Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/2977

4.12.2024

# 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

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

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. 23,

a także mając na uwadze, co następuje:

(1) Europejskie ramy tożsamości cyfrowej ustanowione rozporządzeniem (UE) nr 910/2014 stanowią kluczowy element budowy bezpiecznego i interoperacyjnego ekosystemu tożsamości cyfrowej w całej Unii. Ramy te – których podstawę stanowią europejskie portfele tożsamości cyfrowej („portfele") – mają na celu ułatwienie dostępu do usług we wszystkich państwach członkowskich, jednocześnie zapewniając ochronę danych osobowych i prywatności.

(2) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([3]) mają zastosowanie do wszystkich czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia.

(3) W art. 5a ust. 23 rozporządzenia (UE) nr 910/2014 zobowiązano Komisję, w razie potrzeby, do ustanowienia odpowiednich specyfikacji i procedur. Ustanawia się je za pomocą czterech rozporządzeń wykonawczych dotyczących: protokołów i interfejsów: rozporządzenie wykonawcze Komisji (UE) 2024/2982 ([4]), integralności i podstawowych funkcji: rozporządzenie wykonawcze Komisji (UE) 2024/2979 ([5]), danych identyfikujących osobę i elektronicznego poświadczenia atrybutów: rozporządzenie wykonawcze Komisji (UE) 2024/2977 ([6]), a także notyfikowania Komisji: rozporządzenie wykonawcze Komisji (UE) 2024/2980 ([7]). W niniejszym rozporządzeniu ustanawia się odpowiednie wymogi dotyczące danych identyfikujących osobę i elektronicznych poświadczeń atrybutów, które mają być wydawane europejskim portfelom tożsamości cyfrowej.

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

([2]) 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).

([3]) 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).

([4]) Rozporządzenie wykonawcze Komisji (UE) 2024/2982 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do protokołów i interfejsów, które mają być obsługiwane przez europejskie ramy tożsamości cyfrowej (Dz.U. L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Rozporządzenie wykonawcze Komisji (UE) 2024/2979 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej (Dz.U. L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Rozporządzenie wykonawcze Komisji (UE) 2024/2977 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wydawanych europejskim portfelom tożsamości cyfrowej (Dz.U. L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Rozporządzenie wykonawcze Komisji (UE) 2024/2980 z dnia 28 listopada 2024 r. ustanawiające 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.U. L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm lub specyfikacji technicznych. Aby zapewnić maksymalną harmonizację działań państw członkowskich w zakresie opracowywania i certyfikacji portfeli, specyfikacje techniczne określone w niniejszym rozporządzeniu wykonawczym opierają się na pracach przeprowadzonych na podstawie zalecenia Komisji (UE) 2021/946 z dnia 3 czerwca 2021 r. w sprawie wspólnego unijnego zestawu narzędzi na potrzeby skoordynowanego podejścia do europejskich ram tożsamości cyfrowej ([8]), a w szczególności architektury i ram odniesienia, które są jego częścią. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([9]) Komisja powinna, w razie potrzeby, poddawać niniejsze rozporządzenie wykonawcze przeglądowi i aktualizacji, aby zachować aktualność względem globalnych zmian, architektury i ram odniesienia oraz przestrzegać najlepszych praktyk na rynku wewnętrznym.

(5) Aby zapewnić uwzględnienie ochrony danych na etapie projektowania i domyślną ochronę danych, portfele powinny być wyposażone w szereg funkcji zapewniających lepszą ochronę prywatności, by uniemożliwić dostawcom środków identyfikacji elektronicznej i elektronicznych poświadczeń atrybutów łączenie danych osobowych uzyskanych w ramach świadczenia innych usług z danymi osobowymi przetwarzanymi w celu świadczenia usług objętych zakresem rozporządzenia (UE) nr 910/2014.

(6) W celu zagwarantowania harmonizacji wszystkie portfele powinny być wyposażone w pewne wspólne funkcje, w tym umożliwiać bezpieczne żądanie, otrzymywanie, wybieranie, łączenie, przechowywanie, usuwanie, udostępnianie i prezentację – pod wyłączną kontrolą użytkownika portfela – danych identyfikujących osobę i elektronicznych poświadczeń atrybutów. Aby zapewnić możliwość przetwarzania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów za pośrednictwem każdej jednostki portfela, specyfikacje techniczne dotyczące atrybutów danych identyfikujących osobę, formatu danych i infrastruktury wymaganej do zapewnienia odpowiedniej wiarygodności danych identyfikujących osobę muszą być obsługiwane przez wszystkie rozwiązania w zakresie portfela. Ponadto wspólne specyfikacje dotyczące atrybutów danych identyfikujących osobę mają zapewnić możliwość wykorzystywania tych danych do celów dopasowywania tożsamości, gdy zajdzie taka potrzeba.

