ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2026/798

z dnia 7 kwietnia 2026 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do norm referencyjnych i specyfikacji dotyczących zdalnej rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej zgodnych ze średnim poziomem bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, jeżeli połączenie to spełnia wymogi wysokiego poziomu bezpieczeństwa

KOMISJA EUROPEJSKA,

uwzględniając 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 ([1]), w szczególności jego art. 5a ust. 24,

a także mając na uwadze, co następuje:

(1) Rejestracja użytkowników w europejskich portfelach tożsamości cyfrowej („portfele") jest kluczowym krokiem w zakresie weryfikacji tożsamości użytkowników portfela, wiązania danych identyfikujących użytkowników z ich portfelami oraz z urządzeniem użytkownika, w którym zainstalowane są jednostki portfela.

(2) Aby zapewnić wysoki poziom zaufania i bezpieczeństwa, a także zharmonizowane podejście we wszystkich państwach członkowskich do rejestracji użytkowników portfela za pomocą procedur zdalnej rejestracji w połączeniu ze środkami identyfikacji elektronicznej odpowiadającymi średniemu poziomowi bezpieczeństwa, w niniejszym akcie wykonawczym ustanawia się specyfikacje i procedury w celu ułatwienia rejestracji użytkowników w europejskim portfelu tożsamości cyfrowej za pomocą środków identyfikacji elektronicznej odpowiadających średniemu poziomowi bezpieczeństwa w połączeniu z dodatkowymi procedurami zdalnej rejestracji, które łącznie spełniają wymogi wysokiego poziomu bezpieczeństwa.

(3) Przedmiotowe normy powinny odzwierciedlać utrwalone praktyki i być powszechnie uznawane w odpowiednich sektorach. Normy te należy dostosować w taki sposób, aby obejmowały wymogi zapewniające bezpieczeństwo i wiarygodność rejestracji użytkowników.

(4) Rozporządzenie wykonawcze Komisji (UE) 2015/1502 ([2]) stanowi, że w przypadku gdy środki identyfikacji elektronicznej są wydawane na wysokim poziomie bezpieczeństwa oraz biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest wymagane powtarzanie procesów potwierdzania i weryfikacji tożsamości. W związku z tym w takim przypadku państwa członkowskie powinny wykorzystywać środki identyfikacji elektronicznej wydane na wysokim poziomie bezpieczeństwa również na potrzeby procesu rejestracji do celów niniejszego rozporządzenia.

(5) W przypadku gdy państwa członkowskie rejestrują użytkowników w portfelach przy użyciu środka identyfikacji elektronicznej, który nie został notyfikowany Komisji, poziom bezpieczeństwa tego środka powinien zostać potwierdzony przez jednostkę oceniającą zgodność zdefiniowaną w art. 2 pkt 13 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([3]) lub przez równoważny organ oraz należy wykazać, że wyniki tej poprzedniej procedury wydawania środka identyfikacji elektronicznej pozostają ważne.

([1]) Dz.U. L 257 z 28.8.2014, s. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Rozporządzenie wykonawcze 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.U. L 235 z 9.9.2015, s. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([3]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) Chociaż załącznik określa wymogi, które należy spełnić, aby osiągnąć określony poziom potwierdzania tożsamości, nie ustanowiono równoważności w odniesieniu do poziomu bezpieczeństwa zdefiniowanego w art. 8 rozporządzenia (UE) nr 910/2014. W związku z tym wymogi określone w załączniku należy uznać za wdrażające wymogi rozporządzenia wykonawczego (UE) 2015/1502 i powinny one być spełniane przez dostawcę danych identyfikujących osobę lub podmiot świadczący usługi potwierdzania tożsamości w imieniu tego dostawcy.

(7) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk i specyfikacji technicznych. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([4]) Komisja powinna poddawać przeglądowi i aktualizować niniejsze rozporządzenie wykonawcze, aby zachować jego aktualność względem globalnych zmian, nowych technologii, norm lub specyfikacji technicznych oraz nadążać za najlepszymi praktykami na rynku wewnętrznym, w szczególności w odniesieniu do rejestracji użytkowników w portfelach.

(8) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([5]), a w stosownych przypadkach, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 ([6]) oraz dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([7]) mają zastosowanie do czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(9) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 30 stycznia 2026 r. ([8]).

