Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2024/2982

4.12.2024

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

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 w państwach członkowskich osobom fizycznym i prawnym, 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 protokołów i interfejsów.

([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 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]), w szczególności na podstawie architektury i ram odniesienia. 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 przejrzystość i wiarygodność stron ufających portfela wobec użytkowników portfela, protokoły i interfejsy stosowane w rozwiązaniach w zakresie portfela powinny zapewniać użytkownikom portfela niezawodny mechanizm uwierzytelniania stron ufających portfela i innych jednostek portfela. Z kolei dostawcy portfela powinni zapewnić mechanizm uwierzytelniania i walidacji jednostek portfela, tak aby strony ufające mogły otrzymać gwarancje w zakresie wiarygodności i autentyczności jednostek portfela. Ponadto infrastruktura techniczna portfeli powinna być również zaprojektowana w taki sposób, aby zagwarantować, że jedynie minimalna niezbędna ilość danych zostanie przekazana wyłącznie upoważnionym stronom ufającym, przy jednoczesnym zachowaniu braku możliwości powiązania ze sobą poszczególnych transakcji. Aby ułatwić wydawanie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów, wszystkie rozwiązania w zakresie portfela powinny obsługiwać minimalny zestaw protokołów i interfejsów.

(6) Do zagwarantowania użyteczności rozwiązań w zakresie portfela we wszystkich państwach członkowskich niezbędne jest, aby rozwiązania w zakresie portfela były zgodne ze wspólnymi specyfikacjami technicznymi, w przypadku gdy dane identyfikujące osobę i elektroniczne poświadczenia atrybutów są przedstawiane stronom ufającym za pośrednictwem portfeli, zarówno w scenariuszu na odległość, jak i w scenariuszu zbliżeniowym. Ponadto jednostki portfela mogą obsługiwać inne protokoły i interfejsy na potrzeby określonych przypadków użycia.

(7) 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. Jak określono w rozporządzeniu (UE) nr 910/2014, strony ufające nie mogą zwracać się do użytkowników o udostępnienie jakichkolwiek danych innych niż te, które zostały wskazane do celów zamierzonego użycia portfeli w procesie rejestracji. Użytkownicy portfela powinni mieć możliwość weryfikacji danych dotyczących rejestracji stron ufających w dowolnym momencie. Jednostki portfela powinny ponadto dawać możliwość pokazywania użytkownikom certyfikatów rejestracji strony ufającej portfela, gdy są one dostępne, w ramach żądania atrybutów. Powinno to umożliwić użytkownikom portfela weryfikację, że atrybuty, których żąda strona ufająca portfela mieszczą się w zakresie jej zarejestrowanych atrybutów, dając pewność, że żądanie jest uzasadnione i wiarygodne.

(8) W celu ochrony danych użytkowników portfela dostawcy portfela powinni zapewnić, aby jednostki portfela dokonywały walidacji żądań wystosowywanych przez strony ufające portfela lub inne jednostki portfela przed udostępnieniem jakichkolwiek danych. Z tego samego powodu i zgodnie z art. 5a ust. 4 lit. d) ppkt (ii) rozporządzenia (UE) nr 910/2014 dostawcy portfela powinni zapewnić, aby jednostki portfela umożliwiały użytkownikom portfela zażądanie do stron ufających portfela usunięcia danych.

(9) Aby umożliwić szybkie reagowanie w przypadku jakichkolwiek obaw dotyczących ochrony danych związanych z art. 5a ust. 4 lit. d) ppkt (iii) rozporządzenia (UE) nr 910/2014, dostawcy portfela powinni zagwarantować, że rozwiązania w zakresie portfela są wyposażone w mechanizmy zgłaszania strony ufającej właściwemu krajowemu organowi ochrony danych. Należy pozostawić dostawcom portfela i organom ochrony danych odpowiednią elastyczność w ustanawianiu stosownych mechanizmów współpracy z organami ochrony danych państw członkowskich.

(10) 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.

([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).

([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).

