu do usługi zaufania; (ii) kontrolami proceduralnymi lub administracyjnymi niezbędnymi do świadczenia usług zaufania: (iii) zarządzaniem usługami zaufania i ich wdrażaniem; b) powiadomienie organu nadzoru, możliwych do zidentyfikowania osób fizycznych, których to dotyczy, oraz opinii publicznej, jeżeli leży to w interesie publicznym, oraz – w stosownych przypadkach – innych odpowiednich właściwych organów o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. a) ppkt (i), (ii) lub (iii), które mają znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w jej ramach dane osobowe, bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin po otrzymaniu informacji o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów ust. 1 lit. a) niniejszego artykułu. W przypadku gdy te normy,		art. 10 ust. 1 pkt 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	1) w przypadku, o których mowa w ust. 1 pkt 1 lub 2: a) raport z oceny zgodności, o którym mowa w art. 21 ust. 1 rozporządzenia 910/2014, wydany przez jednostkę oceniającą zgodność, b) politykę świadczenia usług objętych wnioskiem, zgodnie z którą mają być świadczone usługi zaufania, oraz adres strony internetowej, pod którym jest umieszczona ta polityka, c) plan zakończenia działalności, o którym mowa w art. 24 ust. 2 lit. i rozporządzenia 910/2014, d) odpowiednio do zakresu wniosku: - dane niezbędne do wystawienia certyfikatu, o którym mowa w art. 10 ust. 1 pkt 1, lub - w przypadku usług wydawania kwalifikowanych elektronicznych poświadczeń atrybutów, oraz kwalifikowanych usług walidacji podpisów i pieczęci elektronicznych – kwalifikowany certyfikat dostawcy usługi zaufania powiązany z usługą, której dotyczy wpis, lub - w przypadku usług wydawania, przez kwalifikowanego dostawcę usług zaufania wydającego	niekwalifikowanych dostawców usług zaufania.

	specyfikacje i procedury są przestrzegane, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.			kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektronicznej, certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi - certyfikat o którym mowa w ust. 4 pkt 1 lit. g załącznika II do rozporządzenia wykonawczego Komisji (UE) 2024/2980 z dnia 28 listopada 2024 r. ustanawiającego zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do notyfikowania Komisji w związku z ekosystemem europejskiego portfela tożsamości cyfrowej (Dz. Urz. UE L 2024/2980 z 04.12.2024)),; 2) w przypadku, o którym mowa w ust. 1 pkt 4 lub 5 – politykę świadczenia usług objętych wnioskiem, zgodnie z którą mają być świadczone usługi zaufania, spełniającą wymagania, o których mowa w art. 19a ust. 1 rozporządzenia 910/2014, oraz adres strony internetowej, pod którym jest umieszczona ta polityka; 3) w przypadku o którym mowa w ust. 1 pkt 6: a) politykę świadczenia usług objętych wnioskiem, zgodnie z	

				którą mają być świadczone usługi zaufania, spełniającą wymagania, o których mowa w art. 19a ust. 1 rozporządzenia 910/2014, oraz adres strony internetowej, pod którym jest umieszczona ta polityka, b) dokument potwierdzający spełnienie wymagań, o których mowa w art. 45f ust. 2 rozporządzenia 910/2014, sporządzony w wyniku niezależnego audytu zewnętrznego, c) kwalifikowany certyfikat dostawcy usługi zaufania powiązany z usługą której dotyczy wpis. ”, (….) 6) w art. 6: a) w ust. 1 pkt 2 otrzymuje brzmienie: „2) niekwalifikowanej usługi zaufania, z wyłączeniem usług, o których mowa w art. 4 ust. 1 pkt 3-6”, b) dodaje się ust. 3 w brzmieniu: „3. Do zgłoszenia niekwalifikowanej usługi zaufania do rejestru, o której mowa w ust. 1 pkt 2, dołącza się, w postaci elektronicznej, politykę świadczenia usług objętych zgłoszeniem, spełniającą	

				wymagania, o których mowa w art. 19a ust. 1 rozporządzenia 910/2014, oraz adres strony internetowej, pod którym jest umieszczona ta polityka."; (…..) 10) w art. 10 ust. 1 pkt 1 otrzymuje brzmienie: 1) tworzy i wydaje kwalifikowanym dostawcom usług zaufania oraz dostawcom usług zaufania o których mowa w art. 4 ust. 6 pkt 3 i 4 certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, o których mowa wlit. g załącznika I, w lit. g załącznika III i lit. h załącznika IV do rozporządzenia 910/2014, oraz certyfikaty służące do weryfikacji innych usług zaufania świadczonych przez dostawców usług zaufania wpisanych na zaufaną listę, zwane dalej „certyfikatami dostawcy usług zaufania;";	
Art. 20 ust 1 i 1a	1. Kwalifikowani dostawcy usług zaufania podlegają audytowi, na swój własny koszt, co najmniej raz na 24 miesiące, przeprowadzanemu przez jednostkę oceniającą zgodność. W ramach audytu potwierdza się, czy kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	rozporządzeniu oraz w art. 21 dyrektywy (UE) 2022/2555. Kwalifikowani dostawcy usług zaufania przedkładają organowi nadzoru powstały w wyniku audytu raport z oceny zgodności w terminie trzech dni roboczych od jego otrzymania. 1a. Kwalifikowani dostawcy usług zaufania informują organ nadzoru co najmniej miesiąc przed jakimkolwiek planowanym audytem oraz umożliwiają organowi nadzoru udział w charakterze obserwatora, na jego wniosek.				
Art. 20 ust. 1b	1b. Państwa członkowskie bez zbędnej zwłoki przekazują Komisji nazwy, adresy i szczegóły akredytacji jednostek oceniających zgodność, o których mowa w ust. 1, oraz wszelkie późniejsze zmiany w tym zakresie. Komisja udostępnia te informacje wszystkim państwom członkowskim.	TAK	Art. 1 pkt 14 (Art. 23 pkt 12 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 12) przekazuje Komisji Europejskiej informacje o jednostkach oceniających zgodność, o których mowa w art. 20 ust. 1b rozporządzenia 910/2014;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 20 ust. 2 i 3	2. Bez uszczerbku dla ust. 1, organ nadzoru może w dowolnym momencie przeprowadzić audyt lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania, na koszt tych	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	dostawców usług zaufania, aby potwierdzić, że dostawcy ci oraz świadczone przez nich kwalifikowane usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu. W przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, organ nadzoru informuje bez zbędnej zwłoki właściwe organy nadzorcze ustanowione zgodnie z art. 51 rozporządzenia (UE) 2016/679. 3. W przypadku gdy kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w niniejszym rozporządzeniu, organ nadzoru nakłada na niego wymóg wyeliminowania, w stosownych przypadkach w ustalonym terminie, niezgodności z tymi wymogami. W przypadku gdy dostawca ten nie wyeliminuje, w stosownych przypadkach w terminie ustalonym przez organ nadzoru, niezgodności z wymogami, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy.				
Art. 20 ust. 3a-3c	3a. W przypadku gdy właściwe organy wyznaczone lub ustanowione na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555 poinformują organ nadzoru, że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w art. 21 tej dyrektywy, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	dostawcy lub świadczonej przez niego usłudze, której to dotyczy. 3b. W przypadku gdy organy nadzorcze ustanowione zgodnie z art. 51 rozporządzenia (UE) 2016/679 poinformują organ nadzoru, że kwalifikowany dostawca usług zaufania nie spełnia któregokolwiek z wymogów określonych w tym rozporządzeniu, organ nadzoru, jeżeli jest to uzasadnione, biorąc pod uwagę w szczególności zakres, czas trwania i skutki tego niespełnienia wymogów, odbiera status kwalifikowany temu dostawcy lub świadczonej przez niego usłudze, której to dotyczy. 3c. Organ nadzoru informuje kwalifikowanego dostawcę usług zaufania o odebraniu jego statusu kwalifikowanego lub statusu kwalifikowanego danej usługi. Organ nadzoru informuje podmiot zgłoszony na podstawie art. 22 ust. 3 niniejszego rozporządzenia do celów aktualizacji zaufanych list, o których mowa w ust. 1 tego artykułu, oraz właściwy organ wyznaczony lub ustanowiony na podstawie art. 8 ust. 1 dyrektywy (UE) 2022/2555.				
Art. 20 ust. 4	4. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w stosownych przypadkach, ustanowi specyfikacje i procedury w odniesieniu do: a) akredytacji jednostek oceniających zgodność oraz raportu z oceny zgodności, o którym mowa w ust. 1; b) wymogów dotyczących audytów, zgodnie z którymi jednostki oceniające zgodność przeprowadzają oceny zgodności, w tym ocenę	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	złożoną, kwalifikowanych dostawców usług zaufania, o których mowa w ust. 1; c) programów oceny zgodności w zakresie przeprowadzania oceny zgodności kwalifikowanych dostawców usług zaufania przez jednostki oceniające zgodność oraz w odniesieniu do przekazywania raportu, o którym mowa w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 21 ust. 1 i 2 oraz ust. 4	1. W przypadku gdy dostawcy usług zaufania zamierzają rozpocząć świadczenie kwalifikowanej usługi zaufania, zgłaszają organowi nadzoru swój zamiar wraz z raportem z oceny zgodności wydanym przez jednostkę oceniającą zgodność potwierdzającym spełnienie wymogów określonych w niniejszym rozporządzeniu oraz w art. 21 dyrektywy (UE) 2022/2555. 2. Organ nadzoru weryfikuje, czy dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu, w szczególności wymogi dotyczące kwalifikowanych dostawców usług zaufania oraz świadczonych przez nich kwalifikowanych usług zaufania. W celu zweryfikowania spełnienia przez dostawcę usług zaufania wymogów określonych w art. 21 dyrektywy (UE) 2022/2555 organ nadzoru zwraca się do właściwych organów wyznaczonych lub ustanowionych na podstawie art. 8 ust. 1 tej dyrektywy o przeprowadzenie działań nadzorczych w tym zakresie oraz o udzielenie informacji na temat rezultatu tych działań bez zbędnej zwłoki i w	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	każdym razie nie później niż w terminie dwóch miesięcy od otrzymania tego wniosku. Jeżeli weryfikacja nie została zakończona w terminie dwóch miesięcy od zgłoszenia, te właściwe organy informują o tym organ nadzoru, podając przy tym przyczyny opóźnienia, oraz wskazują termin, w którym weryfikacja ma zostać zakończona. W przypadku gdy organ nadzoru stwierdzi, że dostawca usług zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w niniejszym rozporządzeniu, organ nadzoru przyznaje danemu dostawcy usług zaufania status kwalifikowanego dostawcy usług zaufania i status kwalifikowanych usług zaufania świadczonym przez niego usługom oraz informuje podmiot, o którym mowa w art. 22 ust. 3, w celu zaktualizowania przez niego zaufanych list, o których mowa w art. 22 ust. 1, nie później niż trzy miesiące po zgłoszeniu zgodnie z ust. 1 niniejszego artykułu. W przypadku gdy weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje o tym dostawcę usług zaufania, podając przyczyny opóźnienia, oraz wskazuje termin, w którym weryfikacja ma zostać zakończona. (…..) 4. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, określi formaty i procedury zgłaszania i weryfikacji na potrzeby ust. 1 i 2 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				

Art. 22 ust. 1	1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.	TAK	Art. 1 pkt 2 (Art. 2 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	2) w art. 2 pkt 2 otrzymuje brzmienie: „2) zaufane listy;”;	Dostosowanie przepisów krajowych umożliwiające prowadzenie w Polsce więcej niż jednej zaufanej listy.
Art. 22 ust. 5	5. Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1–4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	TAK	Art. 1 pkt 3 lit. a (Art. 3 ust. 4 pkt 2a-2c ustawy o usługach zaufania oraz identyfikacji elektronicznej)	w art. 3 w ust. 4: a) po pkt 2 dodaje się pkt 2a-2c w brzmieniu: „2a) adres poczty elektronicznej służący do kontaktu w sprawach związanych ze świadczonymi usługami zaufania; 2b) adres strony internetowej; 2c) numer telefonu służący do kontaktu z użytkownikami i organem nadzoru, jeżeli został podany;”,	Zmiana w związku ze wskazaniem w Decyzji Wykonawczej Komisji (UE) 2025/2164 z dnia 27 października 2025 r. zmieniającej decyzję wykonawczą (UE) 2015/1505 nowszej wersji normy, na której opiera się wzór zaufanych list. W normie ETSI TS 119 612 v2.4.1 wymaga się podania adresu email oraz strony internetowej oraz umożliwia się podanie numerów telefonów. W związku z tym należy odpowiednio poszerzyć zakres danych, które znajdą się w rejestrze i co za tym idzie we wnioskach o wpis oraz na zaufanej liście.

Art. 24 ust. 1-1c, ust. 2 lit. a, d, e, fa, fb, g, h, i oraz uchyla się lit. j, ust. 4a-5	1. Wydając kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów, kwalifikowany dostawca usług zaufania weryfikuje tożsamość oraz, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której ma być wydany kwalifikowany certyfikat lub kwalifikowane elektroniczne poświadczenie atrybutów. 1a. Weryfikacji tożsamości, o której mowa w ust. 1, dokonuje kwalifikowany dostawca usług zaufania, za pomocą odpowiednich środków, bezpośrednio albo za pośrednictwem strony trzeciej, w oparciu o jedną z następujących metod lub, w razie potrzeby, ich połączenie, zgodnie z aktami wykonawczymi, o których mowa w ust. 1c: a) za pomocą europejskiego portfela tożsamości cyfrowej lub notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa; b) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a), c) lub d); c) przy użyciu innych metod identyfikacji, które z dużą dozą pewności zapewniają identyfikację osoby i których zgodność jest potwierdzona przez jednostkę oceniającą zgodność; d) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	1b. Weryfikacji atrybutów, o których mowa w ust. 1, dokonuje kwalifikowany dostawca usług zaufania, za pomocą odpowiednich środków, bezpośrednio albo za pośrednictwem strony trzeciej, w oparciu o jedną z następujących metod lub, w razie potrzeby, ich połączenie, zgodnie z aktami wykonawczymi, o których mowa w ust. 1c: a) za pomocą europejskiego portfela tożsamości cyfrowej lub notyfikowanego środka identyfikacji elektronicznej, który spełnia wymogi określone w art. 8 w odniesieniu do wysokiego poziomu bezpieczeństwa; b) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej, wydanych zgodnie z ust. 1a lit. a), c) lub d); c) za pomocą kwalifikowanego elektronicznego poświadczenia atrybutów; d) stosując inne metody, które z dużą dozą pewności zapewniają weryfikację atrybutów, i których zgodność jest potwierdzona przez jednostkę oceniającą zgodność; e) poprzez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej, za pomocą odpowiednich dowodów oraz procedur, zgodnie z prawem krajowym. 1c. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów weryfikacji tożsamości i atrybutów zgodnie z ust. 1, 1a i 1b niniejszego artykułu. Te akty wykonawcze				

	przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. (…….) w ust. 2: a) informuje organ nadzoru co najmniej miesiąc przed wprowadzeniem jakiejkolwiek zmiany w świadczeniu przez niego kwalifikowanych usług zaufania lub z co najmniej trzymiesięcznym wyprzedzeniem w przypadku zamiaru zaprzestania tej działalności; (….) d) przed nawiązaniem stosunku umownego informuje w jasny, kompleksowy i łatwo dostępny sposób, w miejscu publicznie dostępnym oraz indywidualnie wszelkie osoby, które mają zamiar skorzystać z kwalifikowanej usługi zaufania, o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej; e) używa wiarygodnych systemów i produktów, które są chronione przed modyfikacją oraz zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez nie obsługiwanych, w tym przy użyciu odpowiednich technik kryptograficznych; (….) fa) niezależnie od art. 21 dyrektywy (UE) 2022/2555, posiada odpowiednie polityki oraz wprowadza odpowiednie środki w celu zarządzania ryzykiem prawnym, biznesowym, operacyjnym oraz innymi bezpośrednimi lub pośrednimi ryzykami dla				

	świadczenia kwalifikowanej usługi zaufania, w tym co najmniej środki związane z: (i) procedurami rejestracji i wdrażania w odniesieniu do usługi; (ii) kontrolami proceduralnymi lub administracyjnymi;(iii)zarządzaniem usługami zaufania oraz ich wdrażaniem; fb) bez zbędnej zwłoki, a w każdym razie nie później niż w terminie 24 godzin od incydentu, powiadamia organ nadzoru, możliwe do zidentyfikowania osoby fizyczne, których to dotyczy, a także – w stosownych przypadkach – inne odpowiednie właściwe organy oraz, na wniosek organu nadzoru, opinię publiczną, jeżeli leży to w interesie publicznym, o wszelkich naruszeniach bezpieczeństwa lub zakłóceniach w świadczeniu usługi lub we wdrażaniu środków, o których mowa w lit. fa) ppkt (i), (ii) lub (iii), które mają znaczący wpływ na świadczoną usługę zaufania lub na przetwarzane w ramach tej usługi dane osobowe; (….) g) wprowadza odpowiednie środki zapobiegające fałszowaniu, kradzieży lub przywłaszczeniu danych, lub nieuprawnionemu usuwaniu, modyfikowaniu lub uniemożliwianiu dostępu do danych; h) rejestruje i udostępnia tak długo, jak jest to konieczne po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszystkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, do celów przedstawienia dowodów w postępowaniach				

	sądowych do celów zapewnienia ciągłości usług. Rejestracja taka może odbywać się drogą elektroniczną; i) posiada aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z postanowieniami, które zostały zweryfikowane przez organ nadzoru zgodnie z art. 46b ust. 4 lit. i); uchyla się lit. j); dodaje się akapit w brzmieniu:,, Organ nadzoru może zażądać dodatkowych informacji oprócz informacji przekazanych zgodnie z akapitem pierwszym lit. a) lub wyników oceny zgodności oraz może uzależnić udzielenie zezwolenia na wdrożenie planowanych zmian w kwalifikowanych usługach zaufania. Jeżeli weryfikacja nie została zakończona w terminie trzech miesięcy od zgłoszenia, organ nadzoru informuje o tym dostawcę usług zaufania, podając przyczyny opóźnienia, oraz wskazuje termin, w którym weryfikacja ma zostać zakończona. (….) 4a. Ust. 3 i 4 stosuje się odpowiednio do unieważniania kwalifikowanych elektronicznych poświadczeń atrybutów. 4b. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, ustanawiających dodatkowe środki, o których mowa w ust. 2 lit. fa) niniejszego artykułu. 5. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi				

	specyfikacje i procedury w odniesieniu do wymogów, o których mowa w ust. 2 niniejszego artykułu. W przypadku gdy te normy, specyfikacje i procedury są przestrzegane, domniemywa się zgodność z wymogami określonymi w niniejszym ustępie. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 24a	**Uznawanie kwalifikowanych usług zaufania** 1. Kwalifikowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim oraz kwalifikowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim uznaje się, odpowiednio, za kwalifikowane podpisy elektroniczne i kwalifikowane pieczęcie elektroniczne we wszystkich pozostałych państwach członkowskich. 2. Kwalifikowane urządzenia do składania podpisu elektronicznego oraz kwalifikowane urządzenia do składania pieczęci elektronicznej certyfikowane w jednym państwie członkowskim uznaje się, odpowiednio, za kwalifikowane urządzenia do składania podpisu elektronicznego i kwalifikowane urządzenia do składania pieczęci elektronicznej we wszystkich pozostałych państwach członkowskich. 3. Kwalifikowany certyfikat podpisów elektronicznych, kwalifikowany certyfikat pieczęci elektronicznych, kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość oraz kwalifikowaną usługę zaufania w zakresie zarządzania urządzeniami do składania	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	kwalifikowanej pieczęci elektronicznej na odległość zapewniane w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowany certyfikat podpisów elektronicznych, kwalifikowany certyfikat pieczęci elektronicznych, kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość oraz kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość we wszystkich pozostałych państwach członkowskich. 4. Kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych oraz kwalifikowaną usługę walidacji kwalifikowanych pieczęci elektronicznych, świadczone w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowaną usługę walidacji kwalifikowanych pieczęci elektronicznych we wszystkich pozostałych państwach członkowskich. 5. Kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych oraz kwalifikowaną usługę konserwacji kwalifikowanych pieczęci elektronicznych, świadczone w jednym państwie członkowskim, uznaje się, odpowiednio, za kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych i kwalifikowaną usługę konserwacji kwalifikowanych pieczęci elektronicznych we wszystkich pozostałych państwach członkowskich. 6. Kwalifikowany elektroniczny znacznik czasu zapewniany w jednym państwie członkowskim				