(10) Komitet ustanowiony w art. 48 rozporządzenia (UE) nr 910/2014 nie wydał opinii w terminie ustalonym przez swego przewodniczącego,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Normy referencyjne i specyfikacje, o których mowa w art. 5a ust. 24 rozporządzenia (UE) nr 910/2014, określono w załączniku do niniejszego rozporządzenia.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1183 z dnia 11 kwietnia 2024 r. w sprawie zmiany rozporządzenia (UE) nr 910/2014 w odniesieniu do ustanowienia europejskich ram tożsamości cyfrowej (Dz.U. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([8]) *EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets* [Formalne uwagi EIOD do projektu rozporządzenia wykonawczego Komisji w odniesieniu do rejestracji użytkowników w europejskich portfelach tożsamości cyfrowej].

Artykuł 2

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.

Sporządzono w Brukseli dnia 7 kwietnia 2026 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

WYKAZ NORM REFERENCYJNYCH I SPECYFIKACJI

Zgodność ocenia się na podstawie klauzul ETSI TS 119 461 V2.1.1 (2025-02) wymienionych w sekcji 1, z zastrzeżeniem dostosowań wymienionych w sekcji 2.

Sekcja 1 – Klauzule mające zastosowanie

—	5	Ocena ryzyka operacyjnego;
—	6	Polityki i praktyki;
—	7	Zarządzanie usługami potwierdzania tożsamości i ich obsługa;
—	8	Wymogi dotyczące usług potwierdzania tożsamości;
—	9.1	Wprowadzenie, zgodność z niniejszym dokumentem, ogólne wymogi dotyczące wszystkich przypadków użycia;
—	9.2.2	Przypadki użycia z wykorzystaniem dokumentu tożsamości do zdalnego potwierdzania tożsamości z udziałem użytkownika;
—	9.2.3	Przypadki użycia z wykorzystaniem dokumentu tożsamości do automatycznego zdalnego potwierdzania tożsamości;
—	9.2.4	Przypadki użycia do potwierdzania tożsamości poprzez uwierzytelnienie za pomocą środków identyfikacji elektronicznej;
—	9.5	Przypadki użycia do dodatkowego potwierdzania tożsamości w celu podniesienia poziomu potwierdzania tożsamości za pomocą środków identyfikacji elektronicznej z podstawowego na rozszerzony.

Sekcja 2 – Dostosowania

1)	5	Ocena ryzyka operacyjnego;
	—	OVR-5-01: Stosuje się wymogi określone w klauzuli 5 normy ETSI EN 319 401 [1].
	—	*Uwaga 1:* Jeżeli potwierdzania tożsamości dokonuje sam dostawca danych identyfikujących osobę, ocena ryzyka dostawcy danych identyfikujących osobę może obejmować potwierdzenie tożsamości.
2)	6.1	Oświadczenie dotyczące praktyki w zakresie usługi potwierdzania tożsamości
	—	OVR-6.1-02: Dostawca usług potwierdzania tożsamości (IPSP) określa w swoim oświadczeniu dotyczącym praktyki przypadki użycia, w odniesieniu do których deklaruje zgodność z niniejszym dokumentem.
	—	*Uwaga 1*: Jeżeli potwierdzenia tożsamości dokonuje sam dostawca danych identyfikujących osobę, oświadczenie dotyczące praktyki dostawcy danych identyfikujących osobę w zakresie usługi potwierdzania tożsamości może obejmować informacje dotyczące potwierdzania tożsamości i nie ma potrzeby sporządzania specjalnego oświadczenia dotyczącego praktyki w zakresie potwierdzania tożsamości.
3)	7.9	Zarządzanie podatnością na zagrożenia i incydentami
	—	OVR-7.9-02: Obowiązki sprawozdawcze zgodnie z normą ETSI EN 319401 [1] REQ-7.9.2-02X i klauzulą 7.9.3 wypełnia się w zależności od kontekstu potwierdzania tożsamości oraz obowiązków dostawcy danych identyfikujących osobę korzystającego z usługi świadczonej przez dostawcę usługi potwierdzania tożsamości.
	—	Przykład: Zgłaszanie danych organowi nadzorczemu nadzorującemu dostawcę europejskich portfeli tożsamości cyfrowej mającego siedzibę w wyznaczającym państwie członkowskim może odbywać się we współpracy między IPSP a dostawcą danych identyfikujących osobę.

4) 7.10 Gromadzenie dowodów

— OVR-7.10-01: Stosuje się wymogi określone w klauzuli 7.10 normy ETSI EN 319 401 [1].