(7) Państwa członkowskie są zobowiązane do zapewnienia, aby portfele były wyposażone w funkcję uwierzytelniania stron ufających, dostawców danych identyfikujących osobę i dostawców elektronicznych poświadczeń atrybutów niezależnie od miejsca ich siedziby w Unii. W tym celu podczas potwierdzania swojej tożsamości wobec jednostek portfela podmioty te powinny korzystać z certyfikatów dostępu strony ufającej portfela. Aby zagwarantować interoperacyjność tych certyfikatów we wszystkich portfelach zapewnianych w Unii, certyfikaty dostępu stron ufających portfela powinny spełniać wspólne normy. Komisja, we współpracy z państwami członkowskimi, powinna ściśle monitorować opracowywanie nowych lub alternatywnych norm, które mogłyby posłużyć jako podstawa dla certyfikatów dostępu strony ufającej. W szczególności należy ocenić modele zaufania, które dowiodły swojej skuteczności i bezpieczeństwa w państwach członkowskich.

(8) Aby zapewnić przejrzystość wobec użytkowników portfela, państwa członkowskie powinny publikować informacje o tym, które rozwiązania w zakresie portfela są obsługiwane przez dostawców danych identyfikujących osobę mających siedzibę na ich terytorium. Z uwagi na konieczność zagwarantowania możliwie największej wiarygodności tożsamości użytkownika należy wprowadzić wymóg zapewnienia wspólnego wysokiego poziomu bezpieczeństwa w zakresie potwierdzania tożsamości użytkowników portfela przed wydaniem danych identyfikujących osobę, odpowiadający wysokiemu poziomowi bezpieczeństwa określonemu w odniesieniu do środków identyfikacji elektronicznej na podstawie rozporządzenia (UE) nr 910/2014. W ten sposób jednostki portfela zapewnią najwyższy dostępny poziom wiarygodności środków identyfikacji w całej Unii. Podczas wprowadzania użytkowników portfela do systemu na wysokim poziomie bezpieczeństwa można korzystać z różnych procedur bezpieczeństwa, na przykład w przypadku gdy zweryfikowano, że użytkownik portfela posiada dowody identyfikacji fotograficznej lub biometrycznej uznawane, lecz niewydawane przez państwo członkowskie, w którym złożono wniosek o wydanie środka identyfikacji elektronicznej, a dowody te odzwierciedlają deklarowaną tożsamość, dowody te należy sprawdzić w celu ustalenia, czy są one ważne zgodnie z odpowiednim wiarygodnym źródłem.

(9) Aby wspierać interoperacyjność, elektroniczne poświadczenia atrybutów powinny być zgodne ze zharmonizowanymi wymogami w zakresie formatu.

(10) Mechanizmy uwierzytelniania dostawców elektronicznych poświadczeń atrybutów oraz weryfikacji autentyczności i ważności jednostek portfela przez tego dostawcę powinny mieć zastosowanie przed wydaniem poświadczeń do jednostek portfela, aby chronić dane użytkowników portfela i zapewnić autentyczność elektronicznych poświadczeń atrybutów.

([8]) Dz.U. L 210 z 14.6.2021, s. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

(11) Aby uniknąć wykorzystywania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów, które utraciły ważność prawną po ich wydaniu jednostce portfela, a także polegania na tych danych, dostawcy danych identyfikujących osobę i elektronicznych poświadczeń atrybutów powinni opublikować politykę określającą okoliczności i procedury unieważnienia.

(12) W celu zagwarantowania, że dane identyfikujące osobę reprezentują użytkownika portfela w sposób niepowtarzalny, państwa członkowskie powinny – oprócz obowiązkowych atrybutów zbioru danych identyfikujących osobę określonych w niniejszym rozporządzeniu – zapewnić atrybuty opcjonalne niezbędne do zapewnienia niepowtarzalnego charakteru zbioru danych identyfikujących osobę.

(13) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([10]) skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 30 września 2024 r.

(14) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu, o którym mowa w art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

*Artykuł 1*

**Przedmiot i zakres stosowania**

W niniejszym rozporządzeniu ustanawia się przepisy dotyczące wydawania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów do jednostek portfela; przedmiotowe przepisy podlegają regularnej aktualizacji w celu zapewnienia zgodności z rozwojem technologii i opracowywanymi normami oraz z pracami prowadzonymi na podstawie zalecenia Komisji (UE) 2021/946, w szczególności z architekturą i ramami odniesienia.