	uznaje się za kwalifikowany elektroniczny znacznik czasu we wszystkich pozostałych państwach członkowskich. 7. Kwalifikowany certyfikat uwierzytelniania witryn internetowych wydany w jednym państwie członkowskim uznaje się za kwalifikowany certyfikat uwierzytelniania witryn internetowych we wszystkich pozostałych państwach członkowskich. 8. Kwalifikowaną usługę rejestrowanego doręczenia elektronicznego świadczoną w jednym państwie członkowskim uznaje się za kwalifikowaną usługę rejestrowanego doręczenia elektronicznego we wszystkich pozostałych państwach członkowskich. 9. Kwalifikowane elektroniczne poświadczenie atrybutów wydane w jednym państwie członkowskim uznaje się za kwalifikowane elektroniczne poświadczenie atrybutów we wszystkich pozostałych państwach członkowskich. 10. Kwalifikowane usługi archiwizacji elektronicznej świadczone w jednym państwie członkowskim uznaje się za kwalifikowane usługi archiwizacji elektronicznej we wszystkich pozostałych państwach członkowskich. 11. Kwalifikowany rejestr elektroniczny zapewniany w jednym państwie członkowskim uznaje się za kwalifikowany rejestr elektroniczny we wszystkich pozostałych państwach członkowskich.				
Art. 25	w art. 25 uchyla się ust. 3;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 26 ust. 2	2. Do dnia 21 maja 2026 r. Komisja oceni, czy konieczne jest przyjęcie aktów wykonawczych w celu ustanowienia wykazu norm referencyjnych oraz, w razie potrzeby, ustanowienia specyfikacji i procedur w odniesieniu do zaawansowanych podpisów elektronicznych. Komisja może przyjąć takie akty wykonawcze na podstawie tej oceny. W przypadku gdy zaawansowany podpis elektroniczny jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 27	w art. 27 uchyla się ust. 4;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 28 ust. 6	6. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 29 ust. 1a	1a. Dane służące do składania podpisu elektronicznego mogą być generowane, zarządzane lub kopiowane w celu utworzenia kopii zapasowej wyłącznie w imieniu podpisującego, na	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	jego żądanie, i przez kwalifikowanego dostawcę usług zaufania, który świadczy kwalifikowaną usługę zaufania w zakresie zarządzania kwalifikowanym urządzeniem do składania podpisu elektronicznego na odległość.				
Art. 29a	**Wymogi dotyczące kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość** Art. 29a.1. Zarządzanie kwalifikowanymi urządzeniami do składania podpisu elektronicznego na odległość jako usługę kwalifikowaną może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który: a) generuje dane służące do składania podpisu elektronicznego lub zarządza nimi w imieniu podpisującego; b) niezależnie od pkt 1 lit. d) załącznika II kopiuje dane służące do składania podpisu elektronicznego wyłącznie w celu utworzenia kopii zapasowej, pod warunkiem że spełnione są następujące wymogi: (i) bezpieczeństwo skopiowanych zbiorów danych musi być na tym samym poziomie co w przypadku oryginalnych zbiorów danych; (ii) liczba skopiowanych zbiorów danych nie może przekraczać minimum niezbędnego do zapewnienia ciągłości usługi; c) spełnia wszelkie wymogi określone w raporcie z certyfikacji konkretnego kwalifikowanego urządzenia do składania podpisu elektronicznego na odległość, wydanym zgodnie z art. 30.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi wykaz norm referencyjnych oraz, w razie potrzeby, specyfikacje i procedury do celów ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 30 ust. 1 i 2	1. Zgodność kwalifikowanych urządzeń do składania podpisu elektronicznego z wymogami określonymi w załączniku II jest certyfikowana przez odpowiednie publiczne lub prywatne podmioty wyznaczone przez państwa członkowskie. 2. Państwa członkowskie zgłaszają Komisji nazwy i adresy podmiotów publicznych lub prywatnych, o których mowa w ust. 1. Komisja udostępnia te informacje państwom członkowskim.	TAK	Art. 1 pkt 14 (Art. 23 pkt 13 ustawy o usługach zaufania oraz identyfikacji elektronicznej) Art. 1 pkt 18 (Art. 37 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (……) 13) wyznacza podmioty certyfikujące urządzenia do składania podpisu elektronicznego, o których mowa w art. 30 ust. 1 rozporządzenia 910/2014, przekazuje Komisji Europejskiej ich nazwy i adresy , zgodnie z art. 30 ust. 2 rozporządzenia 910/2014, oraz informacje o urządzeniach certyfikowanych przez te podmioty, zgodnie z art. 31 ust. 1 rozporządzenia 910/2014; 18) uchyla się art. 37.	Przeniesienie dotychczasowego przepisu art. 37 do art. 23, w którym znalazły się inne zadania ministra związane z licznymi dodatkowymi zadaniami nałożonymi na państwa członkowskie w związku ze zmianami w rozporządzeniu eIDAS.

Art. 30 ust. 3a	3a. Ważność certyfikacji, o której mowa w ust. 1, nie może przekraczać pięciu lat, pod warunkiem że co dwa lata przeprowadza się ocenę podatności na zagrożenia. W przypadku gdy zostaną stwierdzone podatności na zagrożenia i nie zostaną one wyeliminowane, certyfikacja zostaje odwołana.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 31 ust. 3	3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi formaty i procedury mające zastosowanie do celów ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 32 ust. 1 i 3	w ust. 1 dodaje się akapit w brzmieniu: W przypadku gdy walidacja kwalifikowanych podpisów elektronicznych jest zgodna z normami, specyfikacjami i procedurami, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w akapicie pierwszym niniejszego ustępu. (….) 3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów walidacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 32a	**Wymogi dotyczące walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach**	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	Art. 32a.1. Proces walidacji zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie potwierdza ważność zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie, pod warunkiem że: a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I; b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu; c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej; d) niepowtarzalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej; e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej; f) integralność podpisanych danych nie została skompromitowana; g) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu. 2. System wykorzystany do walidacji zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie musi zapewniać stronie ufającej prawidłowy wynik procesu walidacji oraz umożliwiać stronie ufającej				

	wykrycie wszelkich problemów związanych z bezpieczeństwem. 3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do walidacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach. W przypadku gdy walidacja zaawansowanych podpisów elektronicznych opartych na kwalifikowanych certyfikatach jest zgodna z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 33 ust. 2	2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanej usługi walidacji, o której mowa w ust. 1 niniejszego artykułu. W przypadku gdy kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych jest zgodna z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 34 ust. 1a i 2	1a. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych są zgodne z normami, specyfikacjami i procedurami, o których mowa w	NIE			Przepis stosowany wprost ,nie wymaga wdrożenia.

	ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 35 ust. 3	w art. 35 uchyla się ust. 3;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 36 ust. 1 i 2	pojedynczy ustęp staje się ust. 1; 2. Do dnia 21 maja 2026 r. Komisja oceni, czy należy konieczne jest przyjęcie aktów wykonawczych w celu sporządzenia wykazu norm referencyjnych oraz, w razie potrzeby, ustanowienia specyfikacji i procedur w odniesieniu do zaawansowanych pieczęci elektronicznych. Komisja może przyjąć takie akty wykonawcze na podstawie tej oceny. W przypadku gdy zaawansowane pieczęcie elektroniczne są zgodne z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 37 ust. 4	w art. 37 uchyla się ust. 4;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 38 ust. 6	6. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów pieczęci elektronicznych. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej jest zgodny z tymi normami, specyfikacjami i procedurami, domniemywa się zgodność z wymogami określonymi w załączniku III. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 39a	**Wymogi dotyczące kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość** Art. 29a stosuje się odpowiednio do kwalifikowanej usługi zarządzania kwalifikowanymi urządzeniami do składania pieczęci elektronicznej na odległość.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 40a	**Wymogi dotyczące walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach** Art. 32a stosuje się odpowiednio do walidacji zaawansowanych pieczęci elektronicznych opartych na kwalifikowanych certyfikatach.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 41	w art. 41 uchyla się ust. 3;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 42 ust. 1a i 2	1a. W przypadku gdy powiązanie daty i czasu z danymi oraz precyzyjność źródła czasu są zgodne z normami, specyfikacjami i procedurami, o których	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 44 ust. 1a, 2, 2a i 2b	1a. W przypadku gdy proces wysyłania i otrzymywania danych jest zgodny z normami, specyfikacjami i procedurami, o których mowa w ust. 2, domniemywa się zgodność z wymogami określonymi w ust. 1. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące procesu wysyłania i otrzymywania danych. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 2a. Dostawcy kwalifikowanych usług rejestrowanego doręczenia elektronicznego mogą uzgodnić interoperacyjność świadczonych przez nich kwalifikowanych usług rejestrowanego doręczenia elektronicznego. Takie ramy interoperacyjności muszą być zgodne z wymogami określonymi w ust. 1, a zgodność ta musi zostać potwierdzona przez jednostkę oceniającą zgodność. 2b. Komisja może, w drodze aktów wykonawczych, sporządzić wykaz norm referencyjnych oraz, w	NIE			Przepis stosowany wprost nie wymaga wdrożenia.

	razie potrzeby, ustanowić specyfikacje i procedury dotyczące ram interoperacyjności, o których mowa w ust. 2a niniejszego artykułu. Specyfikacje techniczne i treść norm muszą być efektywne kosztowo i proporcjonalne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 45	**Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych** 1. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV. Ocenę zgodności z tymi wymogami przeprowadza się zgodnie z normami, specyfikacjami i procedurami, o których mowa w ust. 2 niniejszego artykułu. 1a. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych wydane zgodnie z ust. 1 niniejszego artykułu, muszą być rozpoznawane przez dostawców przeglądarek internetowych. Dostawcy przeglądarek internetowych muszą zapewniać, aby dane dotyczące tożsamości poświadczone w certyfikacie oraz dodatkowe poświadczone atrybuty były wyświetlane w sposób przyjazny dla użytkownika. Dostawcy przeglądarek internetowych zapewniają obsługę kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1 niniejszego artykułu, oraz interoperacyjność z tymi certyfikatami, z wyjątkiem mikroprzedsiębiorstw lub małych przedsiębiorstw zdefiniowanych w art. 2 załącznika do zalecenia Komisji 2003/361/WE, w ciągu pierwszych pięciu lat ich działalności w charakterze dostawców usług przeglądania stron internetowych.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	1b. Kwalifikowane certyfikaty uwierzytelniania witryn internetowych nie podlegają jakimkolwiek obowiązkowym wymogom innym niż wymogi określone w ust. 1. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych certyfikatów uwierzytelniania witryn internetowych, o których mowa w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 45a	**Środki zapobiegawcze w zakresie cyberbezpieczeństwa** 1. Dostawcy przeglądarek internetowych nie mogą wprowadzać jakichkolwiek środków sprzecznych z ich obowiązkami określonymi w art. 45, w szczególności wymogów uznawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oraz wyświetlania dostarczonych danych dotyczących tożsamości w sposób przyjazny dla użytkownika. 2. Na zasadzie odstępstwa od ust. 1 oraz jedynie w przypadku uzasadnionych podejrzeń związanych z naruszeniem bezpieczeństwa lub utratą integralności konkretnego certyfikatu lub zestawu certyfikatów, dostawcy przeglądarek internetowych mogą wprowadzać środki zapobiegawcze w odniesieniu do tego certyfikatu lub zestawu certyfikatów. 3. W przypadku gdy dostawca przeglądarki internetowej wprowadza takie środki	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	zapobiegawcze na podstawie ust. 2, bez zbędnej zwłoki zgłasza swoje podejrzenia na piśmie – wraz z opisem środków wprowadzonych w reakcji na te podejrzenia – Komisji, właściwemu organowi nadzorczemu, podmiotowi, któremu wydano dany certyfikat, oraz kwalifikowanemu dostawcy usług zaufania, który wydał dany certyfikat lub zestaw certyfikatów. Po otrzymaniu takiego zgłoszenia właściwy organ nadzorczy wydaje danemu dostawcy przeglądarki internetowej potwierdzenie otrzymania. 4. Właściwy organ nadzoru bada kwestie zawarte w zgłoszeniu zgodnie z art. 46b ust. 4 lit. k). W przypadku gdy w wyniku tego dochodzenia nie odebrano statusu certyfikatu kwalifikowanego, organ nadzoru informuje o tym odpowiednio danego dostawcę przeglądarki internetowej oraz zwraca się do tego dostawcy o zakończenie środków zapobiegawczych, o których mowa w ust. 2 niniejszego artykułu.				
Art. 45b ust. 1	**Skutki prawne elektronicznego poświadczenia atrybutów** 1. Elektronicznemu poświadczeniu atrybutów nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że ma postać elektroniczną lub że nie spełnia wymogów dotyczących kwalifikowanych elektronicznych poświadczeń atrybutów.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 45b ust. 2 i 3	2. Kwalifikowane elektroniczne poświadczenie atrybutów oraz poświadczenia atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu ma taki	TAK	Art. 1 pkt 13 (Art. 22f ustawy o	Art. 22f. 1. Podmioty odpowiedzialne za źródła autentyczne mogą wydawać elektroniczne poświadczenia	Zgodnie z art. 45b ust. 2 oraz art. 3 pkt 46 rozporządzenia 910/2014 podmioty

	sam skutek prawny jak poświadczenia wydane zgodnie z prawem w postaci papierowej. 3. Poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu w jednym z państw członkowskich uznaje się za poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu we wszystkich państwach członkowskich.		usługach zaufania oraz identyfikacji elektronicznej)	atrybutów, o których mowa w art. 3 pkt 44 lub 46 rozporządzenia 910/2014, po złożeniu wniosku, o którym mowa w art. 4 ust. 1 pkt 5 lub 6 i uzyskaniu wpisu do rejestru. 2. Minister właściwy do spraw informatyzacji może wydawać elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, w imieniu podmiotów odpowiedzialnych za źródła autentyczne, na wniosek, o którym mowa w art. 22i.	sektora publicznego odpowiedzialne za źródło autentyczne mogą wydawać elektroniczne poświadczenie atrybutów w swoim imieniu mające skutek prawny określony w art. 45b rozporządzenia 910/2014. Przepis ust. 1 ma na celu jednoznaczne ustanowienie obowiązku wpisania się takich podmiotów do rejestru dostawców usług zaufania. Minister właściwy do spraw informatyzacji zapewnia obecnie rozwiązanie umożliwiające uzyskanie przez użytkownika aplikacji mObywatel dokumentów mobilnych. W związku z tym proponuje się, aby minister właściwy do spraw informatyzacji był podmiotem, który może wydawać elektroniczne poświadczenie atrybutów w imieniu

					podmiotu sektora publicznego odpowiedzialny za źródło autentyczne.
Art. 45c	**Elektroniczne poświadczenie atrybutów w usługach publicznych** W przypadku gdy zgodnie z prawem krajowym dostęp do usługi online świadczonej przez podmiot sektora publicznego wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelnienia, dane identyfikujące osobę w elektronicznym poświadczeniu atrybutów nie zastępują identyfikacji elektronicznej przy użyciu środków identyfikacji elektronicznej i uwierzytelniania przy identyfikacji elektronicznej, chyba że państwo członkowskie wyraźnie na to zezwoli. W takim przypadku akceptuje się również kwalifikowane elektroniczne poświadczenia atrybutów wydane w innych państwach członkowskich.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 45d	**Wymogi dotyczące kwalifikowanego elektronicznego poświadczenia atrybutów** 1. Kwalifikowane elektroniczne poświadczenie atrybutów musi spełniać wymogi określone w załączniku V. 2. Ocenę zgodności z wymogami określonymi w załączniku V przeprowadza się zgodnie z normami, specyfikacjami i procedurami, o których mowa w ust. 5 niniejszego artykułu. 3. Kwalifikowane elektroniczne poświadczenia atrybutów nie podlegają jakimkolwiek	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	obowiązkowym wymogom oprócz wymogów określonych w załączniku V. 4. W przypadku gdy kwalifikowane elektroniczne poświadczenie atrybutów zostało unieważnione po wydaniu, traci ono ważność z chwilą jego unieważnienia i w żadnym przypadku nie można przywrócić jego poprzedniego statusu. 5. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury dotyczące kwalifikowanych elektronicznych poświadczeń atrybutów. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 45e ust. 1	1. Państwa członkowskie zapewniają, w terminie 24 miesięcy od dnia wejścia w życie aktów wykonawczych, o których mowa w art. 5a ust. 23 i art. 5c ust. 6, aby przynajmniej w odniesieniu do atrybutów wymienionych w załączniku VI, w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym, wprowadzono środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów, weryfikację tych atrybutów drogą elektroniczną, na żądanie użytkownika, zgodnie z prawem Unii lub prawem krajowym.	TAK	Art. 1 pkt 13 (Art. 22c ust. 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22c. 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	Przeniesiono ogólne wymagania rozporządzenia eIDAS do prawa krajowego, ponieważ cały czas powstają kolejne źródła autentyczne w rozumieniu załącznika VI tego rozporządzenia. Ich wymienianie w ustawie o usługach zaufania oraz identyfikacji elektronicznej powodowałoby

				art. 45e ust. 1 rozporządzenia 910/2014.	konieczność ciągłych zmian tej ustawy. W związku z tym, że rozporządzenie eIDAS obowiązuje bezpośrednio, nie ma takiej potrzeby.
Art. 45e ust. 2	2. Do dnia 21 listopada 2024 r. Komisja, uwzględniając odpowiednie normy międzynarodowe, sporządzi, w drodze aktów wykonawczych, wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do katalogu atrybutów, a także schematów poświadczania atrybutów i procedur weryfikacji kwalifikowanych elektronicznych poświadczeń atrybutów do celów ust. 1 niniejszego artykułu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskich portfeli tożsamości cyfrowej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 45f ust. 1 i 2	**Wymogi dotyczące elektronicznego poświadczenia atrybutów wydanego przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu** 1. Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu musi spełniać następujące wymogi: a) wymogi określone w załączniku VII;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	b) kwalifikowany certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej podmiotu sektora publicznego, o którym mowa w art. 3 pkt 46, zidentyfikowanego jako wydawca, o którym mowa w załączniku VII lit. b), zawiera określony zestaw certyfikowanych atrybutów w formie nadającej się do automatycznego przetwarzania oraz: (i) wskazanie, że podmiot wydający został ustanowiony zgodnie z prawem Unii lub prawem krajowym jako podmiot odpowiedzialny za źródło autentyczne, na podstawie którego wydawane jest elektroniczne poświadczenie atrybutów, lub jako podmiot wyznaczony do działania w jego imieniu; (ii) dostarczenie zestawu danych jednoznacznie reprezentujących źródło autentyczne, o którym mowa w ppkt (i); oraz (iii) wskazanie prawa Unii lub prawa krajowego, o którym mowa w ppkt (i). 2. Państwo członkowskie, w którym mają siedzibę podmioty sektora publicznego, o których mowa w art. 3 pkt 46, zapewnia, aby podmioty sektora publicznego, które wydają elektroniczne poświadczenia atrybutów, zapewniały poziom rzetelności i wiarygodności równoważny kwalifikowanym dostawcom usług zaufania zgodnie z art. 24.				
Art. 45 f ust. 3	3. Państwa członkowskie notyfikują Komisji podmioty sektora publicznego, o których mowa w art. 3 pkt 46. Notyfikacja ta obejmuje raport z oceny zgodności wydany przez jednostkę oceniającą zgodność, potwierdzający spełnienie wymogów	TAK	Art. 1 pkt 14 (Art. 23 pkt 14 ustawy o usługach	Art. 23. Minister właściwy do spraw informatyzacji: (…)	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji

	określonych w ust. 1, 2 i 6 niniejszego artykułu. Komisja - przy użyciu zabezpieczonego kanału komunikacji - udostępnia publicznie wykaz podmiotów sektora publicznego, o których mowa w ust. 3 pkt 46, w postaci pozwalającej na automatyczne przetwarzanie, elektronicznie podpisany lub opatrzony pieczęcią elektroniczną.		zaufania oraz identyfikacji elektronicznej)	14) notyfikuje Komisji Europejskiej podmioty sektora publicznego, o których mowa w art. 3 pkt 46 rozporządzenia 910/2014, zgodnie z art. 45f ust. 3 rozporządzenia 910/2014;	rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 45f ust. 4-8	4. W przypadku gdy elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu zostało unieważnione po wydaniu, traci ono ważność od momentu jego unieważnienia i nie można przywrócić jego poprzedniego statusu. 5. Elektroniczne poświadczenie atrybutów wydane przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu uznaje się za zgodne z wymogami określonymi w ust. 1, w przypadku gdy przestrzega ono norm, specyfikacji i procedur, o których mowa w ust. 6. 6. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do elektronicznego poświadczania atrybutów wydawanego przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego	NIE			Przepis stosowany wprost nie wymaga wdrożenia.