(11) 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 zasady dotyczące protokołów i interfejsów rozwiązań w zakresie portfela w odniesieniu do:

1) wydawania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów do jednostek portfela;

2) prezentacji atrybutów danych identyfikujących osobę i elektronicznych poświadczeń atrybutów stronom ufającym portfela i innym jednostkom portfela;

3) przekazywania żądań usunięcia danych stronom ufającym portfela;

4) zgłaszania stron ufających portfela organom nadzorczym ustanowionym na podstawie art. 51 rozporządzenia (UE) 2016/679;

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

2) „użytkownik portfela" oznacza użytkownika, który kontroluje jednostkę 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) „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;

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

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;

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) „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;

10) „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;

11) „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;

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

13) „wbudowane reguły ujawniania” oznaczają zbiór zasad wbudowanych w elektronicznym poświadczeniu atrybutów przez dostawcę tego poświadczenia; zasady te określają warunki, jakie musi spełnić strona ufająca portfela, aby uzyskać dostęp do elektronicznego poświadczenia atrybutów;

14) „certyfikat rejestracji strony ufającej portfela” oznacza obiekt danych, który wskazuje atrybuty, które zarejestrowała strona ufająca z zamiarem ich żądania od użytkowników;

15) „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;

16) „powiązanie kryptograficzne” oznacza metodę łączenia danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów z jednostkami portfela za pomocą środków kryptograficznych.

Artykuł 3

Przepisy ogólne

W odniesieniu do protokołów i interfejsów, o których mowa w art. 4 i 5, dostawcy portfela muszą zapewnić, aby jednostki portfela:

1) uwierzytelniały i walidowały certyfikaty dostępu strony ufającej portfela w przypadku interakcji ze stronami ufającymi portfela;

2) uwierzytelniały i walidowały poświadczenia jednostki portfela innych jednostek portfela, jeżeli wchodzą one w interakcję z innymi jednostkami portfela;

3) w stosownych przypadkach, uwierzytelniały i walidowały żądania przekazane za pomocą certyfikatów dostępu strony ufającej portfela lub poświadczeń jednostki portfela składanych przez inne jednostki portfela;

4) w stosowanych przypadkach; uwierzytelniały i walidowały certyfikat rejestracji strony ufającej portfela;

5) wyświetlały użytkownikom portfela informacje zawarte w certyfikatach dostępu strony ufającej portfela lub w poświadczeniach jednostki portfela;

6) wyświetlały użytkownikom portfela, w stosownych przypadkach, atrybuty, które użytkownicy portfela mają obowiązek przedstawić;

7) w stosownych przypadkach, wyświetlały użytkownikom portfela informacje zawarte w certyfikacie rejestracji strony ufającej portfela;

8) przedstawiały poświadczenia jednostki portfela danej jednostki portfela stronom ufającym portfela lub jednostkom portfela, które o to wystąpiły;

9) nie przedstawiały stronom ufającym portfela ani jednostkom portfela żadnych zażądanych przez nie atrybutów, dopóki nie zostaną spełnione następujące wymogi:

   a) weryfikacja, czy bezpieczna aplikacja kryptograficzna portfela uwierzytelniła tożsamość użytkownika portfela;

   b) w stosownych przypadkach, weryfikacja, czy wbudowane reguły ujawniania zostały przetworzone w jednostce portfela zgodnie z art. 11 rozporządzenia wykonawczego (UE) 2024/2979;

   c) weryfikacja, czy użytkownicy portfela zatwierdzili prezentację częściowo lub w całości;

10) umożliwiły stosowanie technik ochrony prywatności, które zapewniają brak możliwości powiązania, w przypadku gdy elektroniczne poświadczenia atrybutów nie wymagają identyfikacji użytkownika portfela przy przedstawianiu poświadczeń lub danych identyfikujących osobę w różnych stronach ufających portfela.

Artykuł 4

Wydawanie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów do jednostek portfela

1. Dostawcy portfela dopilnowują, aby rozwiązania w zakresie portfela obsługiwały protokoły i interfejsy na potrzeby wydawania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów jednostkom portfela.

2. Dostawcy portfela zapewniają, aby jednostki portfela zwracały się o wydanie danych identyfikujących osobę i elektronicznych poświadczeń atrybutów wyłącznie do stron posiadających autentyczny i ważny certyfikat dostępu strony ufającej portfela, uwierzytelniający strony jako:

a) dostawcę danych identyfikujących osobę;

b) dostawcę kwalifikowanego elektronicznego poświadczenia atrybutów;

c) dostawcę elektronicznego poświadczenia atrybutów wydanego przez podmiot sektora publicznego odpowiedzialny za oryginalne źródło lub w jego imieniu; lub

d) dostawcę niekwalifikowanego elektronicznego poświadczenia atrybutów.