*Artykuł 2*

**Definicje**

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „użytkownik portfela” oznacza użytkownika, który kontroluje jednostkę portfela;

2) „jednostka portfela” oznacza niepowtarzalną konfigurację rozwiązania w zakresie portfela, która obejmuje instancje portfela, bezpieczne aplikacje kryptograficzne portfela i bezpieczne urządzenia kryptograficzne portfela dostarczane przez dostawcę portfela indywidualnemu użytkownikowi portfela;

3) „rozwiązanie w zakresie portfela” oznacza połączenie oprogramowania, sprzętu, usług, ustawień i konfiguracji, z uwzględnieniem instancji portfela, co najmniej jednej bezpiecznej aplikacji kryptograficznej portfela oraz co najmniej jednego bezpiecznego urządzenia kryptograficznego portfela;

4) „dostawca danych identyfikujących osobę” oznacza osobę fizyczną lub prawną odpowiedzialną za wydanie i unieważnienie danych identyfikujących osobę oraz za zapewnienie, aby dane identyfikujące osobę odnoszące się do użytkownika były powiązane kryptograficznie z jednostką portfela;

5) „poświadczenie jednostki portfela” oznacza obiekt danych, który opisuje komponenty jednostki portfela lub umożliwia uwierzytelnienie oraz walidację tych komponentów;

6) „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;

7) „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]) 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).

8) „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;

9) „dostawca portfela” oznacza osobę fizyczną lub prawną, która dostarcza rozwiązania w zakresie portfela;

10) „aktywa krytyczne” oznaczają aktywa wewnątrz jednostki portfela lub z nią związane o tak istotnym znaczeniu, że naruszenie ich dostępności, poufności lub integralności miałoby bardzo poważny, szkodliwy wpływ na zdolność do polegania na danej jednostce portfela;

11) „strona ufająca portfela” oznacza stronę ufającą, która zamierza polegać na jednostkach portfela w celu świadczenia usług publicznych lub prywatnych za pośrednictwem cyfrowej interakcji;

12) „certyfikat dostępu strony ufającej portfela” oznacza certyfikat pieczęci lub podpisów elektronicznych uwierzytelniający i walidujący stronę ufającą portfela, wydany przez dostawcę certyfikatów dostępu strony ufającej portfela;

13) „dostawca certyfikatów dostępu strony ufającej portfela” oznacza osobę fizyczną lub prawną upoważnioną przez państwo członkowskie do wydawania certyfikatów dostępu strony ufającej stronom ufającym portfela zarejestrowanym w tym państwie członkowskim.

*Artykuł 3*

**Wydawanie danych identyfikujących osobę do jednostek portfela**

1. Dostawcy danych identyfikujących osobę wydają dane identyfikujące osobę do jednostek portfela zgodnie z systemami identyfikacji elektronicznej, w ramach których dostarczane są rozwiązania w zakresie portfela.

2. Dostawcy danych identyfikujących osobę zapewniają, aby dane identyfikujące osobę wydane do jednostek portfela zawierały informacje niezbędne do uwierzytelnienia i walidacji danych identyfikujących osobę.

3. Dostawcy danych identyfikujących osobę zapewniają, aby dane identyfikujące osobę wydawane do jednostek portfela były zgodne ze specyfikacjami technicznymi określonymi w załączniku.

4. Państwa członkowskie zapewniają, aby dane identyfikujące osobę wydane danemu użytkownikowi portfela były niepowtarzalne na poziomie danego państwa członkowskiego.

5. Dostawcy danych identyfikujących osobę zapewniają, aby wydawane przez nich dane identyfikujące osobę były powiązane kryptograficznie z jednostką portfela, której zostały wydane.

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.

7. Państwa członkowskie wprowadzają do systemu użytkowników portfela zgodnie z określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 ([11]) 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.

8. Wydając dane identyfikujące osobę do jednostek portfela, dostawcy danych identyfikujących osobę potwierdzają swoją tożsamość wobec jednostek portfela, korzystając z certyfikatu dostępu strony ufającej portfela lub za pomocą innego mechanizmu uwierzytelniania zgodnie z systemem identyfikacji elektronicznej notyfikowanym na wysokim poziomie bezpieczeństwa.

([11]) 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).