	imieniu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 7. Do dnia 21 listopada 2024 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury do celów ust. 3 niniejszego artykułu. Te akty wykonawcze muszą być spójne z aktami wykonawczymi, o których mowa w art. 5a ust. 23, dotyczącymi wdrożenia europejskiego portfela tożsamości cyfrowej. Przyjmuje się je zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2. 8. Podmioty sektora publicznego, o których mowa w art. 3 pkt 46, wydające elektroniczne poświadczenie atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej, które są zapewniane zgodnie z art. 5a.				
Art. 45g	**Wydawanie elektronicznych poświadczeń atrybutów do europejskich portfeli tożsamości cyfrowej** 1. Dostawcy elektronicznych poświadczeń atrybutów zapewniają użytkownikom europejskiego portfela tożsamości cyfrowej możliwość żądania, otrzymywania i przechowywania elektronicznego poświadczenia atrybutów, a także zarządzania nim, niezależnie od państwa członkowskiego, w którym zapewniany jest europejski portfel tożsamości cyfrowej.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	2. Dostawcy kwalifikowanych elektronicznych poświadczeń atrybutów zapewniają interfejs z europejskimi portfelami tożsamości cyfrowej, które są zapewniane zgodnie z art. 5a.				
Art. 45h	**Dodatkowe przepisy w odniesieniu do świadczenia usług elektronicznego poświadczania atrybutów** 1. Dostawcy kwalifikowanych i niekwalifikowanych usług elektronicznego poświadczania atrybutów nie mogą łączyć danych osobowych związanych ze świadczeniem tych usług z danymi osobowymi pochodzącymi z jakichkolwiek innych usług oferowanych przez nich lub przez ich partnerów handlowych. 2. Dane osobowe związane ze świadczeniem usług elektronicznego poświadczania atrybutów muszą być logicznie oddzielone od wszelkich innych danych przechowywanych przez dostawcę elektronicznego poświadczenia atrybutów. 3. Dostawcy usług kwalifikowanych elektronicznego poświadczania atrybutów wdrażają świadczenie takich kwalifikowanych usług zaufania w sposób, który jest funkcjonalnie oddzielony od innych świadczonych przez nich usług.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 45i	SEKCJA 10 USŁUGI ARCHIWIZACJI ELEKTRONICZNEJ **Skutki prawne usług archiwizacji elektronicznej** 1. Danym elektronicznym oraz elektronicznym dokumentom przechowywanym przy użyciu usługi archiwizacji elektronicznej nie można odmówić skutku prawnego ani dopuszczalności jako dowodu	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	w postępowaniu sądowym wyłącznie z tego powodu, że dane te mają postać elektroniczną lub że nie są przechowywane przy użyciu kwalifikowanej usługi archiwizacji elektronicznej. 2. Dane elektroniczne oraz elektroniczne dokumenty przechowywane przy użyciu kwalifikowanej usługi archiwizacji elektronicznej korzystają z domniemania ich integralności i pochodzenia przez cały okres przechowywania przez kwalifikowanego dostawcę usług zaufania.				
Art. 45j	**Wymogi dotyczące kwalifikowanych usług archiwizacji elektronicznej** 1. Kwalifikowane usługi archiwizacji elektronicznej muszą spełniać następujące wymogi: a) są świadczone przez kwalifikowanych dostawców usług zaufania; b) wykorzystują procedury i technologie umożliwiające zapewnienie trwałości i czytelności danych elektronicznych i dokumentów elektronicznych poza technologiczny okres ważności i co najmniej na cały okres prawnego lub umownego okresu przechowywania, przy jednoczesnym zachowaniu ich integralności i autentyczności pochodzenia; c) zapewniają przechowywanie tych danych elektronicznych i dokumentów elektronicznych w taki sposób, aby były zabezpieczone przed utratą i modyfikacją, z wyjątkiem zmian dotyczących ich nośnika lub formatu elektronicznego; d) umożliwiają one upoważnionym stronom ufającym otrzymanie w automatyczny sposób raportu potwierdzającego, że dane elektroniczne i	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	dokumenty elektroniczne pobrane z kwalifikowanego archiwum elektronicznego korzystają z domniemania integralności danych od początku okresu przechowywania do momentu pobrania. Raport, o którym mowa w lit. d) akapitu pierwszego, musi być przekazywany w sposób niezawodny i efektywny oraz opatrzony kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną dostawcy kwalifikowanej usługi archiwizacji elektronicznej. 2. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do kwalifikowanych usług archiwizacji elektronicznej. W przypadku gdy kwalifikowana usługa archiwizacji elektronicznej spełnia wymogi tych norm, specyfikacji i procedur, domniemywa się zgodność z wymogami dotyczącymi kwalifikowanych usług archiwizacji elektronicznej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 45k	SEKCJA 11 REJESTRY ELEKTRONICZNE **Skutki prawne rejestrów elektronicznych** 1. Rejestrowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że rejestr ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych rejestrów elektronicznych.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	2. Wpisy danych zawarte w kwalifikowanym rejestrze elektronicznym korzystają z domniemania ich niepowtarzalnego i dokładnego sekwencyjnego uporządkowania chronologicznego oraz ich integralności.				
	Wymogi dotyczące kwalifikowanych rejestrów elektronicznych 1. Kwalifikowane rejestry elektroniczne muszą spełniać następujące wymogi: a) są tworzone i zarządzane przez co najmniej jednego kwalifikowanego dostawcę usług zaufania; b) ustalają pochodzenie wpisów danych w rejestrze; c) zapewniają niepowtarzalne sekwencyjne uporządkowanie chronologiczne wpisów danych w rejestrze; d) rejestrują dane w taki sposób, że każda późniejsza zmiana danych jest natychmiast wykrywalna, co zapewnia ich integralność w czasie. 2. W przypadku gdy rejestr elektroniczny przestrzega norm, specyfikacji i procedur, o których mowa w ust. 3, domniemywa się zgodność z wymogami określonymi w ust. 1. 3. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, sporządzi wykaz norm referencyjnych oraz, w razie potrzeby, ustanowi specyfikacje i procedury w odniesieniu do wymogów określonych w ust. 1 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 46a ust. 1-5	**Nadzór nad ramami dla europejskiego portfela tożsamości cyfrowej** 1. Państwa członkowskie wyznaczają na swoim terytorium jeden lub większą liczbę organów nadzoru. Organy nadzoru wyznaczone zgodnie z akapitem pierwszym muszą otrzymać niezbędne uprawnienia i odpowiednie zasoby do wykonywania swoich zadań w sposób skuteczny, efektywny i niezależny. 2. Państwa członkowskie przekazują Komisji nazwy i adresy swoich organów nadzoru wyznaczonych zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie. Komisja publikuje wykaz zgłoszonych organów nadzoru. 3. Organy nadzoru wyznaczone zgodnie z ust. 1 spełniają następującą rolę: a) sprawują nadzór nad dostawcami europejskich portfeli tożsamości cyfrowej mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego oraz zapewniają - za pomocą działań nadzorczych *ex ante* i *ex post* - aby ci dostawcy i dostarczane przez nich europejskie portfele tożsamości cyfrowej spełniały wymogi określone w niniejszym rozporządzeniu; b) podejmują w razie potrzeby działania - za pomocą działań nadzorczych ex post - w odniesieniu do mających siedzibę na terytorium wyznaczającego państwa członkowskiego dostawców europejskich portfeli tożsamości cyfrowej po otrzymaniu informacji, że dostawcy lub europejskie portfele tożsamości cyfrowej,	TAK	Art. 1 pkt 13 (Art. 22j pkt 3 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22j. Minister właściwy do spraw informatyzacji: (…) 3) jest organem nadzoru, o którym mowa w art. 46a ust. 1 rozporządzenia 910/2014, oraz przekazuje Komisji Europejskiej odpowiednie informacje w tym zakresie.	Obecnie minister właściwy do spraw informatyzacji pełni rolę organu nadzoru nad dostawcami usług zaufania oraz nad krajowym schematem identyfikacji elektronicznej zatem zasadne jest aby nie powielać tego typu kompetencji w innych organach administracji. Jednakże realizując zadania w zakresie nadzoru minister musi zapewnić że nadzór będzie sprawowany niezależnie od zadań w zakresie zapewnienia europejskiego portfela tożsamości cyfrowej.

	dostarczane przez tych dostawców, naruszają niniejsze rozporządzenie. 4. Zadania organów nadzoru wyznaczonych zgodnie z ust. 1 obejmują w szczególności: a) współpracę z innymi organami nadzoru oraz udzielanie im pomocy zgodnie z art. 46c i 46e; b) żądanie informacji niezbędnych do monitorowania zgodności z niniejszym rozporządzeniem; c) informowanie odpowiednich właściwych organów wyznaczonych lub ustanowionych w danym państwie członkowskim zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 o wszelkich poważnych naruszeniach bezpieczeństwa lub utracie integralności, o których dowiedziały się w trakcie wykonywania swoich zadań oraz - w przypadku gdy poważne naruszenie lub utrata integralności dotyczą innych państw członkowskich - informowanie pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego w danym państwie członkowskim zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555 oraz pojedynczych punktów kontaktowych wyznaczonych w innych państwach członkowskich zgodnie z art. 46c ust. 1 niniejszego rozporządzenia, a także informowanie opinii publicznej lub zobowiązanie do tego dostawców europejskiego portfela tożsamości cyfrowej, w przypadku gdy organ nadzoru stwierdzi, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym; d) prowadzenie kontroli na miejscu i nadzoru zdalnego;				

	e) zobowiązywanie dostawców europejskich portfeli tożsamości cyfrowej do wyeliminowania wszelkich przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu; f) zawieszanie lub cofnięcie rejestracji oraz włączenia stron ufających do mechanizmu, o którym mowa w art. 5b ust. 7, w przypadku niezgodnego z prawem lub oszukańczego korzystania z europejskiego portfela tożsamości cyfrowej; g) współpracę z właściwymi organami nadzorczymi ustanowionymi na podstawie art. 51 rozporządzenia (UE) 2016/679, w szczególności poprzez informowanie ich, bez zbędnej zwłoki, w przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, a także informowanie ich o naruszeniach bezpieczeństwa, które przypuszczalnie stanowią naruszenie ochrony danych osobowych. 5. W przypadku gdy organ nadzoru wyznaczony zgodnie z ust. 1 zobowiązuje dostawcę europejskiego portfela tożsamości cyfrowej do wyeliminowania wszelkich przypadków niespełnienia wymogów wynikających z niniejszego rozporządzenia zgodnie z ust. 4 lit. e), a dostawca ten nie podejmuje odpowiednich działań, ani - w stosownych przypadkach - nie podejmuje ich w terminie wyznaczonym przez ten organ nadzoru, organ nadzoru wyznaczony zgodnie z ust. 1 może, mając na uwadze w szczególności zakres, czas trwania oraz skutki takiego niespełniania wymogów, nakazać temu dostawcy zawieszenie lub zaprzestanie dostarczania europejskiego portfela tożsamości cyfrowej. Organ nadzoru bez zbędnej				

	zwłoki informuje organy nadzoru z pozostałych państw członkowskich, Komisję, strony ufające oraz użytkowników europejskiego portfela tożsamości cyfrowej o decyzji nakazującej zawieszenie lub zaprzestanie dostarczania europejskiego portfela tożsamości cyfrowej.				
Art. 46a ust. 6	6. Do dnia 31 marca każdego roku każdy organ nadzoru wyznaczony zgodnie z ust. 1 przedkłada Komisji sprawozdanie ze swoich głównych działań w poprzednim roku kalendarzowym. Komisja udostępnia te coroczne sprawozdania Parlamentowi Europejskiemu i Radzie. 7. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, określi formaty i procedury w odniesieniu do sprawozdania, o którym mowa w ust. 6 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 46b ust. 1 i 2	**Nadzór nad usługami zaufania** 1. Państwa członkowskie wyznaczają organ nadzoru ustanowiony na ich terytorium lub wyznaczają - za obopólnym porozumieniem z innym państwem członkowskim - organ nadzoru z siedzibą w tym innym państwie członkowskim. Ten organ nadzoru odpowiedzialny jest za zadania nadzoru w wyznaczającym państwie członkowskim w odniesieniu do usług zaufania. Organy nadzoru wyznaczone zgodnie z akapitem pierwszym muszą otrzymać niezbędne uprawnienia i odpowiednie zasoby do wykonywania swoich zadań.	NIE	Obecnie obowiązujący art. 27 ust. 1 i ust. 2 pkt 1 i 9 ustawy o usługach zaufania oraz identyfikacji elektronicznej	Art. 27. 1. Nadzór nad dostawcami usług zaufania sprawuje minister właściwy do spraw informatyzacji. 2. W zakresie nadzoru, o którym mowa w ust. 1, minister właściwy do spraw informatyzacji: 1) wykonuje zadania określone w przepisach rozporządzenia 910/2014; (…) 9) wykonuje inne zadania określone w przepisach prawa.	W związku przeniesieniem przepisów o nadzorze na dostawcami usług zaufania z art. 17 rozporządzenia eIDAS do art. 46b bez zmiany ich merytorycznego znaczenia nie ma potrzeby zmian przepisów krajowych.

	2. Państwa członkowskie przekazują Komisji nazwy i adresy swoich organów nadzoru wyznaczonych zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie. Komisja publikuje wykaz zgłoszonych organów nadzoru.				
Art. 46b ust. 3, 4, 6 i 7	3. Rolą organów nadzoru wyznaczonych zgodnie z ust. 1 jest: a) sprawowanie nadzoru nad kwalifikowanymi dostawcami usług zaufania z siedzibą na terytorium wyznaczającego państwa członkowskiego oraz zapewnianie – za pomocą działań nadzorczych ex ante i ex post – aby określone w niniejszym rozporządzeniu wymogi były spełniane przez tych kwalifikowanych dostawców usług zaufania oraz przez świadczone przez nich kwalifikowane usługi zaufania; b) podejmowanie, w razie potrzeby, działań w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych *ex post* – gdy dowiedzą się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania przypuszczalnie nie spełniają wymogów określonych w niniejszym rozporządzeniu. 4. Zadania organu nadzoru wyznaczonego zgodnie z ust. 1 obejmują w szczególności: a) informowanie odpowiednich właściwych organów wyznaczonych lub ustanowionych w danym państwie członkowskim zgodnie z art. 8 ust. 1 dyrektywy (UE) 2022/2555 o wszelkich poważnych naruszeniach bezpieczeństwa lub utracie integralności, o których dowiedział się w trakcie	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	wykonywania swoich zadań oraz – w przypadku gdy poważne naruszenie lub utrata integralności dotyczą innych państw członkowskich – informowanie pojedynczego punktu kontaktowego wyznaczonego lub ustanowionego w danym państwie członkowskim zgodnie z art. 8 ust. 3 dyrektywy (UE) 2022/2555 oraz pojedynczych punktów kontaktowych wyznaczonych w innych państwach członkowskich zgodnie z art. 46c ust. 1 niniejszego rozporządzenia, a także informowanie opinii publicznej lub zobowiązanie do tego dostawcy usług zaufania, w przypadku gdy organ nadzoru stwierdzi, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym; b) współpracę z innymi organami nadzoru oraz udzielanie im pomocy zgodnie z art. 46c i 46e; c) analizowanie raportów z oceny zgodności, o których mowa w art. 20 ust. 1 i art. 21 ust. 1; d) składanie sprawozdań Komisji na temat swoich głównych działań zgodnie z ust. 6 niniejszego artykułu; e) przeprowadzanie audytów lub zwracanie się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania zgodnie z art. 20 ust. 2; f) współpracę z właściwymi organami nadzoru ustanowionymi zgodnie z art. 51 rozporządzenia (UE) 2016/679, w szczególności poprzez informowanie ich, bez zbędnej zwłoki, w przypadku podejrzenia naruszenia przepisów dotyczących ochrony danych osobowych, a także informowanie ich o naruszeniach bezpieczeństwa, które				

	przypuszczalnie stanowią naruszenie ochrony danych osobowych; g) przyznawanie dostawcom usług zaufania i świadczonym przez nich usługom statusu kwalifikowanego dostawcy usług zaufania i kwalifikowanych usług, a także odebranie tego statusu zgodnie z art. 20 i 21; h) informowanie organu odpowiedzialnego za krajową zaufaną listę, o której mowa w art. 22 ust. 3, o swoich decyzjach o przyznaniu lub odebraniu statusu kwalifikowanego, chyba że organ ten jest również organem nadzoru wyznaczonym zgodnie z ust. 1 niniejszego artykułu; i) sprawdzanie istnienia i prawidłowego stosowania postanowień dotyczących planów zakończenia działalności w przypadkach, gdy kwalifikowany dostawca usług zaufania zaprzestaje działalności, w tym sposobu, w jaki zapewnia się dalszą dostępność informacji zgodnie z art. 24 ust. 2 lit. h); j) zobowiązywanie dostawców usług zaufania do wyeliminowania wszelkich przypadków niespełnienia wymogów określonych w niniejszym rozporządzeniu; k) rozpatrywanie zgłoszeń wnoszonych przez dostawców przeglądarek internetowych zgodnie z art. 45a oraz w razie potrzeby podejmowanie działań. (…..) 6. Do dnia 31 marca każdego roku każdy organ nadzoru wyznaczony zgodnie z ust. 1 przedkłada Komisji sprawozdanie ze swoich głównych działań w poprzednim roku kalendarzowym. Komisja				

	udostępnia te coroczne sprawozdania Parlamentowi Europejskiemu i Radzie. 7. Do dnia 21 maja 2025 r. Komisja przyjmie wytyczne dotyczące wykonywania przez organy nadzoru wyznaczone zgodnie z ust. 1 zadań, o których mowa w ust. 4 niniejszego artykułu, oraz – w drodze aktów wykonawczych – określi formaty i procedury w odniesieniu do sprawozdania, o którym mowa w ust. 6 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 46b ust. 5	5. Państwa członkowskie mogą wymagać, aby organ nadzoru wyznaczony zgodnie z ust. 1 utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z prawem krajowym.	NIE	Obecnie obowiązujące przepisy rozdziału 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej	Rozdział 2 Krajowa infrastruktura zaufania Art. 2. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje: 1)rejestr dostawców usług zaufania, zwany dalej "rejestrem"; 2) zaufane listy; 3)narodowe centrum certyfikacji.	W związku przeniesieniem przepisów o nadzorze na dostawcami usług zaufania z art. 17 rozporządzenia eIDAS do art. 46b bez zmiany ich merytorycznego znaczenia nie ma potrzeby zmian w przepisach krajowych.
Art. 46c ust. 1-3	**Pojedyncze punkty kontaktowe** 1. Każde państwo członkowskie wyznacza pojedynczy punkt kontaktowy ds. usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów identyfikacji elektronicznej. 2. Każdy pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu ułatwienia współpracy	TAK	Art. 1 pkt 14 (Art. 23 pkt 18-19 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 18) wyznacza pojedynczy punkt kontaktowy do spraw usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej

	transgranicznej między organami nadzoru dla dostawców usług zaufania oraz między organami nadzoru dla dostawców europejskich portfeli tożsamości cyfrowej, a także, w stosownych przypadkach, z Komisją oraz Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz z innymi właściwymi organami w swoim państwie członkowskim. 3. Każde państwo członkowskie podaje do wiadomości publicznej oraz bez zbędnej zwłoki przekazuje Komisji nazwę i adres pojedynczego punktu kontaktowego wyznaczonego zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie.			identyfikacji elektronicznej o którym mowa art. 46c ust. 1 rozporządzenia 910/2014; 19) podaje do wiadomości publicznej oraz bez zbędnej zwłoki przekazuje Komisji nazwę i adres pojedynczego punktu kontaktowego, o którym mowa w pkt 18, oraz informacje o zmianach w tym zakresie;	Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 46c ust. 4	2. Każdy pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu ułatwienia współpracy transgranicznej między organami nadzoru dla dostawców usług zaufania oraz między organami nadzoru dla dostawców europejskich portfeli tożsamości cyfrowej, a także, w stosownych przypadkach, z Komisją oraz Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) oraz z innymi właściwymi organami w swoim państwie członkowskim. 3. Każde państwo członkowskie podaje do wiadomości publicznej oraz bez zbędnej zwłoki przekazuje Komisji nazwy i adresy pojedynczego punktu kontaktowego wyznaczonego zgodnie z ust. 1, oraz informacje o wszelkich późniejszych zmianach w tym zakresie. 4. Komisja publikuje wykaz pojedynczych punktów kontaktowych zgłoszonych zgodnie z ust. 3.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 46d	Wzajemna pomoc 1. W celu ułatwienia nadzoru i egzekwowania obowiązków wynikających z niniejszego rozporządzenia organy nadzoru wyznaczone zgodnie z art. 46a ust. 1 i art. 46b ust. 1 mogą zwracać się, w tym za pośrednictwem grupy współpracy ustanowionej na podstawie art. 46e ust. 1, o wzajemną pomoc do organów nadzoru w innym państwie członkowskim, w którym ma siedzibę dany dostawca europejskiego portfela tożsamości cyfrowej lub dany dostawca usług zaufania, lub w którym znajdują się jego sieć i systemy informatyczne lub świadczone są jego usługi. 2. Wzajemna pomoc oznacza co najmniej, że: a) organ nadzoru stosujący środki nadzoru i egzekwowania w jednym państwie członkowskim informuje organ nadzoru w innym zainteresowanym państwie członkowskim oraz prowadzi z nim konsultacje; b) organ nadzoru może zwrócić się do organu nadzoru innego zainteresowanego państwa członkowskiego o wprowadzenie środków nadzoru lub egzekwowania, w tym – na przykład – może zwrócić się z wnioskiem o przeprowadzenie kontroli dotyczących raportów z oceny zgodności, o których mowa w art. 20 i 21, w odniesieniu do świadczenia usług zaufania; c) w stosownych przypadkach organy nadzoru mogą prowadzić wspólne dochodzenia z organami nadzoru z innych państw członkowskich.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	Ustalenia i procedury dotyczące wspólnych działań, o których mowa w akapicie pierwszym, są uzgadniane i określane przez zainteresowane państwa członkowskie zgodnie z ich prawem krajowym. 3. Organ nadzoru, do którego kierowany jest wniosek o pomoc, może odrzucić ten wniosek z któregokolwiek z poniższych względów: a) pomoc, o którą się zwrócono, nie jest proporcjonalna do działań nadzorczych organu nadzoru prowadzonych zgodnie z art. 46a i 46b; b) organ nadzoru nie jest właściwy do udzielenia pomocy, której dotyczy wniosek; c) udzielenie pomocy, której dotyczy wniosek, byłoby niezgodne z niniejszym rozporządzeniem. 4. Do dnia 21 maja 2025 r., a następnie co dwa lata grupa współpracy ustanowiona na podstawie art. 46e ust. 1 wydaje wytyczne dotyczące aspektów organizacyjnych i procedur wzajemnej pomocy, o której mowa w ust. 1 i 2 niniejszego artykułu.				
Art. 46e ust. 1	Grupa Współpracy na rzecz Europejskiej Tożsamości Cyfrowej 1. W celu wspierania i ułatwiania transgranicznej współpracy państw członkowskich oraz wymiany informacji dotyczących usług zaufania, europejskich portfeli tożsamości cyfrowej i notyfikowanych systemów identyfikacji elektronicznej Komisja ustanawia Grupę Współpracy na rzecz Europejskiej Tożsamości Cyfrowej (zwaną dalej »grupą współpracy«).	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 46e ust. 2	Grupa Współpracy na rzecz Europejskiej Tożsamości Cyfrowej (…) 2. Grupa współpracy składa się z przedstawicieli mianowanych przez państwa członkowskie oraz przez Komisję. Grupie współpracy przewodniczy Komisja., Komisja zapewnia również obsługę sekretariatu grupy współpracy.	TAK	Art. 1 pkt 14 (Art. 23 pkt 15 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 15) wyznacza przedstawicieli do grupy współpracy;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 46e ust. 3-7	3. Do udziału w posiedzeniach grupy współpracy i uczestnictwa w jej pracach w charakterze obserwatorów mogą być zapraszani – na zasadzie ad hoc – przedstawiciele odpowiednich zainteresowanych stron. 4. Do udziału w pracach grupy współpracy w charakterze obserwatora zapraszana jest ENISA, gdy grupa współpracy przeprowadza wymianę poglądów, najlepszych praktyk i informacji w odniesieniu do istotnych aspektów cyberbezpieczeństwa, takich jak zgłaszanie przypadków naruszenia bezpieczeństwa, a także gdy rozpatrywane są kwestie stosowania certyfikatów lub norm cyberbezpieczeństwa. 5. Grupa współpracy ma następujące zadania:	NIE/TAK	Art. 1 pkt 14 (Art. 23 pkt 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: 1) koordynuje działania na poziomie krajowym na rzecz współpracy z państwami członkowskimi Unii Europejskiej w sprawach dotyczących systemów identyfikacji elektronicznej, prowadzonej zgodnie z art. 46e rozporządzenia 910/2014; (…)	Przepis stosowany wprost, poza obowiązkiem wynikającym z ust. 6. Zasadne jest wyznaczenie ministra do spraw informatyzacji jako podmiotu zapewniającego skuteczną i efektywną współpracę wyznaczonych przedstawicieli w Grupie Współpracy.

	a) wymiana porad oraz współpraca z Komisją w zakresie nowych inicjatyw politycznych w dziedzinie portfeli tożsamości cyfrowej, środków identyfikacji elektronicznej i usług zaufania; b) doradzanie Komisji, w stosownych przypadkach, na wczesnym etapie przygotowywania projektów aktów wykonawczych i delegowanych, które mają zostać przyjęte na podstawie niniejszego rozporządzenia; c) w celu wspierania organów nadzoru w wykonywaniu przepisów niniejszego rozporządzenia: (i) wymiana najlepszych praktyk i informacji dotyczących wykonywania przepisów niniejszego rozporządzenia; (ii) ocena istotnych zmian w obszarach portfela tożsamości cyfrowej, identyfikacji elektronicznej i usług zaufania; (iii) organizowanie regularnych wspólnych spotkań z odpowiednimi zainteresowanymi stronami z całej Unii, aby dyskutować na temat działań prowadzonych przez grupę współpracy oraz zbierać informacje o nowych wyzwaniach politycznych; (iv) wymiana poglądów, najlepszych praktyk i informacji na temat odpowiednich aspektów cyberbezpieczeństwa europejskich portfeli tożsamości cyfrowej, systemów identyfikacji elektronicznej oraz usług zaufania – przy wsparciu ze strony ENISA; (v) wymiana najlepszych praktyk w odniesieniu do opracowywania i wdrażania polityki zgłaszania				

	naruszeń bezpieczeństwa, o których mowa w art. 5e i 10; (vi) organizacja wspólnych spotkań z grupą współpracy ds. bezpieczeństwa sieci i informacji ustanowioną zgodnie z art. 14 ust. 1 dyrektywy (UE) 2022/2555 w celu wymiany istotnych informacji dotyczących usług zaufania i identyfikacji elektronicznej powiązanych cyberzagrożeń, incydentów, podatności na zagrożenia, inicjatyw na rzecz podnoszenia świadomości, szkoleń, ćwiczeń i umiejętności, budowania zdolności w zakresie norm i specyfikacji technicznych, a także norm i specyfikacji technicznych; (vii) dyskutowanie, na wniosek organu nadzoru, na temat konkretnych wniosków o pomoc wzajemną, o której mowa w art. 46d; (viii) ułatwianie wymiany informacji między organami nadzoru poprzez udzielanie wskazówek dotyczących aspektów organizacyjnych i procedur wzajemnej pomocy, o której mowa w art. 46d; d) organizacja wzajemnej oceny systemów identyfikacji elektronicznej podlegających notyfikacji zgodnie z niniejszym rozporządzeniem. 6. Państwa członkowskie zapewniają skuteczną i efektywną współpracę swoich wyznaczonych przedstawicieli w grupie współpracy. 7. Do dnia 21 maja 2025 r. Komisja, w drodze aktów wykonawczych, ustanowi niezbędne ustalenia proceduralne w celu ułatwienia współpracy między państwami członkowskimi, o której mowa w ust. 5 lit. d) niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z				

	procedurą sprawdzającą, o której mowa w art. 48 ust. 2.				
Art. 47 ust. 2, 3 i 5	2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 5c ust. 8, art. 24 ust. 4b i art. 30 ust. 4, powierza się Komisji na czas nieokreślony od dnia 17 września 2014 r. 3. Przekazanie uprawnień, o których mowa w art. 5c ust. 8, art. 24 ust. 4b i art. 30 ust. 4, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych. (….) 5. Akt delegowany przyjęty na podstawie art. 5c ust. 8, art. 24 ust. 4b lub art. 30 ust. 4 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Art. 48a	**Wymogi dotyczące sprawozdawczości** 1. Państwa członkowskie zapewniają zbieranie danych statystycznych dotyczących funkcjonowania	TAK	Art. 1 pkt 14 (Art. 23 pkt 20 ustawy o	Art. 23. Minister właściwy do spraw informatyzacji:	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4

	europejskich portfeli tożsamości cyfrowej oraz kwalifikowanych usług zaufania dostarczanych lub świadczonych na ich terytorium. 2. Dane statystyczne zbierane zgodnie z ust. 1 obejmują następujące elementy: a) liczbę osób fizycznych i prawnych posiadających ważny europejski portfel tożsamości cyfrowej; b) rodzaj i liczbę usług akceptujących używanie europejskiego portfela tożsamości cyfrowej; c) liczbę skarg użytkowników i incydentów związanych z ochroną konsumentów lub ochroną danych w odniesieniu do stron ufających i kwalifikowanych usług zaufania; d) zestawienie zawierające dane dotyczące incydentów uniemożliwiających używanie europejskiego portfela tożsamości cyfrowej; e) podsumowanie poważnych incydentów związanych z bezpieczeństwem, naruszeń ochrony danych i użytkowników europejskich portfeli tożsamości cyfrowej lub kwalifikowanych usług zaufania, których to dotyczy. 3. Dane statystyczne, o których mowa w ust. 2, udostępnia się publicznie w otwartym i powszechnie używanym formacie nadającym się do odczytu maszynowego. 4. Do dnia 31 marca każdego roku państwa członkowskie przedkładają Komisji sprawozdanie dotyczące danych statystycznych zebranych zgodnie z ust. 2."		usługach zaufania oraz identyfikacji elektronicznej)	(…) 20) wykonuje obowiązki o których mowa w art. 48a rozporządzenia 910/2014.”;	września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.

Art. 49	**Przegląd** 1. Komisja dokonuje przeglądu stosowania niniejszego rozporządzenia i do dnia 21 maja 2026 r. przedłoży sprawozdanie Parlamentowi Europejskiemu i Radzie. W sprawozdaniu tym Komisja oceni w szczególności, czy należy zmienić zakres stosowania niniejszego rozporządzenia lub jego poszczególnych przepisów, w tym – w szczególności – przepisów zawartych w art. 5c ust. 5, biorąc pod uwagę doświadczenia zdobyte przy stosowaniu niniejszego rozporządzenia, a także rozwój technologiczny, sytuację rynkową i prawną. W razie potrzeby do sprawozdania dołącza się wniosek dotyczący zmiany niniejszego rozporządzenia. 2. Sprawozdanie, o którym mowa w ust. 1, obejmuje ocenę dostępności, bezpieczeństwa i użyteczności notyfikowanych środków identyfikacji elektronicznej oraz europejskich portfeli tożsamości cyfrowej objętych zakresem stosowania niniejszego rozporządzenia, oraz ocenę, czy wszyscy prywatni dostawcy usług online korzystający z usług identyfikacji elektronicznej świadczonych przez strony trzecie do celów uwierzytelniania użytkowników muszą zostać zobowiązani do akceptowania wykorzystywania notyfikowanych środków identyfikacji elektronicznej i europejskiego portfela tożsamości cyfrowej. 3. Do dnia 21 maja 2030 r., a następnie co cztery lata Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie z postępów w osiąganiu celów niniejszego rozporządzenia.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 51	**Środki przejściowe** 1. Bezpieczne urządzenia do składania podpisu, których zgodność ustalono zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE, w dalszym ciągu uznaje się za kwalifikowane urządzenia do składania podpisu elektronicznego na podstawie niniejszego rozporządzenia do dnia 21 maja 2027 r. 2. Kwalifikowane certyfikaty wydane osobom fizycznym na podstawie dyrektywy 1999/93/WE w dalszym ciągu uznaje się za kwalifikowane certyfikaty podpisów elektronicznych na podstawie niniejszego rozporządzenia do dnia 21 maja 2026 r. 3. Zarządzanie kwalifikowanymi urządzeniami do składania podpisów i pieczęci elektronicznych na odległość przez kwalifikowanych dostawców usług zaufania, innych niż kwalifikowani dostawcy usług zaufania świadczący kwalifikowane usługi zaufania na potrzeby zarządzania kwalifikowanymi urządzeniami do składania podpisów i pieczęci elektronicznych na odległość zgodnie z art. 29a i 39a, może być prowadzone, bez konieczności uzyskania statusu kwalifikowanego do celów świadczenia tych usług zarządzania, do dnia 21 maja 2026 r. 4. Kwalifikowani dostawcy usług zaufania, którym na podstawie niniejszego rozporządzenia przyznano status kwalifikowany przed dniem 20 maja 2024 r., przedkładają organowi nadzoru raport z oceny zgodności potwierdzający zgodność z art. 24 ust. 1, 1a i 1b najszybciej jak to możliwe, nie później jednak niż w dniu 21 May 2026 r.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

Art. 2	**Wejście w życie** Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*. Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.
Załączniki I-IV	**Załącznik I** W załączniku I do rozporządzenia (UE) nr 910/2014 lit. (i) otrzymuje brzmienie: ,, i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu;" **Załącznik II** W załączniku II do rozporządzenia (UE) nr 910/2014, uchyla się pkt 3 i 4. **Załącznik III** W załączniku III do rozporządzenia (UE) nr 910/2014 lit. i) otrzymuje brzmienie: ,, i) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu;" **Załącznik IV** W załączniku IV do rozporządzenia (UE) nr 910/2014 wprowadza się następujące zmiany: 1) lit. c) otrzymuje brzmienie:,, c) w odniesieniu do osób fizycznych: co najmniej imię i nazwisko osoby, której wydano certyfikat, lub pseudonim; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane;ca)w odniesieniu do osób prawnych: niepowtarzalny	NIE			Załącznik stosowany wprost, nie wymaga wdrożenia.

	zestaw danych jednoznacznie reprezentujących osobę prawną, której wydano certyfikat, zawierający co najmniej nazwę osoby prawnej, której wydawany jest certyfikat oraz – w stosownych przypadkach – numer rejestrowy zgodnie z oficjalnym rejestrem;" 2) lit. j) otrzymuje brzmienie:,, j) informacje na temat statusu ważności kwalifikowanego certyfikatu lub miejsce usług statusu ważności certyfikatu, w którym można dowiedzieć się o statusie ważności kwalifikowanego certyfikatu.				
Załącznik V	**Załącznik V** **WYMOGI DOTYCZĄCE KWALIFIKOWANEGO ELEKTRONICZNEGO POŚWIADCZENIA ATRYBUTÓW** Kwalifikowane elektroniczne poświadczenie atrybutów musi zawierać: a) wskazanie – co najmniej w formie nadającej się do automatycznego przetwarzania – że dane poświadczenie zostało wydane jako kwalifikowane elektroniczne poświadczenie atrybutów; b) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane elektroniczne poświadczenia atrybutów, obejmujący co najmniej państwo członkowskie, w którym dostawca ma siedzibę, oraz: (i) w odniesieniu do osoby prawnej: nazwę oraz – w stosownym przypadku – numer rejestrowy zgodnie z oficjalnym rejestrem,	NIE			Załącznik stosowany wprost, nie wymaga wdrożenia.

	(ii) w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby; c) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane; d) poświadczony atrybut lub poświadczone atrybuty, w tym – w stosownych przypadkach – informacje niezbędne do określenia zakresu tych atrybutów; e) szczegółowe dane dotyczące początku i końca okresu ważności poświadczenia; f) kod identyfikacyjny poświadczenia, który musi być niepowtarzalny dla kwalifikowanego dostawcy usług zaufania, oraz – w stosownych przypadkach – wskazanie systemu poświadczeń, którego częścią jest dane poświadczenie atrybutów; g) kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania; h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej, o których mowa w lit. g); i) informacje na temat statusu ważności kwalifikowanego poświadczenia lub miejsce usług, w którym można dowiedzieć się o statusie ważności kwalifikowanego poświadczenia.				
Załącznik VI	**Załącznik VI** **MINIMALNY WYKAZ ATRYBUTÓW**	TAK	Art. 1 pkt 13 (Art. 22c ust 1 ustawy o	Art. 22c. 1. Podmioty sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014,	Przeniesiono ogólne wymagania rozporządzenia eIDAS

	Zgodnie z art. 45e państwa członkowskie zapewniają, aby wprowadzono środki umożliwiające kwalifikowanym dostawcom usług zaufania, którzy dostarczają kwalifikowane elektroniczne poświadczenia atrybutów weryfikację drogą elektroniczną, na żądanie użytkownika, autentyczności następujących atrybutów w zestawieniu z odpowiednim źródłem autentycznym na poziomie krajowym lub poprzez wyznaczonych pośredników uznanych na poziomie krajowym zgodnie z prawem Unii lub prawem krajowym oraz w przypadku gdy atrybuty te polegają na źródłach autentycznych w sektorze publicznym: 1) adres; 2) wiek; 3) płeć; 4) stan cywilny; 5) skład rodziny; 6) narodowość lub obywatelstwo; 7) wykształcenie, tytuły i licencje; 8) kwalifikacje zawodowe, tytuły i licencje; 9) pełnomocnictwa i upoważnienia do reprezentowania osób fizycznych lub prawnych; 10) publicznoprawne zezwolenia i licencje; 11) w odniesieniu do osób prawnych – dane finansowe i dane dotyczące przedsiębiorstwa.		usługach zaufania oraz identyfikacji elektronicznej)	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.	do prawa krajowego ponieważ cały czas powstają kolejne źródła autentyczne w rozumieniu załącznika VI tego rozporządzenia. Ich wymienianie w ustawie o usługach zaufania oraz identyfikacji elektronicznej powodowałby konieczność ciągłych zmian tej ustawy. W związku z tym, że rozporządzenie eIDAS obowiązuje bezpośrednio, nie ma takiej potrzeby.
Załącznik nr VII	**Załącznik VII** **WYMOGI DOTYCZĄCE ELEKTRONICZNEGO POŚWIADCZENIA ATRYBUTÓW**	NIE			Załącznik stosowany wprost, nie wymaga wdrożenia.

	WYDAWANEGO PRZEZ PODMIOT PUBLICZNY ODPOWIEDZIALNY ZA ŹRÓDŁO AUTENTYCZNE LUB W JEGO IMIENIU Elektroniczne poświadczenie atrybutów wydawane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu musi zawierać: a) wskazanie – co najmniej w formie nadającej się do automatycznego przetwarzania– że poświadczenie zostało wydane jako elektroniczne poświadczenie atrybutów wydawane przez podmiot publiczny odpowiedzialny za źródło autentyczne lub w jego imieniu; b) zestaw danych jednoznacznie reprezentujących podmiot publiczny wydający elektroniczne poświadczenie atrybutów, w tym co najmniej państwo członkowskie, w którym ten podmiot publiczny ma siedzibę, oraz nazwę podmiotu oraz, w stosownych przypadkach, jego numer rejestrowy zgodnie z oficjalnym rejestrem; c) zestaw danych jednoznacznie reprezentujących podmiot, do którego poświadczone atrybuty się odnoszą; w przypadku gdy używany jest pseudonim, musi to być wyraźnie wskazane; d) poświadczony atrybut lub poświadczone atrybuty, w tym – w stosownych przypadkach – informacje niezbędne do określenia zakresu tych atrybutów; e) szczegółowe dane dotyczące początku i końca okresu ważności poświadczenia; f) kod identyfikacyjny poświadczenia, który musi być niepowtarzalny dla wydającego podmiotu publicznego, oraz – w stosownych przypadkach –				

	wskazanie systemu poświadczeń, którego częścią jest dane poświadczenie atrybutów; g) kwalifikowany podpis elektroniczny lub kwalifikowaną pieczęć elektroniczną wydającego podmiotu; h) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący kwalifikowanemu podpisowi elektronicznemu lub kwalifikowanej pieczęci elektronicznej, o których mowa w lit. g); (i) informacje na temat statusu ważności poświadczenia lub miejsce usług, w którym można dowiedzieć się o statusie ważności poświadczenia.				
„Rozporządzenie 2024/2977”.					
Art. 3 ust. 4 oraz Załącznik. Tabela 1. Obowiązkowe dane identyfikujące osobę w przypadku osoby fizycznej.	4. Państwa członkowskie zapewniają, aby dane identyfikujące osobę wydane danemu użytkownikowi portfela były niepowtarzalne na poziomie danego państwa członkowskiego.	TAK	Art. 7 pkt 4 (Art. 14a ust. 2 pkt 5 ustawy o aplikacji mObywatel)	2. Europejski portfel tożsamości cyfrowej, zawiera zestaw danych identyfikujących osobę fizyczną, obejmujący: (…) 5) numer PESEL	Numer PESEL jest identyfikatorem jednoznacznie identyfikującym osobę fizyczną nadawanym osobie, której dane są gromadzone w rejestrze PESEL i rejestrze mieszkańców. Zestaw obowiązkowych danych identyfikujących osobę fizyczną przewidziany w załączniku nie zapewnia niepowtarzalności na poziomie danego państwa członkowskiego.