3. W odniesieniu do wydawania danych identyfikujących osobę i elektronicznych poświadczeń atrybutów jednostce portfela dostawcy portfela muszą zapewnić, aby spełnione zostały następujące wymogi:

a) w przypadku gdy użytkownicy portfela korzystają ze swojej jednostki portfela w celu zwrócenia się o wydanie danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów do dostawców danych identyfikujących osobę lub dostawców elektronicznych poświadczeń atrybutów, którzy umożliwiają wydawanie danych identyfikujących osobę lub poświadczeń elektronicznych w więcej niż jednym formacie, jednostka portfela składa wniosek o wydanie tych danych we wszystkich formatach, o których mowa w art. 8 rozporządzenia wykonawczego (UE) 2024/2979 ustanawiającego zasady stosowania rozporządzenia (UE) nr 910/2014 w odniesieniu do integralności i podstawowych funkcji europejskich portfeli tożsamości cyfrowej;

b) w przypadku gdy użytkownicy portfela korzystają ze swojej jednostki portfela w celu interakcji z dostawcami danych identyfikujących osobę lub elektronicznych poświadczeń atrybutów, jednostki portfela umożliwiają uwierzytelnianie i walidację komponentów jednostek portfela, przedstawiając poświadczenia jednostki portfela dostawcom na ich wniosek;

c) rozwiązania w zakresie portfela obsługują mechanizmy umożliwiające dostawcom danych identyfikujących osobę weryfikację wydania, dostarczenia i aktywacji zgodnie z wymogami dotyczącymi wysokiego poziomu bezpieczeństwa określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 ([11]);

d) jednostki portfela weryfikują autentyczność i ważność danych identyfikujących osobę oraz elektronicznych poświadczeń atrybutów.

Artykuł 5

Prezentacja atrybutów stronom ufającym portfela

1. Dostawcy portfela zapewniają, aby rozwiązania w zakresie portfela obsługiwały protokoły i interfejsy do celów prezentacji atrybutów stronom ufającym portfela, zdalnie i, w stosownych przypadkach, zbliżeniowo, zgodnie z normami określonymi w załączniku.

2. Dostawcy portfela dopilnowują, aby – na wniosek użytkowników – jednostki portfela odpowiadały na skutecznie uwierzytelnione i zwalidowane żądania stron ufających portfela, o których mowa w art. 3, zgodnie z normami określonymi w załączniku.

3. Dostawcy portfela zapewniają, aby jednostki portfela obsługiwały potwierdzenie posiadania kluczy prywatnych odpowiadających kluczom publicznym wykorzystywanym w powiązaniach kryptograficznych.

([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).

4. Dostawcy portfela dopilnowują, aby rozwiązania w zakresie portfela obsługiwały selektywne ujawnianie atrybutów danych identyfikujących osobę oraz elektronicznych poświadczeń atrybutów.

5. Ust. 1–4 stosuje się odpowiednio do interakcji między dwoma jednostkami portfela w pobliżu.

Artykuł 6

Przekazywanie żądań usunięcia danych

1. Dostawcy portfela zapewniają, aby jednostki portfela obsługiwały protokoły i interfejsy umożliwiające użytkownikom portfela zwrócenie się do stron ufających portfela, z którymi kontaktowali się oni za pośrednictwem tych jednostek portfela, o usunięcie ich danych osobowych przekazanych za pośrednictwem tych jednostek portfela, zgodnie z art. 17 rozporządzenia (UE) 2016/679.

2. Protokoły i interfejsy, o których mowa w ust. 1, muszą umożliwiać użytkownikom portfela wybór stron ufających portfela, którym będą przekazywane żądania usunięcia danych.

3. Jednostki portfela wyświetlają użytkownikowi portfela uprzednio przekazane żądania usunięcia danych złożone za pośrednictwem tych jednostek portfela.

Artykuł 7

Zgłaszanie stron ufających portfela organom nadzorczym ustanowionym na podstawie art. 51 rozporządzenia (UE) 2016/679

1. Dostawcy portfela dopilnowują, aby jednostki portfela umożliwiały użytkownikom portfela łatwe zgłaszanie stron ufających portfela organom nadzorczym ustanowionym na podstawie art. 51 rozporządzenia (UE) 2016/679.

2. Dostawcy portfela wdrażają protokoły i interfejsy na potrzeby zgłaszania stron ufających portfela zgodnie z krajowymi przepisami proceduralnymi państw członkowskich.

3. Dostawcy portfela zapewniają, aby jednostki portfela umożliwiały użytkownikom portfela uzasadnienie sprawozdań, w tym przez załączenie odpowiednich informacji w celu identyfikacji stron ufających portfela, oraz oświadczeń użytkowników portfela w formacie nadającym się do odczytu maszynowego.

Artykuł 8

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

NORMY, O KTÓRYCH MOWA W ART. 5 UST. 1 I 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024