9. Przed wydaniem danych identyfikujących osobę jednostce portfela dostawcy danych identyfikujących osobę uwierzytelniają i walidują poświadczenie jednostki portfela danej jednostki portfela oraz weryfikują, czy dana jednostka portfela należy do rozwiązania w zakresie portfela akceptowanego przez dostawcę danych identyfikujących osobę, lub korzystają z innego mechanizmu uwierzytelniania zgodnie z systemem identyfikacji elektronicznej notyfikowanym na wysokim poziomie bezpieczeństwa.

*Artykuł 4*

**Wydawanie elektronicznych poświadczeń atrybutów do jednostek portfela**

1. Elektroniczne poświadczenia atrybutów wydawane do jednostek portfela muszą być zgodne z co najmniej jedną z norm ujętych w wykazie określonym w załączniku I do rozporządzenia wykonawczego (UE) 2024/2979.

2. Dostawcy elektronicznych poświadczeń atrybutów potwierdzają swoją tożsamość wobec jednostek portfela przy użyciu swojego certyfikatu dostępu strony ufającej portfela.

3. Dostawcy elektronicznych poświadczeń atrybutów zapewniają, aby elektroniczne poświadczenia atrybutów wydawane do jednostek portfela zawierały informacje niezbędne do uwierzytelniania i walidacji tych elektronicznych poświadczeń atrybutów.

*Artykuł 5*

**Unieważnienie danych identyfikujących osobę**

1. Dostawcy danych identyfikujących osobę wydanych jednostce portfela muszą posiadać spisane ogólnodostępne zasady dotyczące zarządzania statusem ważności, w tym, w stosownych przypadkach, warunki, na jakich takie dane identyfikujące osobę mogą zostać niezwłocznie unieważnione.

2. Wyłącznie dostawcy danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów mogą unieważnić wydane przez nich dane identyfikujące osobę lub elektroniczne poświadczenia atrybutów.

3. W sytuacji, gdy dostawcy danych identyfikujących osobę unieważnią dane identyfikujące osobę, w ciągu 24 godzin i za pomocą specjalnych i bezpiecznych kanałów informują użytkowników portfela, których dotyczą te dane identyfikujące osobę, o unieważnieniu i jego przyczynach. Informacje należy przekazać w formie zwięzłej, łatwo dostępnej oraz używając jasnego i przystępnego języka.

4. W przypadku gdy dostawcy danych identyfikujących osobę unieważnią dane identyfikujące osobę wydane do jednostek portfela, muszą tego dokonać w każdym z następujących przypadków:

a) na wyraźne żądanie użytkownika portfela, którego jednostce portfela wydano dane identyfikujące osobę lub elektroniczne poświadczenie atrybutów;

b) w przypadku gdy poświadczenie jednostki portfela, do którego wydano dane identyfikujące osobę, zostało unieważnione;

c) w innych sytuacjach określonych przez dostawców danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów w ich zasadach, o których mowa w ust. 1.

5. Dostawcy danych identyfikujących osobę wydanych do jednostki portfela zapewniają, aby unieważnień nie można było cofnąć.

6. Unieważnione dane identyfikujące osobę pozostają dostępne tak długo, jak wymaga tego prawo Unii lub prawo krajowe.

7. W przypadku gdy dostawcy danych identyfikujących osobę unieważnią dane identyfikujące osobę wydane do jednostek portfela, udostępniają publicznie – w sposób gwarantujący ochronę prywatności – status ważności wydawanych przez siebie danych identyfikujących osobę oraz wskazują lokalizację tych informacji w danych identyfikujących osobę.

8. Dostawcy danych identyfikujących osobę umożliwiają stosowanie technik ochrony prywatności, które zapewniają brak możliwości powiązania, w przypadku gdy elektroniczne poświadczenia atrybutów nie wymagają identyfikacji użytkownika.

*Artykuł 6*

**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.

Sporządzono w Brukseli dnia 28 listopada 2024 r.

*W imieniu Komisji*
*Przewodnicząca*
Ursula VON DER LEYEN

*ZAŁĄCZNIK*

**SPECYFIKACJE TECHNICZNE DOTYCZĄCE DANYCH IDENTYFIKUJĄCYCH OSOBĘ, O KTÓRYCH MOWA W ART. 3 UST. 3**

1. **Zbiór danych identyfikujących osobę fizyczną**

*Tabela 1*

**Obowiązkowe dane identyfikujące osobę w przypadku osoby fizycznej**

| Identyfikator danych | Definicja | Występowanie |
|---|---|---|
| family_name | Aktualne nazwisko (nazwiska) użytkownika, którego dotyczą dane identyfikujące osobę. | Obowiązkowe |
| given_name | Aktualne imię (imiona), w tym, w stosownych przypadkach, drugie imię (imiona) użytkownika, którego dotyczą dane identyfikujące osobę. | Obowiązkowe |
| birth_date | Dzień, miesiąc i rok urodzenia użytkownika, którego dotyczą dane identyfikujące osobę. | Obowiązkowe |
| birth_place | 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. | Obowiązkowe |
| nationality | Co najmniej jeden kod państwa alfa-2 według normy ISO 3166-1, odzwierciedlający obywatelstwo użytkownika, którego dotyczą dane identyfikujące osobę. | Obowiązkowe |