Art. 3 ust. 6	6. Państwa członkowskie udostępniają publicznie wykaz rozwiązań w zakresie portfela obsługiwanych przez dostawców danych identyfikujących osobę, które są częścią systemów identyfikacji elektronicznej tego państwa członkowskiego.	TAK	Art. 4 pkt 2 (Art. 20aa ust. 1 lit. d ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2025 r. poz. 1703), zwanej dalej ustawą o informatyzacji działalności podmiotów realizujących zadania publiczne) Art. 7 pkt 4 (Art. 14a ust. 1 pkt 4 ustawy o aplikacji mObywatel)	Art. 20aa.1. Minister właściwy do spraw informatyzacji odpowiada za funkcjonowanie systemu teleinformatycznego, który: 1) zapewnia obsługę publicznego systemu identyfikacji elektronicznej, w którym wydawany jest: (…) „d) europejski portfel tożsamości cyfrowej, o którym mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel”, „Art. 14a. 1. Minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, w tym: (…) 4) dane identyfikujących osobę, o których mowa w ust. 2 i powiązanie tych danych z europejskim portfelem tożsamości cyfrowej.	Rozwiązania w zakresie europejskiego portfela tożsamości cyfrowej obsługiwanych przez dostawców danych identyfikujących osobę, będą wynikały z przepisów prawa i co za tym idzie będą publicznie dostępne

			(Art. 14b ust. 9-11 ustawy o aplikacji mObywatel)	9. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, szczegółowe warunki organizacyjno-techniczne, jakie spełnia punkt potwierdzający tożsamość, o którym mowa w ust. 1 pkt 3, oraz szczegółowe przypadki, w których ten punkt nie potwierdza tożsamości, mając na względzie zapewnienie odpowiedniego poziomu bezpieczeństwa i pewności w procesie potwierdzania tożsamości oraz poufności kluczowych elementarnych czynności. 10. Minister właściwy do spraw informatyzacji może określić w drodze rozporządzenia wymagania dotyczące weryfikacji tożsamości o której mowa w ust. 1 pkt 2, mając na uwadze specyfikację techniczną ETSI TS 119 461 oraz wymogi określone w rozporządzeniu 2015/1502. 11. Minister właściwy do spraw informatyzacji może określić w drodze rozporządzenia wymagania dotyczące weryfikacji tożsamości, o której mowa w ust. 1 pkt 4, mając na uwadze specyfikację techniczną ETSI TS 119 461 oraz wymogi określone w rozporządzeniu 2015/1502	

Art. 3 ust. 7	Państwa członkowskie wprowadzają do systemu użytkowników portfela zgodnie z określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 wymogami dotyczącymi wprowadzania do systemu na wysokim poziomie bezpieczeństwa. Podczas wprowadzania do systemu - przed wydaniem danych identyfikujących osobę jednostce portfela odpowiedniego użytkownika portfela - dostawcy danych identyfikujących osobę przeprowadzają weryfikację tożsamości użytkownika portfela zgodnie z wymogami w zakresie sprawdzania i weryfikacji tożsamości.	TAK	Art. 7 pkt 4 (Art. 14b ust. 1 ustawy o aplikacji mObywatel)	Art. 14b. 1. Użytkownikiem europejskiego portfela tożsamości cyfrowej, może zostać osoba fizyczna, która została uwierzytelniona w jeden z następujących sposobów: 1) za pomocą profilu osobistego albo; 2) za pomocą wydawanego w Polsce środka identyfikacji elektronicznej, dla którego potwierdzono spełnienie wymagań dla średniego poziomu bezpieczeństwa, z dodatkową weryfikacją tożsamości spełniającą wymagania określone w rozporządzeniu wykonawczym Komisji (UE) 2026/798 z dnia 7 kwietnia 2026 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi	Zapewnienie weryfikacji tożsamości użytkowników w sposób zgodny z wymogami dla wysokiego poziomu bezpieczeństwa.

				wysokiego poziomu bezpieczeństwa ((Dz. Urz. UE L 2026/798 z 08.04.2026)), określoną w przepisach wydanych na podstawie ust. 4, albo 3) w punkcie potwierdzającym tożsamość podczas obecności fizycznej osoby ubiegającej się o wydanie europejskiego portfela tożsamości cyfrowej po okazaniu dokumentu stwierdzającego tożsamość i obywatelstwo, który zawiera dowody identyfikacji fotograficznej lub biometrycznej, o których mowa w załączniku do rozporządzenia wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L 235z 09.09.2015, z późn. zm.), zwanego dalej „rozporządzeniem 2015/1502”, umożliwiające potwierdzenie deklarowanej	

				tożsamości, celem porównania co najmniej jednej cechy fizycznej osoby, której tożsamość jest weryfikowana, albo	
			Art. 7 pkt 4 (Art. 14c ustawy o aplikacji mObywatel)	4) z wykorzystaniem innej metody weryfikacji tożsamości, określonej w przepisach wydanych na podstawie ust. 10. Art. 14c. 1. Użytkownikiem europejskiego portfela tożsamości cyfrowej osoby prawnej może zostać: 1) osoba fizyczna po uwierzytelnieniu za pomocą europejskiego portfela tożsamości cyfrowej, wydanego tej osobie oraz kwalifikowanego elektronicznego poświadczenia atrybutów poświadczającego pełnomocnictwo tej osoby do posługiwania się europejskim portfelem tożsamości cyfrowej osoby prawnej; 2) osoba fizyczna wskazana we wniosku osoby prawnej złożonym do ministra właściwego do spraw informatyzacji za pomocą usługi online udostępnianej przez tego ministra; 3) osoba fizyczna prowadząca działalność gospodarczą po uwierzytelnieniu za pomocą	

				europejskiego portfela tożsamości cyfrowej. 2. Wniosek, o którym mowa w ust. 1 pkt 2, zawiera: 1) nazwę i odpowiednio numer KRS lub numer w Katalogu Podmiotów Publicznych wnioskującej osoby prawnej, dla której ma być wydany europejski portfel tożsamości cyfrowej; 2) imię (imiona), nazwisko i numer PESEL osoby fizycznej uprawnionej do dysponowania europejskim portfelem tożsamości cyfrowej osoby prawnej. 3. Wniosek, o którym mowa w ust. 1 pkt 2, opatruje się kwalifikowanym podpisem elektronicznym osoby lub osób, które są uprawnione do zarządzania osobą prawną. 4. Minister właściwy do spraw informatyzacji umożliwia użytkownikowi europejskiego portfela tożsamości cyfrowej za pomocą którego została potwierdzona tożsamość, pobranie danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą odpowiednio z Krajowego Rejestru Sądowego, Katalogu Podmiotów Publicznych lub Centralnej Ewidencji i Informacji	

				o Działalności Gospodarczej oraz zapewnia kryptograficznie powiązanie tych danych z europejskim portfelem tożsamości cyfrowej. 5. Europejski portfel tożsamości cyfrowej osoby prawnej jest powiązany z europejskim portfelem tożsamości cyfrowej osoby fizycznej dysponującej tym portfelem w taki sposób, że użycie europejskiego portfela tożsamości cyfrowej osoby prawnej wymaga uprzedniego uwierzytelnienia użytkownika europejskiego portfela tożsamości cyfrowej osoby fizycznej, który jest powiązany z tym portfelem; 6. Powiązanie, o którym mowa w ust. 5 może być cofnięte: 1) przez ministra właściwego do spraw informatyzacji na wniosek osoby prawnej, dla której wydano portfel; 2) przez osobę fizyczną, której europejski portfel tożsamości cyfrowej jest powiązany z tym europejskim portfelem tożsamości cyfrowej osoby prawnej; 3) w przypadku unieważnienia poświadczeń jednostki portfela, o	

				którym mowa w art. 7 rozporządzenia 2024/2979; 4) w przypadkach, o których mowa w art. 5a ust. 9 lit. b i c rozporządzenia 910/2014; 5) na żądanie unieważnienia, przez użytkownika portfela, poświadczeń jednostki portfela, o którym mowa w art. 6 ust. 3 lit. c rozporządzenia 2024/2979. 7. Osoba prawna, której wydano dane identyfikujące do europejskiego portfela tożsamości cyfrowej lub osoba fizyczna będąca użytkownikiem europejskiego portfela tożsamości cyfrowej osoby prawnej, może cofnąć powiązanie danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą z europejskim portfelem tożsamości cyfrowej, o którym mowa w art. 14a ust. 1. Cofnięcie powiązania oznacza unieważnienie europejskiego portfela tożsamości cyfrowej osoby prawnej. 8. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia szczegółowy, sposób powiązania, o którym mowa w ust. 5, oraz szczegółowy sposób	

<table>
<tr><td></td><td colspan="3"></td><td></td><td></td><td>cofnięcia takiego powiązania, o którym mowa w ust. 6, uwzględniając wymogi określone w załączniku do rozporządzeniu 2015/1502.</td><td></td></tr>
<tr><td rowspan="5">Załącznik. Tabela 1. Obowiązkowe dane identyfikujące osobę w przypadku osoby fizycznej.</td><td>Identyfikator danych</td><td>Definicja</td><td>Występowan</td><td rowspan="5">TAK</td><td rowspan="5">Art.7 pkt 4
(Art. 14a ust. 2 pkt 1-4 i 6 oraz ust. 5 ustawy o aplikacji mObywatel)</td><td rowspan="5">2. Europejski portfel tożsamości cyfrowejzawiera zestaw danych identyfikujących osobę fizyczną, obejmujący:
1) imię (imiona);
2) nazwisko;
3) datę urodzenia;
4) miejsce urodzenia;
(…)
6) obywatelstwo;
(…)
5. Dane, o których mowa, w ust. 2:
1) pkt 1-8 – są pobierane automatycznie z rejestru PESEL,
2) pkt 9 – są pobierane automatycznie z Rejestru Dowodów Osobistych lub, jeżeli nie jest to możliwe, z dokumentu potwierdzającego tożsamość spełniającego zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, określone w dokumencie - Doc 9303 Machine</td><td rowspan="5">Realizacja wymogu uwzględnienia obowiązkowych elementów danych.
Dane będą zgodne z danymi z rejestru PESEL.</td></tr>
<tr><td>family_name</td><td>Aktualne nazwisko (nazwiska) użytkownika, którego dotyczą dane identyfikujące osobę.</td><td>Obowiązkow</td></tr>
<tr><td>given_name</td><td>Aktualne imię (imiona), w tym, w stosownych przypadkach, drugie imię (imiona) użytkownika, którego dotyczą dane identyfikujące osobę.</td><td>Obowiązkow</td></tr>
<tr><td>birth_date</td><td>Dzień, miesiąc i rok urodzenia użytkownika, którego dotyczą dane identyfikujące osobę.</td><td>Obowiązkow</td></tr>
<tr><td>birth_place</td><td>Państwo zgodnie z kodem państwa alpha-2 według normy ISO 3166-1 lub stan, prowincja, powiat, obszar lokalny, gmina, miasto, miejscowość lub wieś urodzenia użytkownika, do którego odnoszą się dane identyfikujące osobę.</td><td>Obowiązkow</td></tr>
</table>

	nationality	Co najmniej jeden kod państwa alfa-2 według normy ISO 3166-1, odzwierciedlający obywatelstwo użytkownika, którego dotyczą dane identyfikujące osobę.	Obowiązkow			Readable Travel Documents część 10, 11 i 12 – po potwierdzeniu tożsamości w sposób określony w art. 14b ust. 1.	
Załącznik. Tabela 2. Opcjonalne dane identyfikujące osobę w przypadku osoby fizycznej	Identyfikator danych	Definicja	Występowan	NIE	Art. 7 pkt 4 (Art. 14a ust. 2 pkt 5 i 7-9 oraz ust. 5 ustawy o aplikacji mObywatel)	2. Europejski portfel tożsamości cyfrowej, o którym mowa w ust. 1, zawiera zestaw danych identyfikujących osobę fizyczną, obejmujący: (…) 5) nr PESEL (…) 7) płeć; 8) nazwisko rodowe jeżeli występuje w rejestrze PESEL; 9) fotografię obejmującą wizerunek twarzy użytkownika europejskiego portfela tożsamości cyfrowej zgodną z wymaganiami określonymi w załączniku do rozporządzenia wykonawczego Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. w sprawie ustanowienia zasad stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych	Numer PESEL jako element zestawu danych identyfikujących osobę jest konieczny, aby europejski portfel tożsamości cyfrowej był użyteczny. Dane o płci są wynikową konsekwencją nr PESEL, który zawiera oznaczenie płci. Nazwisko rodowe jest elementem wykorzystywanym przy dodatkowym potwierdzaniu tożsamości w niektórych krajowych usługach online. Dane będą zgodne z danymi z rejestru PESEL
	Resident address	Pełny adres zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę, pod którym użytkownik ten obecnie przebywa lub można się z nim skontaktować (ulica, numer domu, miasto itp.).	Opcjonalne				
	Resident country	Kraj, w którym obecnie zamieszkuje użytkownik, którego dotyczą dane identyfikujące osobę, wyrażony jako kod państwa alfa-2 według normy ISO 3166-1.	Opcjonalne				
	Resident state	Stan, prowincja, powiat lub obszar lokalny aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.	Opcjonalne				

	Resident city	Gmina, miasto lub wieś aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.	Opcjonalne			identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz. Urz. UE L 2024/2977 z 04.12.2024) 5. Dane, o których mowa, w ust. 2: 1) pkt 1-8 – są pobierane automatycznie z rejestru PESEL, 2) pkt 9 – są pobierane automatycznie z Rejestru Dowodów Osobistych lub, jeżeli nie jest to możliwe, z dokumentu potwierdzającego tożsamość spełniającego zalecenia Organizacji Międzynarodowego Lotnictwa Cywilnego, określone w dokumencie - Doc 9303 Machine Readable Travel Documents część 10, 11 i 12 – po potwierdzeniu tożsamości w sposób określony w art. 14b ust. 1.	Fotografia twarzy użytkownika portfela jest elementem podwyższającym bezpieczeństwo w przypadku użycia portfela podczas obecności fizycznej. Dane będą pobierane z Rejestru Dowodów Osobistych lub z dokumentów potwierdzających tożsamość.
	Resident postal code	Kod pocztowy miejsca aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.	Opcjonalne				
	Resident street	Nazwa ulicy aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę.	Opcjonalne				
	resident_house number	Numer domu, w którym aktualnie mieszka użytkownik, którego dotyczą dane identyfikujące osobę, w tym wszelkie informacje uzupełniające.	Opcjonalne				
	Personal administrative number	Wartość przypisana osobie fizycznej, która jest niepowtarzalna wśród wszystkich osobistych numerów administracyjnych wydanych przez dostawcę danych identyfikujących osobę. W przypadku gdy państwa	Opcjonalne				

		członkowskie zdecydują się na włączenie tego atrybutu, mają obowiązek opisać w swoich systemach identyfikacji elektronicznej, w ramach których wydawane są dane identyfikujące osobę, politykę, którą stosują do wartości tego atrybutu, w tym, w stosownych przypadkach, szczególne warunki przetwarzania tej wartości.				
	portrait	Wizerunek twarzy użytkownika portfela zgodny ze specyfikacjami ISO 19794-5 lub ISO 39794	Opcjonalne			
	Family name birth	Nazwisko (nazwiska) użytkownika danych identyfikujących osobę w momencie urodzenia.	Opcjonalne			
	Given name birth	Imię (imiona), w tym drugie imię (imiona) użytkownika danych identyfikujących osobę w momencie urodzenia.	Opcjonalne			
	sex	Dopuszcza się jedną z następujących wartości: 0 = nieznana;	Opcjonalne			

		1 = mężczyzna; 2 = kobieta; 3 = inna; 4 = osoba interseksualna; 5 = różnorodna; 6 = otwarta; 9 = nie dotyczy; W odniesieniu do wartości 0, 1, 2 i 9 stosuje się normę ISO/IEC 5218.					
	Email address	Adres poczty elektronicznej użytkownika, którego dotyczą dane identyfikujące osobę [zgodny z formatem RfC 5322].	Opcjonalne				
	Mobile phone number	Numer telefonu komórkowego użytkownika, którego dotyczą dane identyfikujące osobę, rozpoczynający się do symbolu "+" jako kodu prefiksu międzynarodowego i kodu państwa, po którym występują tylko cyfry	Opcjonalne				
Załącznik. Tabela 3.	aktualna nazwa prawna		Obowiązkow	TAK	Art. 7 pkt 4	3. Europejski portfel tożsamości cyfrowej, zawiera zestaw danych	Realizacja wymogu uwzględnienia

Obowiązkowe dane identyfikujące osobę w przypadku osoby prawnej.	niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy w czasie.	Obowiązkow		(Art. 14a ust. 3 pkt 1-2 ustawy o aplikacji mObywatel)	identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą, obejmujący: 1) nazwę (firmę) zgodną z odpowiednim wpisem do: a) Centralnej Ewidencji i Informacji o Działalności Gospodarczej, b) Krajowego Rejestru Sądowego, c) Katalogu Podmiotów Publicznych, o którym mowa w art. 20u ust. 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, zwanego dalej „Katalogiem Podmiotów Publicznych”; 2) numer identyfikacji podatkowej (NIP);	obowiązkowych elementów danych.
Załącznik. Tabela 4. Opcjonalne dane identyfikujące osobę w przypadku osoby prawnej	aktualny adres	Opcjonalne	NIE	Art. 7 pkt 4 (Art. 14a ust. 3 pkt 3-4 ustawy o aplikacji mObywatel)	3. Europejski portfel tożsamości cyfrowej, o którym mowa w ust. 1, zawiera zestaw danych identyfikujących osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą, obejmujący: (…) 3) numer KRS, jeżeli został nadany; 4) numer Katalogu Podmiotów Publicznych, jeżeli został nadany.	Zapewnieni możliwości rozpoznawania osoby prawnej posługującej się europejskim portfelem tożsamości cyfrowej na podstawie nr KRS lub KPP.
	numer identyfikacyjny VAT	Opcjonalne				
	numer identyfikacji podatkowej	Opcjonalne				
	niepowtarzalny identyfikator europejski, o którym mowa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2017/1132.	Opcjonalne				

	identyfikator podmiotu prawnego (LEI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2022/1860		Opcjonalne				
	numer rejestracyjny i identyfikacyjny przedsiębiorcy (EORI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) nr 1352/2013		Opcjonalne				
	numer akcyzowy określony w art. 2 pkt 12 rozporządzenia Rady (UE) nr 389/2012		Opcjonalne				
Załącznik. Tabela 5. Metadane dotyczące danych identyfikujących osobę.	expiry_date	Data (i w miarę możliwości godzina) wygaśnięcia danych identyfikujących osobę	Obowiązkow	TAK/NIE	Art. 7 pkt 4 (Art. 14a ust. 4 ustawy o aplikacji mObywatel)	4. Europejski portfel tożsamości cyfrowej zawiera zestaw metadanych dotyczących zestawu danych identyfikujących osobę fizyczną, osobę prawną lub osobę fizyczną prowadzącą działalność gospodarczą, obejmujący: 1) datę i godzinę wygaśnięcia ważności danych identyfikujących daną osobę; 2) nazwę organu, który wydał dane identyfikujące daną osobę; 3) dwuznakowy kod ISO 3166-1 dla Rzeczypospolitej Polskiej; 4) numer danych identyfikujących daną osobę nadany przez organ, o którym mowa w pkt 2.	Realizacja wymogu uwzględnienia obowiązkowych elementów danych. Dodatkowe nadawanie numeru zestawowi danych identyfikujących osobę ułatwi unieważnianie określonych zestawów oraz weryfikację ich ważności bez potrzeby przetwarzania danych osobowych.
	issuing_authority	Nazwa organu administracyjnego, który wydał dane identyfikujące osobę, lub kod kraju alfa-2 danego państwa członkowskiego zgodnie z normą ISO 3166, jeżeli nie istnieje odrębny organ uprawniony	Obowiązkow				

		do wydawania danych identyfikujących osobę.				
	issuing_country	Kod państwa alfa-2, jak określono w normie ISO 3166-1, państwa lub terytorium dostawcy danych identyfikujących osobę.	Obowiązkow			
	document_numbe r	Numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę.	Opcjonalne			
	issuing_jurisdictio n	Kod podziału terytorialnego państwa jurysdykcji, w którym wydano dane identyfikujące osobę, zgodnie z normą ISO 3166-2:2020, pkt 8. Pierwsza część kodu jest taka sama jak wartość	Opcjonalne			

		dla państwa wydającego.				
	lokalizacja_status	Umiejscowienie informacji o statusie ważności danych identyfikujących osobę, w przypadku gdy dostawcy danych identyfikujących osobę unieważniają dane identyfikujące osobę.	Opcjonalne			
Rozporządzenie 2024/2979						
Art. 2 pkt 1, 10, 12	1) "bezpieczna aplikacja kryptograficzna portfela" oznacza aplikację, która zarządza aktywami krytycznymi, łącząc się z funkcjami kryptograficznymi i niekryptograficznymi zapewnianymi przez bezpieczne urządzenie kryptograficzne portfela oraz korzystając z tych funkcji; 10) "instancja portfela" oznacza aplikację zainstalowaną i skonfigurowaną na urządzeniu lub w środowisku użytkownika portfela, która jest częścią jednostki portfela i z której użytkownik portfela korzysta do interakcji z daną jednostką portfela;	TAK	Art. 7 pkt 4 (Art. 14a ust. 1 pkt 1-3 ustawy o aplikacji mObywatel)	Art. 14a. 1. Minister właściwy do spraw informatyzacji zapewnia europejski portfel tożsamości cyfrowej, w tym: 1) oprogramowanie przeznaczone dla urządzeń mobilnych umożliwiające korzystanie przez użytkownika z tego portfela, zapewniające w szczególności instancję portfela, o której mowa w art. 2 pkt 10 rozporządzenia wykonawczego Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiającego zasady	Wskazanie ministra właściwego do spraw informatyzacji jako podmiotu zapewniającego europejski portfel tożsamości cyfrowej i jednocześnie kluczowe elementy tego portfela.