— *Uwaga 1*: Długoterminowe wymogi dotyczące zatrzymywania dowodów mogą być spełnione przez dostawcę danych identyfikujących osobę wnioskującego o potwierdzenie tożsamości, a nie przez IPSP, jeżeli oba te podmioty są różnymi podmiotami.

— *Uwaga 2*: Zastosowanie mają wymogi klauzuli 8.5.2 niniejszego dokumentu.

5) 7.11 Zarządzanie ciągłością działania

— OVR-7.11-02: Procesy zarządzania kryzysowego zgodnie z normą ETSI EN 319401 [1], REQ-7.11.3-01X są zgodne z wymogami kontekstu potwierdzania tożsamości i obowiązkami dostawcy danych identyfikujących osobę korzystającego z usługi IPSP.

6) 7.12 Zakończenie działalności i plany zakończenia działalności

— OVR-7.12-01: Stosuje się wymogi określone w klauzuli 7.12 normy ETSI EN 319401 [1], z wyjątkiem REQ-7.12-11.

— *Uwaga*: Jeżeli IPSP i dostawca danych identyfikujących osobę wnioskujący o potwierdzenie tożsamości są różnymi podmiotami, mogą uzgodnić wzajemną lub jednostronną pomoc w opracowywaniu planów zakończenia działalności.

7) 8.1 Inicjacja

— INI-8.1-05: W przypadku przerwania lub niepowodzenia procesu zdalnego potwierdzania tożsamości IPSP zapewnia, aby osobom fizycznym udostępniono wystarczające wyjaśnienia i środki zaradcze, w szczególności w przypadku automatycznego zdalnego potwierdzania tożsamości. Informacje te powinny zapewniać osobom fizycznym możliwość skutecznej reakcji w celu szybkiego rozwiązania problemu oraz, w razie potrzeby, skorzystania z przysługujących im praw jako osób, których dane dotyczą, takich jak prawo do sprostowania lub możliwość zaskarżenia decyzji do właściwego administratora.

8) 8.2.1 Wymogi ogólne

— COL-8.2.1-08: IPSP wdraża środki zapewniające zgodność z wymogami uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych zgodnie z art. 25 rozporządzenia (UE) 2016/679 podczas procesu rejestracji, w szczególności w odniesieniu do przetwarzania danych biometrycznych. Odpowiednie środki mogą obejmować odpowiednie kontrole kryptograficzne, urządzenia i środki organizacyjne zwiększające prywatność. Środki te powinny ograniczać gromadzenie danych do tego, co jest absolutnie niezbędne do przetwarzania danych biometrycznych i wszelkich innych danych osobowych, które mają być gromadzone z fizycznych i cyfrowych źródeł identyfikacji w celu powiązania danych identyfikujących użytkownika z jego portfelami i urządzeniem użytkownika, w którym zainstalowana jest jednostka portfela.

9) 8.2.4 Korzystanie z istniejących środków identyfikacji elektronicznej jako dowodów

— [WARUNKOWO] COL-8.2.4-02X: Jeżeli podstawowy poziom potwierdzania tożsamości jest ukierunkowany, środki identyfikacji elektronicznej muszą zostać notyfikowane co najmniej na poziomie średniego poziomu bezpieczeństwa lub ich poziom bezpieczeństwa musi zostać potwierdzony przez akredytowaną jednostkę oceniającą zgodność zdefiniowaną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008 lub przez równoważny organ, a jeżeli spełnione są wszystkie mające zastosowanie wymogi, wynikiem oceny jest zaświadczenie o zgodności oparte na audycie certyfikacyjnym. Ten formalny proces certyfikacji opiera się na procesie oceny bezpieczeństwa, który odnosi się do poziomów bezpieczeństwa określonych dla notyfikowanych środków identyfikacji elektronicznej lub certyfikowanych europejskich portfeli tożsamości cyfrowej na podstawie rozporządzenia (UE) nr 910/2014 [i.25].

— COL-8.2.4-02 A: nieważny.

10) 8.3.1 Wymogi ogólne

— VAL-8.3.1-11X: W ramach procesu potwierdzania tożsamości weryfikuje się, czy dowody są ważne w momencie potwierdzania tożsamości.