W przypadku gdy wartość atrybutu nie jest znana danej osobie lub nie może zostać wydana w inny sposób jako część zbioru danych identyfikujących osobę, państwa członkowskie powinny zastosować wartość atrybutu odpowiednią do danej sytuacji.

*Tabela 2*

**Opcjonalne dane identyfikujące osobę w przypadku osoby fizycznej**

| Identyfikator danych | Definicja | Występowanie |
|---|---|---|
| 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 |

| Identyfikator danych | Definicja | Występowanie |
|---|---|---|
| resident_city | Gmina, miasto lub wieś aktualnego zamieszkania użytkownika, którego dotyczą dane identyfikujące osobę. | Opcjonalne |
| 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.<br>W przypadku gdy państwa 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. | Opcjonalne |
| 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:<br>0 = nieznana;<br>1 = mężczyzna;<br>2 = kobieta;<br>3 = inna;<br>4 = osoba interseksualna;<br>5 = różnorodna;<br>6 = otwarta;<br>9 = nie dotyczy;<br>W odniesieniu do wartości 0, 1, 2 i 9 stosuje się normę ISO/IEC 5218. | Opcjonalne |
| 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 |

2. **Zbiór danych identyfikujących osobę prawną**

*Tabela 3*

**Obowiązkowe dane identyfikujące osobę w przypadku osoby prawnej**

| Element danych | Występowanie |
|---|---|
| aktualna nazwa prawna | Obowiązkowe |
| niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy w czasie. | Obowiązkowe |

W przypadku gdy element danych nie jest znany danej osobie lub nie może zostać wydany w inny sposób jako część zbioru danych identyfikujących osobę, państwa członkowskie powinny zastosować wartość atrybutu odpowiednią do danej sytuacji.

*Tabela 4*

**Opcjonalne dane identyfikujące osobę w przypadku osoby prawnej**

| Element danych | Występowanie |
|---|---|
| aktualny adres | Opcjonalne |
| 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 |

3. **Zbiór metadanych dotyczących danych identyfikujących osobę**

*Tabela 5*

**Metadane dotyczące danych identyfikujących osobę**

| Identyfikator danych | Definicja | Występowanie |
|---|---|---|
| expiry_date | Data (i w miarę możliwości godzina) wygaśnięcia danych identyfikujących osobę | Obowiązkowe |
| 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 do wydawania danych identyfikujących osobę. | Obowiązkowe |
| issuing_country | Kod państwa alfa-2, jak określono w normie ISO 3166-1, państwa lub terytorium dostawcy danych identyfikujących osobę. | Obowiązkowe |

| Identyfikator danych | Definicja | Występowanie |
|---|---|---|
| document_number | Numer danych identyfikujących osobę nadany przez dostawcę danych identyfikujących osobę. | Opcjonalne |
| issuing_jurisdiction | 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 dla państwa wydającego. | Opcjonalne |
| lokalizacja_status | Umiejscowienie informacji o statusie ważności danych identyfikujących osobę, w przypadku gdy dostawcy danych identyfikujących osobę unieważniają dane identyfikujące osobę. | Opcjonalne |

4. **Kodowanie atrybutów danych identyfikujących osobę**

Dane identyfikujące osobę wydaje się w dwóch formatach:

1) formacie określonym w normie ISO/IEC 18013-5:2021;

2) formacie „Verifiable Credentials Data Model 1.1.” (model weryfikowalnych danych uwierzytelniających 1.1.), zalecenie W3C, 3 marca 2022 r.

5. **Szczegółowe informacje dotyczące infrastruktury zaufania**

Wykaz dostawców danych identyfikujących osobę udostępniony przez Komisję zgodnie z rozporządzeniem wykonawczym (UE) 2024/2980 ustanawiającym zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do notyfikowania Komisji w związku z ekosystemem europejskiego portfela tożsamości musi umożliwiać uwierzytelnianie danych identyfikujących osobę.