	12) "bezpieczne urządzenie kryptograficzne portfela" oznacza urządzenie odporne na manipulacje, które zapewnia otoczenie połączone z bezpieczną aplikacją kryptograficzną portfela i przez nią wykorzystywane, aby chronić aktywa krytyczne i zapewniać funkcje kryptograficzne na potrzeby bezpiecznego wykonywania operacji krytycznych			stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej Dz. Urz. UE L 2024/2979 z 04.12.2024, z późn. zm.), zwanego dalej „rozporządzeniem 2024/2979"; 2) bezpieczną aplikację kryptograficzną portfela, o której mowa w art. 2 pkt 1 rozporządzenia 2024/2979; 3) bezpieczne urządzenie kryptograficzne portfela, o którym mowa w art. 2 pkt 12 rozporządzenia 2024/2979;	
Rozporządzenie 2025/846					
Art. 2 ust. 1 i ust. 8	1. W przypadku gdy podmiot sektora publicznego działa jako strona ufająca w kontekście transgranicznej usługi online oferowanej przez ten podmiot sektora publicznego lub w jego imieniu, państwa członkowskie zapewniają, aby proces określony w ust. 2 był wykorzystywany w celu zapewnienia jednoznacznego dopasowywania tożsamości osób fizycznych. 8. Państwa członkowskie mogą polegać na scentralizowanych systemach dopasowywania tożsamości, obsługiwanych przez podmiot sektora publicznego mający siedzibę w tym państwie członkowskim, w celu zapewnienia, aby notyfikowane środki identyfikacji elektronicznej lub	TAK/NIE	Art. 1 pkt 10 lit. a (Art. 21a ust. 1 pkt 2 lit c ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 21a.1. Krajowy schemat identyfikacji elektronicznej obejmuje: (…) 2) przyłączone do węzła krajowego: (…) c) system scentralizowany, o którym mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/846 z dnia 6 maja 2025 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr	W związku z tym że system dopasowywania tożsamości będzie przyłączony do węzła krajowego obowiązek zapewnienia transgranicznego dopasowywania tożsamości osób fizycznych będzie realizowany za pośrednictwem węzła krajowego.

	portfele z innego państwa członkowskiego mogły być dopasowywane do istniejących rejestracji i rejestrów przy użyciu procedur online.		Art. 1 pkt 13 (Art. 22a ust. 7-9 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	910/2014 w odniesieniu do transgranicznego dopasowywania tożsamości osób fizycznych (Dz. Urz. UE L 2025/846 z 07.05.2025), zwanym dalej „rozporządzeniem 2025/846. Art. 22a (….) 7. Strony ufające korzystają z dopasowywania tożsamości w ramach systemu scentralizowanego, jeżeli system teleinformatyczny, w którym udostępniane są ich usługi online, wymagające takiego dopasowania, jest przyłączony do węzła krajowego. 8. Strony ufające, będące podmiotami publicznymi, są obowiązane przyłączyć system teleinformatyczny, w którym są udostępniane ich usługi online, wymagające dopasowania tożsamości, do węzła krajowego. 9. Strony ufające, niebędące podmiotami publicznymi, mogą przyłączyć system teleinformatyczny, w którym udostępniane są ich usługi online, wymagające dopasowania tożsamości, do węzła krajowego.	

Art. 2 ust. 2-5	2. Jednoznaczne dopasowywanie tożsamości dokonywane jest przez stronę ufającą lub w jej imieniu, lub w rejestrze, z którego korzystają strony ufające, lub w systemie scentralizowanym, poprzez żądanie, w stosownych przypadkach, otrzymywanie i walidację autentyczności informacji wymienionych w ust. 3 lub 4, stosownie do przypadku. 3. W przypadku korzystania z portfela informacje, które mają być wykorzystywane do jednoznacznego dopasowywania tożsamości, to obowiązkowe dane identyfikujące osobę określone w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2024/2977 wraz z wszelkimi opcjonalnymi danymi, które są potrzebne do zapewnienia niepowtarzalności przedstawionego zbioru danych, w tym, w stosownych przypadkach, z dodatkowymi informacjami lub procedurami uzupełniającymi. 4. W przypadku korzystania z notyfikowanego systemu identyfikacji elektronicznej informacje, które mają być wykorzystywane do jednoznacznego dopasowywania tożsamości, są atrybutami obowiązkowymi minimalnego zestawu danych dotyczących osoby fizycznej określonymi w pkt 1 załącznika do rozporządzenia wykonawczego (UE) 2015/1501, w tym, w stosownych przypadkach, dodatkowymi informacjami lub procedurami uzupełniającymi. 5. Przy ustalaniu, czy istnieje jednoznaczne dopasowanie tożsamości, strona ufająca lub strona działająca w jej imieniu dopasowuje informacje przekazane przez użytkownika do informacji przekazanych przez stronę ufającą lub stronę działającą w jej imieniu, lub do rejestru, z którego	TAK	Art. 1 pkt 13 (Art. 22a ust. 1-6 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22a. 1. Minister właściwy do spraw informatyzacji zapewnia funkcjonowanie systemu scentralizowanego, o którym mowa w rozporządzeniu 2025/846, umożliwiającego dopasowywanie tożsamości, o którym w art. 11a rozporządzenia 910/2014. 2. System scentralizowany zapewnia w szczególności: 1) dopasowywanie tożsamości osoby fizycznej do danych gromadzonych w rejestrze PESEL, w przypadku gdy ta osoba po raz pierwszy występuje z wnioskiem o udzielenie dostępu do usługi online świadczonej przez stronę ufającą, będącą osobą fizyczną lub osobą prawną, która polega na, europejskim portfelu tożsamości cyfrowej, innym środku identyfikacji elektronicznej, lub na usłudze zaufania, zwaną dalej „stroną ufającą”, a ta strona ufająca wymaga podania numeru PESEL w celu ustalenia, czy osoba fizyczna ma już nadany numer PESEL; 2) możliwość żądania przez stronę ufającą od osoby fizycznej podania dodatkowych danych, o których mowa w ust. 3 pkt 3, i przekazania przez nią tych danych w celu jednoznacznego dopasowania tożsamości w przypadku,	Wskazanie możliwości wstępnego dopasowania do rejestru PESEL i zakresu danych jakie mogą być przetwarzane w systemie scentralizowanym oprócz danych określonych w rozporządzeniach 2024/2977 i 2015/1501 celem jednoznacznego dopasowania. Wskazanie konieczności uzyskania zgody użytkownika. Wskazanie sposobu przekazania danych po ustaleniu wyniku dopasowania.

	korzystają strony ufające, które już się zarejestrowały.			gdy dopasowanie tożsamości jest niejednoznaczne; 3) możliwość zachowania wyników dopasowywania tożsamości, w szczególności numeru PESEL, w celu uniknięcia ponownego dopasowywania tożsamości tej samej osoby wykorzystującej ten sam środek identyfikacji elektronicznej. 3. W systemie scentralizowanym przetwarzane są dane osobowe, obejmujące: 1) dane identyfikujące osobę fizyczną, o których mowa w załączniku do rozporządzenia wykonawczego 2015/1501 – w przypadku osoby fizycznej posługującej się notyfikowanym środkiem identyfikacji elektronicznej; 2) dane identyfikujące osobę, o których mowa w załączniku do rozporządzenia 2024/2977 – w przypadku osoby fizycznej posługującej się europejskim portfelem tożsamości cyfrowej; 3) imiona rodziców, rodzaj, serię i numer dokumentu potwierdzającego tożsamość lub numer PESEL – w przypadku potrzeby podania dodatkowych danych w celu jednoznacznego	

				dopasowania tożsamości osoby fizycznej do danych gromadzonych w rejestrze PESEL lub danych znajdujących się w systemie teleinformatycznym strony ufającej. 4. W przypadku dopasowania tożsamości do danych gromadzonych w rejestrze PESEL, za pomocą systemu scentralizowanego: 1) użytkownik usługi online informowany jest o dopasowaniu i możliwości wysłania ustalonego numeru PESEL do strony ufającej; 2) za zgodą użytkownika usługi online dane identyfikujące osobę, o których mowa w ust. 3 pkt 1 lub 2, wraz z ustalonym numerem PESEL, są wysyłane do strony ufającej. 5. W przypadku niedopasowania tożsamości do danych gromadzonych w rejestrze PESEL, za pomocą systemu scentralizowanego: 1) użytkownik usługi online jest informowany o niedopasowaniu; 2) za zgodą użytkownika do strony ufającej są wysyłane: a) dane identyfikujące osobę, o których mowa w ust. 3 pkt 1 lub 2, wraz z informacją, o nieudanej	

				próbie dopasowania tych danych do danych gromadzonych w rejestrze PESEL, lub b) seria i numer dokumentu potwierdzającego tożsamość tego użytkownika podany przez tego użytkownika. 6. Dane identyfikujące osobę fizyczną są wysyłane za pomocą systemu scentralizowanego w formacie danych zgodnym z formatem danych wysyłanych przez węzeł krajowy.	
Art. 3	Art. 3.Obowiązki stron ufających w przypadku gdy proces dopasowywania tożsamości był skuteczny 1. Gdy użytkownik po raz pierwszy przeprowadza proces dopasowywania tożsamości i uznaje się go za skuteczny zgodnie z art. 2 ust. 7, strona ufająca lub strona działająca w jej imieniu zapewniają, lub w rejestrze, z którego korzystają strony ufające lub systemie scentralizowanym zapewnia się, aby użytkownika powiadomiono, że uzyskał dostęp do usługi, o dostęp do której wnioskował. 2. W stosownych przypadkach użytkownik jest również informowany, czy: a) został zarejestrowany jako nowy użytkownik; b) został skutecznie dopasowany do jednego istniejącego użytkownika strony ufającej; lub c) został skutecznie dopasowany do jednego istniejącego użytkownika w rejestrze, z którego	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	korzysta strona ufająca lub strona działająca w jej imieniu; d) może ponownie wykorzystać zakończone procesy dopasowywania tożsamości w przyszłości, wybierając jedną z poniższych opcji, z uwzględnieniem czasu przechowywania: – przechowywanie powiązania w rejestrze prowadzonym przez stronę ufającą lub w rejestrze, z którego korzysta strona ufająca, które może być ponownie wykorzystane w przyszłych wnioskach o dostęp; – wydanie specjalnego elektronicznego poświadczenia atrybutów zawierającego powiązanie, które można ponownie wykorzystać w przyszłych wnioskach o dostęp; – wykorzystanie alternatywnych opcji zapewnionych przez stronę ufającą lub stronę działającą w imieniu strony ufającej lub system scentralizowany, które można ponownie wykorzystać w przyszłych wnioskach o dostęp.				
Art. 4	Art. 4. Obowiązki stron ufających w przypadku gdy proces dopasowywania tożsamości był nieskuteczny 1. W przypadku gdy proces dopasowywania tożsamości zostanie uznany za nieskuteczny zgodnie z art. 2 ust. 7, strona ufająca lub strona działająca w jej imieniu zapewniają lub w systemie scentralizowanym zapewnia się, aby użytkownika notyfikowanych środków identyfikacji elektronicznej lub portfela poinformowano, czy: a) dane nie zostały udostępnione skutecznie ani jednoznacznie dopasowane do jakiegokolwiek	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	istniejącego użytkownika strony ufającej lub w rejestrze, z którego korzysta strona ufająca lub strona działająca w jej imieniu; b) są dostępne inne opcje dopasowania tożsamości dostępne dla użytkownika lub inne metody uzyskania dostępu do usługi. 2. Opcje lub inne metody, o których mowa w ust. 1 pkt (b), mogą obejmować: a) inny notyfikowany środek identyfikacji elektronicznej lub inny portfel; b) aktualizację informacji już zarejestrowanych przez stronę ufającą, stronę działającą w jej imieniu lub w rejestrze, z którego korzysta strona ufająca, lub w scentralizowanym systemie dopasowywania tożsamości; c) dodatkowe informacje dostarczone przez stronę ufającą lub stronę działającą w jej imieniu na potrzeby dopasowywania tożsamości lub przez system scentralizowany. 3. W przypadku gdy metody uzupełniające skutkują skutecznym i jednoznacznym dopasowaniem lub rejestracją, zastosowanie mają obowiązki określone w art. 3. 4. W przypadku gdy strona ufająca lub system scentralizowany stwierdzą, że użytkownik nie został wcześniej zarejestrowany, początkowo albo po bezskutecznym przeprowadzeniu uzupełniających procesów dopasowywania tożsamości, strona ufająca lub system scentralizowany mogą go uznać za nowego użytkownika i, w stosownych przypadkach, zarejestrować zgodnie z				

	odpowiednimi przepisami krajowymi lub praktykami administracyjnymi. 5. W przypadku gdy metody uzupełniające nie prowadzą do skutecznego i jednoznacznego dopasowania, strona dokonująca dopasowania tożsamości może ocenić, czy użytkownik nie ma wcześniejszych interakcji ze stroną ufającą lub rejestrem, z którego korzysta strona ufająca, i w związku z tym uznaje się go za nowego użytkownika. 6. W przypadku gdy istnieje nowy użytkownik, strony ufające stosują proces określony w art. 3. Strony ufające mogą rejestrować nowych użytkowników zgodnie z prawem krajowym lub krajowymi praktykami administracyjnymi.				
Art. 5	Art. 5. Obowiązki stron ufających po zakończeniu procesu dopasowywania tożsamości 1. W przypadku skutecznego lub nieskutecznego zakończenia procesu dopasowywania tożsamości określonego w art. 2 strona ufająca lub strona działająca w jej imieniu, lub rejestr, z którego korzysta strona ufająca, prowadzą rejestry dotyczące procesu dopasowywania tożsamości i jego wyników, obejmujące następujące informacje, jeżeli są dostępne: a) wartości podane przez użytkownika i stronę ufającą, które są wykorzystywane do przeprowadzenia procesu dopasowywania tożsamości; b) data i godzina procesu dopasowywania tożsamości;	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.

	c) wszelkie istotne dokumenty przekazane w ramach metod uzupełniających, o których mowa w art. 4 ust. 1 i 2, niezbędne do rozstrzygania sporów; d) w stosownych przypadkach wszelkie identyfikatory lub numery rachunków stosowane przez stronę ufającą lub rejestr, z którego korzystają strony ufające, lub strona działająca w jej imieniu, lub scentralizowany system dopasowywania tożsamości, które odnoszą się do osoby fizycznej. 2. Strony ufające lub strony działające w ich imieniu uwzględniają zasady bezpieczeństwa i prywatności już w fazie projektowania związane z rejestrowaniem informacji zawartych w ust. 1. 3. Strony ufające lub strony działające w ich imieniu przechowują rejestry przez co najmniej 6 miesięcy, a maksymalnie przez 12 miesięcy ze względów bezpieczeństwa. Do innych celów, w tym do umożliwienia rejestracji i rozpatrywania skarg użytkowników, czas przechowywania może zostać przedłużony, jeżeli wymaga tego prawo Unii lub prawo krajowe				
Rozporządzenie 2025/848					
Art. 3 ust. 1-3	1. Państwa członkowskie ustanawiają i prowadzą co najmniej jeden krajowy rejestr stron ufających portfela zawierający informacje dotyczące zarejestrowanych stron ufających portfela mających siedzibę w danym państwie członkowskim. 2. Rejestr musi zawierać co najmniej informacje określone w załączniku I.	TAK	Art. 1 pkt 13 (Art. 22b ust. 1, 5 oraz ust. 14 pkt 1-3 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22b. 1. Minister właściwy do spraw informatyzacji prowadzi, przy użyciu systemu teleinformatycznego, rejestr stron ufających europejskiemu portfelowi tożsamości cyfrowej, o którym mowa w art. 3 ust. 1 rozporządzenia 2025/848, zwany dalej „rejestrem stron ufających”	Wskazanie ministra właściwego do spraw informatyzacji jako podmiotu prowadzącego rejestr stron ufających europejskiemu portfelowi tożsamości cyfrowej.