11) 8.3.3 Walidacja fizycznego dokumentu tożsamości

— VAL-8.3.3-21: Skuteczność środków służących spełnieniu wymogów VAL-8.3.3-05X, VAL-8.3.3-05 A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07 A i VAL-8.3.3-07X potwierdza akredytowana jednostka oceniająca zgodność określona w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008 lub równoważny organ.

— VAL-8.3.3-22: Obraz referencyjny twarzy z fizycznego dokumentu tożsamości jest pobierany przy użyciu komunikacji zbliżeniowej, a w ramach procesu dokonuje się biernego lub aktywnego uwierzytelnienia mikroprocesora na fizycznym dokumencie tożsamości.

12) 9.1 Wprowadzenie, zgodność z niniejszym dokumentem, ogólne wymogi dotyczące wszystkich przypadków użycia

— USE-9.1-01X: Aby zachować zgodność z niniejszym dokumentem, proces potwierdzania tożsamości musi być zgodny z przypadkiem użycia określonym w pkt 9.5 niniejszego dokumentu dla rozszerzonego poziomu potwierdzania tożsamości.

— USE-9.1-03X: nieważny.

13) 9.2.3.4 Przypadek użycia do zautomatyzowanych procesów

— USE-9.2.3.4-04: IPSP ustanawia wartości docelowe wskaźnika błędnych akceptacji (FAR) i wskaźnika błędnych odrzuceń (FRR) na podstawie analizy ryzyka i stosowanej przez niego procedury analizy zagrożeń, przestrzegając metody określonej w sprawozdaniu ENISA pt. „Metodyka sektorowych ocen cyberbezpieczeństwa" [i.28] lub równoważnej metodyki w ramach w pełni zautomatyzowanych procesów potwierdzania tożsamości. Wartości docelowe stosowane przez IPSP nie mogą przekraczać wartości ustalonych dla hybrydowych przypadków użycia, o ile takie występują. IPSP utrzymuje te wartości docelowe FAR i FRR w sposób spójny, uzasadniony analizą ryzyka i procedurą analizy zagrożeń.

14) 9.5.1 Wymogi ogólne

— Ustęp pierwszy: W przypadku gdy wnioskodawca jest osobą fizyczną, w tym osobą fizyczną reprezentującą osobę prawną, a tożsamość wnioskodawcy została potwierdzona zgodnie z podstawowym poziomem potwierdzania tożsamości poprzez uwierzytelnienie za pomocą środka identyfikacji elektronicznej i wymagane jest podniesienie poziomu potwierdzania tożsamości i do poziomu rozszerzonego, zastosowanie mają następujące wymogi.

— USE-9.5.1-08: Dodatkowe potwierdzanie tożsamości wymagane w celu wzmocnienia wiarygodności tożsamości ma zastosowanie wyłącznie do identyfikacji elektronicznej, która nie została wydana w oparciu o zautomatyzowane porównanie obrazów twarzy na potrzeby procesu pierwotnego wydania.

15) 9.5.2 Przypadek użycia do podnoszenia poziomu potwierdzania tożsamości do poziomu rozszerzonego poprzez pełne potwierdzanie tożsamości za pomocą dokumentu tożsamości

— USE-9.5.2-01: Potwierdzanie tożsamości w celu podniesienia poziomu potwierdzania tożsamości z podstawowego na rozszerzony musi być zgodne z wymogami dotyczącymi rozszerzonego poziomu potwierdzania tożsamości w odniesieniu do jednego z przypadków użycia opisanych w pkt 9.2.2 lub 9.2.3 niniejszego dokumentu dla rozszerzonego poziomu potwierdzania tożsamości.

16) 9.5.3 Przypadek użycia do podnoszenia poziomu potwierdzania tożsamości do rozszerzonego poprzez wykorzystanie wcześniej pobranego referencyjnego obrazu twarzy.

— USE-9.5.3-01: Aby uzyskać referencyjny obraz twarzy i powiązać niezbędne atrybuty tożsamości z tym referencyjnym obrazem twarzy, stosuje się proces potwierdzania tożsamości spełniający wymogi poziomu rozszerzonego w odniesieniu do jednego z przypadków użycia opisanych w pkt 9.2.2 lub 9.2.3 niniejszego dokumentu lub proces potwierdzania tożsamości poddany wzajemnej ocenie lub certyfikowany przez akredytowaną jednostkę oceniającą zgodność określoną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008 lub równoważny organ w celu zapewnienia wysokiego poziomu bezpieczeństwa zgodnie z rozporządzeniem (UE) nr 910/2014 [i.25].