	3. Państwa członkowskie wyznaczają co najmniej jeden podmiot rejestrujący do zarządzania co najmniej jednym krajowym rejestrem stron ufających portfela i jego obsługi.			oraz zapewnia utrzymanie i rozwój tego rejestru, w tym: 1) zapewnia ochronę przed nieuprawnionym dostępem do rejestru; 2) zapewnia integralność danych przetwarzanych w rejestrze; 3) zapewnia dostępność systemu teleinformatycznego, przy użyciu którego jest prowadzony rejestr; 4) przeciwdziała uszkodzeniom systemu teleinformatycznego, przy użyciu którego jest prowadzony rejestr; 5) określa zasady bezpieczeństwa przetwarzanych danych, w tym danych osobowych; 6) określa zasady zgłaszania naruszenia ochrony danych osobowych; 7) zapewnia rozliczalność działań dokonywanych na danych w rejestrze; 8) zapewnia poprawność danych przetwarzanych w rejestrze. (…..) 5. Wniosek, o którym mowa w ust. 3, zawiera dane i informacje określone w załączniku I do rozporządzenia 2025/848 oraz	Doprecyzowanie zakresu danych, jakie znajdą się w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej, oprócz danych o których mowa w załączniku I do rozporządzenia 2025/848.

				adres do doręczeń elektronicznych wpisany do bazy adresów elektronicznych, o której mowa w art. 25 ust. 1 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz. U. z 2026 r. poz. 3 i 507). (….) 14. System teleinformatyczny, przy użyciu którego jest prowadzony rejestr stron ufających zapewnia: 1) uwierzytelnianie użytkowników w sposób określony w ust. 3 oraz za pomocą certyfikatu dostępu strony ufającej portfelowi; 2) wystawianie uwierzytelnionym użytkownikom, będącym podmiotami sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014, wpisanymi do Katalogu Podmiotów Publicznych, certyfikatów rejestracji strony ufającej portfelowi, odpowiadających dokonanym wpisom odnoszącym się do poszczególnych usług; 3) automatyczne unieważnienie certyfikatów rejestracji strony ufającej portfelowi wydanych w sposób, o którym mowa w pkt 2, w związku z zaistniałymi we wpisie do rejestru stron ufających zmianami	

				danych, które zostały umieszczone w tych certyfikatach;	
Art. 4 ust. 1	1 Państwa członkowskie ustanawiają i publikują co najmniej jedną krajową politykę rejestracji mającą zastosowanie do krajowych rejestrów ustanowionych na ich terytorium.	TAK	Art. 1 pkt 13 (Art. 22b ust. 15 pkt 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	15. Minister właściwy do spraw informatyzacji określa i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej: 1) krajową politykę rejestracji w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej, o której mowa w rozporządzeniu 2025/848;	Wskazano, że minister właściwy do spraw informatyzacji ustanawia i publikuje w BIP krajową politykę rejestracji w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej.
Art. 6 ust. 1-4	1. Podmioty rejestrujące ustanawiają łatwe w użycie elektroniczne i w miarę możliwości zautomatyzowane procesy rejestracji dla stron ufających portfela. 2. Podmioty rejestrujące bez zbędnej zwłoki rozpatrują wnioski o rejestrację i udzielają wnioskodawcy odpowiedzi na wniosek o rejestrację w terminie określonym w mającej zastosowanie polityce rejestracji, z wykorzystaniem odpowiednich środków oraz zgodnie z przepisami i procedurami państwa członkowskiego, w którym ustanowiono rejestr krajowy. 3. W miary możliwości podmioty rejestrujące dokonują weryfikacji w sposób zautomatyzowany: a) dokładność, ważność, autentyczność i integralność informacji wymaganych na mocy art. 5; b) w stosownych przypadkach pełnomocnictwo przedstawicieli stron ufających portfela sporządzone i przedłożone zgodnie z przepisami i	TAK	Art. 1 pkt 13 (Art. 22b ust. 3-4, 6-7, 10 i 17 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	3. Wpis do rejestru stron ufających i zmiany we wpisie następują na wniosek złożony w postaci elektronicznej do ministra właściwego do spraw informatyzacji: 1) z wykorzystaniem formularza elektronicznego udostępnionego przez ministra właściwego do spraw informatyzacji, po uwierzytelnieniu strony ufającej europejskiemu portfelowi tożsamości cyfrowej za pomocą: a) w przypadku osób fizycznych za pomocą: – środka identyfikacji elektronicznej osoby fizycznej zapewniającego wysoki poziom bezpieczeństwa, – danych weryfikowanych za pomocą kwalifikowanego podpisu	Przepisy ustanawiające sposoby uzyskania wpisu (wyłącznie drogą elektroniczną), możliwość skorzystania z pośrednictwa podmiotów wydających certyfikaty i weryfikację danych z właściwymi rejestrami źródłowymi. Wskazanie, że wpis jest czynnością materialno-techniczną i następuje po zweryfikowaniu kompletności danych zawartych we wniosku. Wskazanie, że minister właściwy do spraw informatyzacji udostępni w BIP specyfikację techniczną wniosku.

	proceduramі państwa członkowskiego, w którym utworzono rejestr; c) rodzaj uprawnienia lub uprawnień stron ufających portfela, jak określono w załączniku I; d)brak istniejącej rejestracji w innym rejestrze krajowym. 4. Podmioty rejestrujące weryfikują informacje, o których mowa w ust. 3, na podstawie dokumentacji potwierdzającej dostarczonej przez strony ufające portfela oraz na podstawie odpowiednich źródeł autentycznych lub innych oficjalnych rejestrów elektronicznych w państwie członkowskim, w którym utworzono rejestr krajowy, do których podmioty rejestrujące mają dostęp zgodnie z mającymi zastosowanie przepisami i procedurami krajowymi.			elektronicznego, jeżeli te dane pozwalają na identyfikację i uwierzytelnienie wymagane w celu realizacji usługi online umożliwiającej wpis do rejestru stron ufających europejskiemu portfelowi tożsamości cyfrowej, b) w przypadku osób prawnych za pomocą: – środka identyfikacji elektronicznej osoby prawnej zapewniającego wysoki poziom bezpieczeństwa lub – zaawansowanej pieczęci elektronicznej weryfikowanej za pomocą kwalifikowanego certyfikatu; 2) za pośrednictwem kwalifikowanego dostawcy usług zaufania świadczącego usługę wydawania certyfikatów dostępu strony ufającej portfelowi lub certyfikatów rejestracji strony ufającej portfelowi. 4. Wniosek, o którym mowa w ust. 3 pkt 2, opatruje się kwalifikowanym podpisem elektronicznym osoby fizycznej albo kwalifikowanym podpisem elektronicznym osoby fizycznej upoważnionej do reprezentowania osoby prawnej, w której imieniu ten wniosek jest składany, oraz zaawansowaną pieczęcią elektroniczną	

				weryfikowaną kwalifikowanym certyfikatem kwalifikowanego dostawcy usług zaufania, za pośrednictwem którego jest składany. Przed opatrzeniem wniosku pieczęcią elektroniczną kwalifikowany dostawca usług zaufania weryfikuje uprawnienia osoby fizycznej do reprezentowania osoby prawnej w sposób zgodny z krajową polityką, o której mowa w ust. 15 pkt 2. (…) 6. Formularz elektroniczny, o którym mowa w ust. 3 pkt 1, umożliwia, po uwierzytelnieniu strony ufającej europejskiemu portfelowi tożsamości cyfrowej, pobranie danych z rejestrów, o których mowa w ust. 7, w celu wstępnego automatycznego uzupełnienia wniosku. 7. Minister właściwy do spraw informatyzacji weryfikuje zgodność danych zawartych we wniosku z danymi wpisanymi: 1) do Centralnej Ewidencji i Informacji o Działalności Gospodarczej; 2) do Krajowego Rejestru Sądowego;	

				3) do Katalogu Podmiotów Publicznych; 4) na zaufaną listę, o której mowa w art. 2 pkt 2; 5) do rejestru PESEL - w przypadku, gdy wniosek o wpis składa osoba fizyczna nieprowadząca działalności gospodarczej. (…) 10. Wpis do rejestru stanowi czynność materialno-techniczną i następuje po zweryfikowaniu kompletności danych zawartych we wniosku zgodnie z ust. 7-9, o czym strona ufająca jest niezwłocznie powiadamiana na adres poczty elektronicznej o którym mowa w pkt 7 lit. c załącznika I do rozporządzenia 2025/848. (…..) 17. Minister właściwy do spraw informatyzacji , udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej specyfikację techniczną wniosku o którym mowa w ust. 3. 18. Wniosek o cofnięcie rejestracji strony ufające portfela, o którym mowa w art. 9 ust. 3 rozporządzenia 2025/848, podmioty, których dotyczy wpis do	

				rejestru stron ufających, składają do ministra właściwego do spraw informatyzacji. 19. Minister właściwy do spraw informatyzacji może w drodze decyzji, z urzędu cofnąć rejestrację strony ufającej portfela, rejestrację usługi, lub rejestrację przypadku zamierzonego użycia, o którym mowa w pkt 9 i 10 załącznika I do rozporządzenia 2025/848, z powodów, o których mowa w art. 9 ust. 2 tego rozporządzenia. 20. Decyzja o cofnięciu rejestracji podlega natychmiastowemu wykonaniu. Przepisu art. 61 § 2 pkt 1 ustawy z dnia 30 sierpnia 2002 r. - Prawo o postępowaniu przed sądami administracyjnymi nie stosuje się. 21. W przypadku cofnięcia rejestracji we wpisie do rejestru umieszcza się adnotację o cofnięciu rejestracji oraz dacie i godzinie cofnięcia rejestracji.	
Art. 6 ust. 5	6. Jeżeli podmiot rejestrujący nie może zweryfikować informacji zgodnie z ust. 3-5, podmiot rejestrujący odrzuca rejestrację.	TAK	Art. 1 pkt 13 (Art. 22b ust. 11 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	11. W przypadku braku kompletności danych lub braku zgodności, o której mowa w ust. 7, minister właściwy do spraw informatyzacji zwraca wniosek wskazując jego braki, z pouczeniem, że ich usunięcie wymaga złożenia ponownego	Wskazanie sposobu odrzucenia rejestracji.

				wniosku.Wniosek zawierający braki nie podlega rozpoznaniu.	
Art. 7 ust. 1	1. Państwa członkowskie upoważniają co najmniej jeden urząd certyfikacji do wydawania certyfikatów dostępu strony ufającej portfela.	TAK	Art. 1 pkt 4 lit. a i c, pkt 7 i 9 (Art. 4 ust. 1 pkt 2 i 3, ust. 6 pkt 3 i art. 8 ust. 1 i ust. 3a, art. 16 pkt 4 i 5 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	4) w art. 4: a) w ust. 1: – pkt 1 i 2 otrzymują brzmienie: „1) dostawcy usług zaufania, który zamierza świadczyć kwalifikowane usługi zaufania; 2) kwalifikowanej usługi zaufania;”, – dodaje się pkt 3-6 w brzmieniu: „3) usługi wydawania certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/848 z dnia 6 maja 2025 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do rejestracji stron ufających portfela (Dz. Urz. UE L 2025/848 z 07.05.2025, z późn. zm), zwanym dalej „rozporządzeniem 2025/848, przez kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektronicznej”;	Wskazanie podmiotów wydających certyfikaty dostępu strony ufającej portfelowi.

				c) w ust. 6 w pkt 2 kropkę zastępuje się średnikiem i dodaje się pkt 3-6 w brzmieniu: „3) usługi wydawania przez kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty podpisu elektronicznego i kwalifikowane certyfikaty pieczęci elektronicznej, certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi; 4) usługi wydawania niekwalifikowanych podpisów elektronicznych lub niekwalifikowanych pieczęci elektronicznych tworzonych na odległość; 5) usługi wydawania do europejskiego portfela tożsamości cyfrowej niekwalifikowanych elektronicznych poświadczeń atrybutów, o których mowa w art. 3 pkt 44 rozporządzenia 910/2014, innych niż określone w art. 3 pkt 46 tego rozporządzenia; 6) usługi wydawania do europejskiego portfela tożsamości cyfrowej elektronicznych poświadczeń atrybutów, o których mowa w art. 3 pkt 46 rozporządzenia 910/2014;	

				5) w art. 5: a) ust. 1 otrzymuje brzmienie: „1. Decyzja, o której mowa w art. 4 ust. 6 pkt 2-5, jest podstawą do wydania certyfikatu, o którym mowa w art. 10 ust. 1 pkt 1, oraz dokonania wpisu na zaufaną listę, a w przypadku kwalifikowanych usług zaufania oznacza nadanie statusu kwalifikowanego dostawcy usług zaufania lub świadczonej przez niego usłudze. b) po ust. 1 dodaje się ust. 1a w brzmieniu 1a. Decyzja, o której mowa w art. 4 ust. 6 pkt 2-4, jest podstawą do wydania certyfikatu, o którym mowa w art. 10 ust. 1 pkt 1.” (….) 8) w art. 8: a) ust. 1 otrzymuje brzmienie: „1. Minister właściwy do spraw informatyzacji wykreśla z rejestru, w drodze decyzji: 1) kwalifikowanego dostawcę usług zaufania, 2) kwalifikowaną usługę zaufania, 3) świadczoną przez kwalifikowanego dostawcę usług zaufania, usługę wydawania	

				certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelowi .”, b) po ust. 1 dodaje się ust. 1a w brzmieniu „1a. Minister właściwy do spraw informatyzacji, w drodze decyzji wykreśla z rejestru niekwalifikowanego dostawcę usług zaufania lub świadczoną przez niego niekwalifikowaną usługę zaufania, o której mowa w art. 4 ust.1 pkt 4-6.”, c) po ust. 3 dodaje się ust. 3a i 3b w brzmieniu: „3a. Decyzja o wykreśleniu z rejestru usługi wydawania certyfikatów dostępu strony ufającej portfelowi i certyfikatów rejestracji strony ufającej portfelowi oznacza odebranie kwalifikowanemu dostawcy usług zaufania uprawnienia do wydawania takich certyfikatów. 3b. Decyzja o wykreśleniu z rejestru niekwalifikowanego dostawcy usług zaufania lub świadczonej przez niego niekwalifikowanej usługi zaufania, o której mowa w art. 4 ust. 1 pkt 4-6, oznacza odebranie	

				temu dostawcy możliwości świadczenia tej usługi.”, d) ust. 5 otrzymuje brzmienie: „5. Decyzja o wykreśleniu, o której mowa w ust. 1 lub ust. 1a, jest podstawą wykreślenia dostawcy usług zaufania z zaufanej listy oraz może być podstawą do unieważnienia certyfikatów, o których mowa w art. 10 ust. 1 pkt 1.”, e) ust. 6 otrzymuje brzmienie: „6. Minister właściwy do spraw informatyzacji wykreśla niekwalifikowanego dostawcę usług zaufania z rejestru w przypadku: 1) ustalenia, że dostawca ten zaprzestał świadczenia usług zaufania; 2) złożenia przez tego dostawcę wniosku o wykreślenie z rejestru; 3) ustalenia, że certyfikaty, o których mowa w art. 10 ust. 1 pkt 1, są wykorzystywane w sposób wykraczający poza zakres ich stosowania, 4) ustalenia, że dostawca ten działa niezgodnie z wymogami art. 19a rozporządzenia 910/2014.”; (…)	

			(Art. 22b ust. 12 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	12. Certyfikaty dostępu strony ufającej portfelowi oraz certyfikaty rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848, wydawane są przez kwalifikowanych dostawców usług zaufania, którzy uzyskali wpis do rejestru, o którym mowa w art. 2 pkt 1.	
Art. 7 ust. 2	2. Państwa członkowskie zapewniają, aby dostawcy certyfikatów dostępu strony ufającej portfela wydawali certyfikaty dostępu strony ufającej portfela wyłącznie zarejestrowanym stronom ufającym portfela.	TAK	Art. 1 pkt 13 (Art. 22b ust. 14 pkt 4 oraz ust. 15 i ust. 16 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	14. System teleinformatyczny, przy użyciu którego jest prowadzony rejestr stron ufających zapewnia: (…) 4) mechanizm informowania kwalifikowanych dostawców usług zaufania o: a) konieczności unieważnienia wydanych przez nich certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi w związku z zaistniałymi we wpisie do rejestru stron ufających zmianami danych,	Ustalenie sposobu informowania dostawców certyfikatów dostępu strony ufającej portfelowi o zmianach w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej i obowiązek dostosowania się tych dostawców do polityk rejestracji i certyfikacji określanych przez ministra właściwego do spraw informatyzacji.

				które zostały umieszczone w tych certyfikatach, b) dokonaniu wpisu do rejestru stron ufających na wniosek, o którym mowa w ust. 3 pkt 2, złożony za ich pośrednictwem. 15. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej: 1) krajową politykę rejestracji w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej, o której mowa w rozporządzeniu 2025/848; 2) krajową politykę certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848;; 3) krajową politykę certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848. 16. Podmioty wydające certyfikaty dostępu strony ufającej portfelowi oraz certyfikaty rejestracji strony ufającej portfelowi stosują się do	

				krajowych polityk, o których mowa w ust. 15.	
Art. 7 ust. 3	3. Państwa członkowskie ustanawiają w sposób zharmonizowany pod względem syntaktycznymi i semantycznym polityki certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfela, zgodnie z wymogami określonymi w załączniku IV.	TAK	Art. 1 pkt 13 (Art. 22b ust. 15 pkt 2 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	15. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej: (…) 2) krajową politykę certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów dostępu strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848;	Wskazanie podmiotu ustanawiającego politykę certyfikacji i sposobu jej ogłaszania.
Art. 8 ust. 1	1. Państwa członkowskie mogą upoważnić co najmniej jeden urząd certyfikacji do wydawania certyfikatów rejestracji strony ufającej portfela.	NIE	Art. 1 pkt 13 (Art. 22b ust. 12 i 13 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	12. Certyfikaty dostępu strony ufającej portfelowi oraz certyfikaty rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848, wydawane są przez kwalifikowanych dostawców usług zaufania, którzy uzyskali wpis do rejestru, o którym mowa w art. 2 pkt 1. 13. Certyfikaty rejestracji strony ufającej portfelowi dla podmiotów sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014, wpisanych do Katalogu Podmiotów Publicznych, mogą być wydawane przez ministra właściwego do spraw informatyzacji.	Wskazanie podmiotów wydających certyfikaty rejestracji strony ufającej portfelowi.

Art. 8 ust. 2	2. W przypadku gdy państwo członkowskie zezwoliło na wydanie certyfikatu rejestracji strony ufającej portfela, to państwo członkowskie: a) wymaga, aby dostawcy certyfikatów rejestracji strony ufającej portfela wydawali certyfikaty rejestracji strony ufającej portfela wyłącznie zarejestrowanym stronom ufającym portfela; b) zapewnia, aby każde planowane wykorzystanie było wyrażone w certyfikatach rejestracji strony ufającej portfela; c) zapewnia, aby certyfikaty rejestracji strony ufającej portfela zawierały ogólną politykę dostępu, harmonizowaną w całej Unii pod względem syntaktycznym i semantycznym, zawierającą informację dla użytkowników, że strona ufająca portfela może żądać wyłącznie danych określonych w certyfikatach rejestracji w odniesieniu do zamierzonego użycia zarejestrowanego w certyfikatach rejestracji. d) zapewnia, aby dostawcy rozwiązań w zakresie portfela mający siedzibę w danym państwie członkowskim spełniali wymogi ogólnej polityki dostępu przez informowanie użytkowników, gdy strona ufająca portfela żąda danych, których nie określono w certyfikacie rejestracji; e) wdraża certyfikaty rejestracji strony ufającej portfela w sposób zharmonizowany pod względem syntaktycznym i semantycznym zgodnie z wymogami określonymi w załączniku V; f) wdraża specjalne polityki certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów rejestracji strony	TAK	Art. 1 pkt 13 (Art. 22b ust. 14 pkt 4 oraz ust. 15 i ust. 16 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	14. System teleinformatyczny, przy użyciu którego jest prowadzony rejestr stron ufających zapewnia: (…) 4) mechanizm informowania kwalifikowanych dostawców usług zaufania o: a) konieczności unieważnienia wydanych przez nich certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi w związku z zaistniałymi we wpisie do rejestru stron ufających zmianami danych, które zostały umieszczone w tych certyfikatach, b) dokonaniu wpisu do rejestru stron ufających na wniosek, o którym mowa w ust. 3 pkt 2, złożony za ich pośrednictwem. 15. Minister właściwy do spraw informatyzacji określi i udostępni w Biuletynie Informacji Publicznej na swojej stronie podmiotowej: 1) krajową politykę rejestracji w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej, o której mowa w rozporządzeniu 2025/848; 2) krajową politykę certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do	Ustalenie sposobu informowania dostawców certyfikatów dostępu strony ufającej portfelowi oraz certyfikatów rejestracji strony ufającej portfelowi o zmianach w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej i obowiązek dostosowania się tych dostawców do polityk rejestracji i certyfikacji określanych przez ministra właściwego do spraw informatyzacji. Wskazanie ministra właściwego do spraw informatyzacji, jako podmiotu określającego politykę certyfikacji i sposobu jej udostępniania.

	ufającej portfela zgodnie z wymogami określonymi w załączniku V; g) zapewnia, aby strony ufające portfela podawały URL polityki prywatności w odniesieniu do zamierzonego użycia.			certyfikatów dostępu strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848; 3) krajową politykę certyfikacji i oświadczenia dotyczące praktyk certyfikacji w odniesieniu do certyfikatów rejestracji strony ufającej portfelowi, o których mowa w rozporządzeniu 2025/848. 16. Podmioty wydające certyfikaty dostępu strony ufającej portfelowi oraz certyfikaty rejestracji strony ufającej portfelowi stosują się do krajowych polityk, o których mowa w ust. 15.	
Załącznik I pkt 12 lit. c, d, j	12. Uprawnienie lub uprawnienia strony ufającej portfela wyrażone w następujący sposób: c) "Non_Q_EAA_Provider" oznacza uprawnienie strony ufającej portfela jako dostawcy usług zaufania wydającego niekwalifikowane elektroniczne poświadczenia atrybutów. d) "PUB_EAA_Provider" oznacza uprawnienie strony ufającej portfela jako dostawcy elektronicznych poświadczeń atrybutów wydanych przez podmiot sektora publicznego odpowiedzialny za źródło autentyczne lub w jego imieniu; j) ESig_ESeal_Creation_Provider" oznacza uprawnienie strony ufającej portfela jako niekwalifikowanego dostawcy usług zaufania świadczącego niekwalifikowaną usługę zaufania na potrzeby tworzenia podpisów elektronicznych lub pieczęci elektronicznych na odległość.	TAK	Art. 1 pkt 4 lit. a (Art. 4 ust. 1 pkt 4-6 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	4) usługi wydawania niekwalifikowanych podpisów elektronicznych lub niekwalifikowanych pieczęci elektronicznych tworzonych na odległość; 5) usługi wydawania niekwalifikowanych elektronicznych poświadczeń atrybutów, o których mowa w art. 3 pkt 44 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz.	Celem przepisów jest zapewnienie umieszczenia danych dotyczących dostawców, którzy świadczą określone w tym przepisie usługi zaufania, w rejestrze dostawców usług zaufania i na zaufanej liście. Powyższe pozwoli na zapewnienie użytkownikom europejskiego portfela tożsamości cyfrowej możliwości natychmiastowej weryfikacji posiadanych

				UE L 257 z 28.08.2014, str. 73, z późn. zm.), zwanego dalej „rozporządzeniem 910/2014”, innych niż elektroniczne poświadczenia atrybutów, o których mowa w art. 3 pkt 46 rozporządzenia 910/2014, 6) usługi wydawania elektronicznych poświadczeń atrybutów, o których mowa w art. 3 pkt 46 rozporządzenia 910/2014”,	przez stronę ufającą odpowiednich uprawnień.
Załącznik I pkt 14 i 15	Załącznik I. Informacje dotyczące stron ufających portfela (…) 14. W stosownych przypadkach wskazanie, że strona ufająca portfela polega na pośredniku działającym w imieniu strony ufającej, która zamierza polegać na portfelu. 15. W stosownych przypadkach powiązanie z pośrednikiem, na który polega strona ufająca portfela działającym w imieniu strony ufającej, która zamierza polegać na portfelu.	TAK	Art. 1 pkt 13 (Art. 22b ust. 8 i 9 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	8. W przypadku, gdy wniosek zawiera wskazanie pośrednika, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, wpisanego do rejestru stron ufających, wpis do tego rejestru następuje po potwierdzeniu tego wskazania przez pośrednika uwierzytelnionego w systemie teleinformatycznym, przy użyciu którego jest prowadzony ten rejestr. Minister właściwy do spraw informatyzacji zapewnia w systemie teleinformatycznym, przy użyciu którego jest prowadzony ten rejestr, możliwość potwierdzenia, o którym mowa w zdaniu pierwszym. 9. W przypadku, gdy wniosek zawiera wskazanie pośrednika, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, wpisanego do rejestru	Zapewnienie mechanizmu samodzielnego potwierdzania w rejestrze stron ufających europejskiemu portfelowi tożsamości cyfrowej przez wskazanego pośrednika, że nim jest, bez potrzeby badania przez rejestratora umów pomiędzy pośrednikiem a końcowa stroną ufającą. Zapewnienie możliwości weryfikacji pośrednika, w przypadku gdy jest on wpisany do rejestru w innym państwie członkowskim.

				stron ufających europejskim portfelom tożsamości cyfrowej prowadzonego w innym państwie członkowskim Unii Europejskiej, do wniosku załącza się sporządzone przez notariusza, w języku polskim, elektroniczne poświadczenie zgodności odpisu umowy na świadczenie usług pośrednictwa, o których mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, zawierające: 1) określenie stron umowy pozwalające na ich jednoznaczną identyfikację; 2) wskazanie strony umowy, która pełni rolę pośrednika, o którym mowa w pkt 14 i 15 załącznika I do rozporządzenia 2025/848, oraz adresu elektronicznego wpisu w rejestrze stron ufających europejskim portfelom tożsamości cyfrowej właściwym dla jego siedziby; 3) wskazanie usług w których ten pośrednik pośredniczy.	
Rozporządzenie 2025/1568					
Art. 1 ust. 1-6	1. W przypadku gdy państwo członkowskie dokonuje wstępnej notyfikacji systemu identyfikacji elektronicznej Komisji i pozostałym państwom członkowskim, wzajemną ocenę rozpoczyna się zgodnie z art. 2.	TAK	Art. 1 pkt 16 lit. b (Art. 24 ust. 4 ustawy o usługach	4. Minister właściwy do spraw informatyzacji zgłasza systemy identyfikacji elektronicznej do notyfikacji, o której mowa w art. 9 rozporządzenia 910/2014, i zmiany	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji

	2. Państwo członkowskie, które dokonuje wstępnej notyfikacji systemu identyfikacji elektronicznej, może w dowolnym momencie wycofać swoją wstępną notyfikację. W przypadku gdy państwo członkowskie wycofuje wstępną notyfikację systemu identyfikacji elektronicznej, wzajemną ocenę uznaje się za zakończoną. 3. Każde państwo członkowskie może podjąć decyzję o udziale we wzajemnej ocenie systemu identyfikacji elektronicznej innego państwa członkowskiego. 4. Każde państwo członkowskie uczestniczące we wzajemnej ocenie pokrywa koszty, które ponosi w ramach procedury. 5. Przedstawiciele państw członkowskich, które przeprowadzają wzajemną ocenę, wykorzystują informacje uzyskane w ramach wzajemnej oceny wyłącznie do celów tej oceny i nie ujawniają osobom trzecim żadnych informacji szczególnie chronionych ani poufnych uzyskanych podczas wzajemnej oceny. 6. Państwo członkowskie, które zdecyduje się uczestniczyć we wzajemnej ocenie systemu identyfikacji elektronicznej innego państwa członkowskiego, ujawnia wszelkie konflikty interesów w odniesieniu do przedstawicieli wyznaczonych przez to państwo członkowskie. W przypadku konfliktu interesów państwo członkowskie, którego system identyfikacji elektronicznej jest poddawany wzajemnej ocenie, może odmówić udziału odpowiedniego przedstawiciela w ocenie swojego systemu identyfikacji elektronicznej.		zaufania oraz identyfikacji elektronicznej)	w tych systemach, oraz realizuje zadania, o których mowa w rozporządzeniu wykonawczym Komisji (UE) 2025/1568 z dnia 29 lipca 2025 r. ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do ustaleń proceduralnych dotyczących wzajemnych ocen systemów identyfikacji elektronicznej i współpracy w zakresie organizacji takich przeglądów w ramach grupy współpracy oraz uchylającym decyzję wykonawczą Komisji (UE) 2015/296 (Dz. Urz. UE L 2025/1568 z 30.07.2025).	rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.

Rozporządzenie 2025/1569					
Art. 5 ust. 1-3	1. Państwa członkowskie przekazują co najmniej informacje określone w załączniku III dotyczące podmiotów sektora publicznego, o których mowa w art. 45f ust. 3 rozporządzenia (UE) nr 910/2014, za pośrednictwem bezpiecznego elektronicznego systemu powiadamiania udostępnionego przez Komisję. 2. Państwa członkowskie notyfikują wszelkie zmiany zgłoszonych informacji. 3. Państwa członkowskie wystosowują notyfikacje co najmniej w języku angielskim. Państwa członkowskie nie mają obowiązku tłumaczenia jakiegokolwiek dokumentu potwierdzającego notyfikacje, jeśli stworzyłoby to nieuzasadnione obciążenie administracyjne lub finansowe.	TAK	Art. 1 pkt 14 (Art. 23 pkt 14 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 23. Minister właściwy do spraw informatyzacji: (…) 14) notyfikuje Komisji Europejskiej podmioty sektora publicznego, o których mowa w art. 3 pkt 46 rozporządzenia 910/2014, zgodnie z art. 45f ust. 3 rozporządzenia 910/2014;	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji.
Art. 7 ust. 3	3. Państwa członkowskie składają wnioski o włączenie atrybutów wymienionych w załączniku VI do rozporządzenia (UE) nr 910/2014 do katalogu atrybutów, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych do celów weryfikacji przez kwalifikowanych dostawców usług zaufania.	TAK	Art. 1 pkt 13 (Art. 22d ust. 1 oraz 22e ust. 1, 4 i 6-8 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22d. 1. Podmiot odpowiedzialny za źródło autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014, które umożliwia weryfikację drogą elektroniczną autentyczności atrybutów wymienionych w załączniku VI do rozporządzenia 910/2014, składa do ministra właściwego do spraw informatyzacji, na piśmie utrwalonym w postaci elektronicznej wniosek o zgłoszenie przez tego ministra atrybutów do katalogu atrybutów prowadzonego przez Komisję Europejską, o którym	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym z tym zobowiązania w tym zakresie powinien

				mowa w rozporządzeniu wykonawczym 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. Urz. UE L 2025/1569 z 30.07.2025, z późn. zm.), zwanym dalej „rozporządzeniem 2025/1569”, dotyczące atrybutów, których dotyczy to źródło. Wniosek zawiera w informacje, o których mowa w art. 7 ust. 5 rozporządzenia 2025/1569. Art. 22e. 1. Minister właściwy do spraw informatyzacji składa wnioski o włączenie atrybutów wymienionych w załączniku VI do rozporządzenia 910/2014 do katalogu atrybutów prowadzonego przez Komisję Europejską, o którym mowa w przepisach wydanych na podstawie art. 45d ust. 5, art. 45e ust. 2 i art. 45f ust. 6 i 7rozporządzenia 910/2014, oraz o modyfikację atrybutów w tym katalogu.	realizować minister właściwy do spraw informatyzacji. Minister właściwy do spraw informatyzacji musi jednak uzyskać niezbędne informacje od podmiotów odpowiedzialnych za źródło autentyczne. Pośrednictwo ministra ma na celu również zapewnienie aby w imieniu Polski nie były składane wnioski, które w ogóle nie powinny podlegać ocenie Komisji, o której mowa w art. 7 ust. 2 rozporządzenia 2025/1569

				(….) 4. W przypadku, gdy minister właściwy do spraw informatyzacji jest podmiotem odpowiedzialnym za źródło autentyczne, o którym mowa w załączniku VI do rozporządzenia 910/2014, składa z urzędu wnioski, o których mowa w ust. 1 i 2. (….) 6. W przypadku, gdy minister właściwy do spraw informatyzacji nie jest podmiotem odpowiedzialnym za źródło autentyczne, o którym mowa w załączniku VI do rozporządzenia 910/2014, składa wnioski, o których mowa w ust. 1 i 2, na wniosek podmiotu, o którym mowa w art. 22d ust. 1 i 2. 7. W przypadku, gdy minister właściwy do spraw informatyzacji jest podmiotem, który wydaje elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, wykorzystujące atrybuty pochodzące z źródła autentycznego, za które nie jest odpowiedzialny, wnioski, o których mowa w ust. 3, składa na wniosek podmiotu, o którym mowa w art. 22d ust. 3.	

				8. Schematy poświadczania atrybutów do katalogu schematów poświadczania atrybutów prowadzonego przez Komisję Europejską mogą zgłaszać: 1) podmioty odpowiedzialne za źródła autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014; 2) kwalifikowani dostawcy usług zaufania świadczący usługi wydawania kwalifikowanych elektronicznych poświadczeń atrybutów; 3) dostawcy usług online wpisani do rejestru stron ufających europejskim portfelom tożsamości cyfrowej, o którym mowa art. 22b ust. 1, w zakresie elektronicznych poświadczeń atrybutów wykorzystujących wpisane do rejestru dane, poświadczenia lub atrybuty, o których mowa w pkt 9 załącznika I do rozporządzenia 2025/848.	
Art. 7 ust. 4	4. Państwa członkowskie mogą się ponadto zwrócić o włączenie atrybutów niewymienionych w załączniku VI do katalogu atrybutów, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych w sektorze publicznym. Podmioty prywatne uznane za podstawowe źródło informacji lub za źródło autentyczne zgodnie z prawem Unii lub prawem krajowym, z uwzględnieniem praktyki	NIE	Art. 1 pkt 13 (Art. 22d ust. 2 oraz 22e ust. 2 ustawy o usługach zaufania oraz	Art. 22d (…) 2. Podmiot odpowiedzialny za źródło autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014, inne niż umożliwiające weryfikację drogą elektroniczną	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych

	administracyjnej, mogą się zwrócić o włączenie atrybutów niewymienionych w załączniku VI do katalogu atrybutów, w każdym przypadku gdy podmiot wnioskujący jest odpowiedzialny za te atrybuty.		identyfikacji elektronicznej)	autentyczności atrybutów wymienionych w załączniku VI do rozporządzenia 910/2014, może składać na piśmie utrwalonym w postaci elektronicznej wniosek o zgłoszenie przez ministra właściwego do spraw informatyzacji atrybutów do katalogu atrybutów prowadzonego przez Komisję Europejską, o którym mowa w art. 7 ust. 1 rozporządzenia 2025/1569. Wniosek zawiera informacje, o których mowa w art. 7 ust. 5 rozporządzenia 2025/1569. Art. 22e (…) 2. Minister właściwy do spraw informatyzacji składa wnioski o włączenie atrybutów niewymienionych w załączniku VI do rozporządzenia 910/2014 do katalogu atrybutów prowadzonego przez Komisję Europejską, o którym mowa w przepisach wydanych na podstawie art. 45d ust. 5, art. 45e ust. 2 i art. 45f ust. 6 i 7 rozporządzenia 910/2014, oraz o modyfikację atrybutów w tym katalogu.	Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji. Minister właściwy do spraw informatyzacji musi jednak uzyskać niezbędne informacje od podmiotów odpowiedzialnych za źródło autentyczne. Pośrednictwo ministra ma na celu również zapewnienie, aby w imieniu Polski nie były składane wnioski, które w ogóle nie powinny podlegać ocenie Komisji, o której mowa w art. 7 ust. 2 rozporządzenia 2025/1569
Art. 8 ust. 3 zdanie pierwsze	3. Właściciele schematu poświadczania atrybutów mogą się zwrócić o dodanie schematów do katalogu schematów.	NIE	Art. 1 pkt 13 (Art. 22d ust. 3 oraz art. 22e ust. 3, ust. 5,	Art. 22d (...)	Dział informatyzacja zgodnie z art. 12a ust. 1 pkt 4 ustawy z dnia 4 września 1997 r. o

			ust. 7 - 8 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	3. Podmiot odpowiedzialny za źródło autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014 może składać na piśmie utrwalonym w postaci elektronicznej wniosek o zgłoszenie przez ministra właściwego do spraw informatyzacji schematów poświadczania atrybutów do katalogu schematów poświadczania atrybutów prowadzonego przez Komisję Europejską, o którym mowa w art. 8 ust. 1 rozporządzenia 2025/1569, dotyczące atrybutów, których dotyczy to źródło. Wniosek zawiera w informacje, o których mowa w art. 8 ust. 3 rozporządzenia 2025/1569. Art. 22e (….) 3. Minister właściwy do spraw informatyzacji składa wnioski o włączenie schematu poświadczania atrybutów do katalogu schematów poświadczania atrybutów prowadzonego przez Komisję Europejską, o którym mowa w przepisach wydanych na podstawie art. 45d ust. 5, art. 45e ust. 2 i art. 45f ust. 6 i 7rozporządzenia 910/2014, lub o modyfikację schematu w tym katalogu. (……)	działach administracji rządowej obejmuje realizację zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji i telekomunikacji. W związku z tym z tym zobowiązania w tym zakresie powinien realizować minister właściwy do spraw informatyzacji. Minister właściwy do spraw informatyzacji musi jednak uzyskać niezbędne informacje od podmiotów odpowiedzialnych za źródło autentyczne. Mając na uwadze, że zgodnie z art. 8 ust. 3 rozporządzenia 2025/1569 wniosek o dodanie schematu do katalogu schematów poświadczania atrybutów lub o modyfikację schematu mogą składać „właściciele schematu” definiowani jako „podmiot

				5. W przypadku, gdy minister właściwy do spraw informatyzacji jest podmiotem, który wydaje elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, wykorzystujące atrybuty pochodzące źródła autentycznego, za które jest odpowiedzialny, składa z urzędu wniosek, o którym mowa w ust. 3. (……) 7. W przypadku, gdy minister właściwy do spraw informatyzacji jest podmiotem, który wydaje elektroniczne poświadczenia atrybutów, o których mowa w art. 45f rozporządzenia 910/2014, wykorzystujące dane pochodzące z źródła autentycznego, za które nie jest odpowiedzialny, wnioski, o których mowa w ust. 3, składa na wniosek podmiotu, o którym mowa w art. 22d ust. 3. 8. Schematy poświadczania atrybutów do katalogu schematów poświadczania atrybutów prowadzonego przez Komisję Europejską mogą zgłaszać: 1) podmioty odpowiedzialne za źródła autentyczne w rozumieniu art. 3 pkt 47 rozporządzenia 910/2014;	odpowiedzialny za ustanowienie i utrzymanie schematu poświadczania atrybutów” należało ustalić kto może być takim podmiotem zgłaszającym schemat do katalogu Komisji Europejskiej. Przyjęto założenie że mogą być nimi trzy rodzaje podmiotów zainteresowanych ustalaniem schematu poświadczenia atrybutów.

				2) kwalifikowani dostawcy usług zaufania świadczący usługi wydawania kwalifikowanych elektronicznych poświadczeń atrybutów; 3) dostawcy usług online wpisani do rejestru stron ufających europejskim portfelom tożsamości cyfrowej, o którym mowa w art. 22b ust. 1, w zakresie elektronicznych poświadczeń atrybutów wykorzystujących wpisane do rejestru dane, poświadczenia lub atrybuty, o których mowa w pkt 9 załącznika I do rozporządzenia 2025/848.	
Art. 9 ust. 1-2	1. Aby umożliwić elektroniczną weryfikację atrybutów, o której mowa w art. 45e ust. 1 rozporządzenia (UE) nr 910/2014, przez kwalifikowanych dostawców usług zaufania wydających kwalifikowane elektroniczne poświadczenia atrybutów, na wniosek użytkownika państwa członkowskie ustanawiają mechanizmy umożliwiające tę weryfikację i mogą udostępnić pojedyncze punkty weryfikacji atrybutów wymienionych w załączniku VI do tego rozporządzenia, w każdym przypadku gdy atrybuty te opierają się na źródłach autentycznych w sektorze publicznym. Państwa członkowskie publikują informacje na temat procedur składania wniosków o weryfikację i otrzymywania wyników weryfikacji	TAK/NIE	Art. 1 pkt 13 (Art. 22c ust 1 ustawy o usługach zaufania oraz identyfikacji elektronicznej)	Art. 22c. 1. Podmioty sektora publicznego w rozumieniu art. 3 pkt 7 rozporządzenia 910/2014, art. 23odpowiedzialne 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.	Obowiązkową weryfikację, o której mowa w art. 45e ust. 1 rozporządzenia (UE) nr 910/2014 zapewniają w Polsce podmioty publiczne odpowiedzialne na poziomie krajowym za źródła autentyczne. W związku tym podmioty te zapewnią mechanizmy o których mowa w art. 9 ust. 1-2 rozporządzenia 2025/1569, każdy we własnym zakresie, gdyż nie planuje się

	2. Mechanizm weryfikacji zapewnia punkt dostępu, w którym kwalifikowani dostawcy usług zaufania wydający kwalifikowane elektroniczne poświadczenia atrybutów mogą elektronicznie wnioskować o weryfikację atrybutów, o której mowa w art. 45e ust. 1 rozporządzenia (UE) nr 910/2014, w oparciu o źródła autentyczne lub wyznaczonych pośredników uznanych na szczeblu krajowym. Atrybuty podlegające weryfikacji zostaną przekazane punktowi weryfikacji przez kwalifikowanego dostawcę usług zaufania na wniosek użytkownika. Podmiot sektora publicznego lub wyznaczony pośrednik udostępnia, za pośrednictwem punktu weryfikacji, wyniki weryfikacji kwalifikowanym dostawcom usług zaufania wydającym kwalifikowane elektroniczne poświadczenia atrybutów.				utworzenia pojedynczego punktu weryfikacji atrybutów realizowanego przez wyznaczonego pośrednika.
Art. 9 ust. 5	5. Państwa członkowskie mogą wprowadzić kontrole dostępu lub inne mechanizmy weryfikacji zapewniające integralność, autentyczność i poufność w celu ustalenia, czy wnioskodawca jest kwalifikowanym dostawcą usług zaufania i działa na wniosek uprawnionego użytkownika. Państwa członkowskie mogą również wprowadzić mechanizmy kontroli w odniesieniu do stosowania metod weryfikacji, jeżeli uznają to za stosowne, z uwzględnieniem istotnych czynników, w tym tego, czy źródła autentyczne zawierają poufne lub wrażliwe dane osobowe. W przypadku gdy państwa członkowskie ustanawiają te mechanizmy kontroli, muszą publikować informacje na temat zakresu mechanizmów kontroli w ramach informacji, o których mowa w ust. 1.	NIE			Przepis stosowany wprost, nie wymaga wdrożenia.