ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/847

z dnia 6 maja 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do reagowania na naruszenia bezpieczeństwa europejskich portfeli 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. 5e ust. 5,

a także mając na uwadze, co następuje:

(1) Europejskie ramy tożsamości cyfrowej („ramy") 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, a zarazem zapewnienie ochrony danych osobowych i prywatności.

(2) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 ([2]) i (UE) 2018/1725 ([3]) oraz – w stosownych przypadkach – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady ([4]) mają zastosowanie do czynności przetwarzania danych osobowych na podstawie niniejszego rozporządzenia. Przepisy dotyczące oceny i przekazywania informacji ustanowione na podstawie niniejszego rozporządzenia pozostają bez uszczerbku dla obowiązku powiadamiania właściwego organu nadzorczego, w stosownych przypadkach, o naruszeniach ochrony danych osobowych na podstawie rozporządzenia (UE) 2016/679 lub rozporządzenia (UE) 2018/1725 oraz obowiązku informowania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych, w stosownych przypadkach na podstawie niniejszego rozporządzenia.

(3) Komisja regularnie przeprowadza ocenę nowych technologii, praktyk, norm i 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 ([5]) w szczególności na podstawie architektury i ram odniesienia stanowiących ich część. Zgodnie z motywem 75 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/1183 ([6]) Komisja powinna poddawać przeglądowi i w razie potrzeby aktualizować niniejsze rozporządzenie, aby zachować jego aktualność względem globalnych zmian oraz architektury i ram odniesienia, a także przestrzegać najlepszych praktyk na rynku wewnętrznym.

([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]) 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).

([4]) 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).

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

([6]) 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).

(4) W przypadku naruszenia bezpieczeństwa lub kompromitacji rozwiązań w zakresie portfela lub mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, lub systemu identyfikacji elektronicznej, w ramach którego zapewnia się rozwiązania w zakresie portfela, reakcja na takie naruszenia bezpieczeństwa lub kompromitacje musi być szybka, skoordynowana i bezpieczna we wszystkich państwach członkowskich, aby chronić użytkowników i utrzymać zaufanie do ekosystemu tożsamości cyfrowej. Pozostaje to bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 ([7]), rozporządzeń Parlamentu Europejskiego i Rady (UE) 2019/881 ([8]) i (UE) 2024/2847 ([9]), w szczególności w odniesieniu do postępowania w przypadku incydentów lub podatności oraz ich uznawania za naruszenia bezpieczeństwa. W związku z tym państwa członkowskie powinny zapewnić terminowe zawieszenie dostarczania i wykorzystywania portfeli, których dotyczy naruszenie bezpieczeństwa lub kompromitacja, lub, w stosownych przypadkach, ich wycofanie.

(5) Aby zapewnić odpowiednie reakcje na naruszenie bezpieczeństwa lub kompromitację, państwa członkowskie powinny ocenić, czy naruszenie bezpieczeństwa lub kompromitacja w odniesieniu do rozwiązania dotyczącego portfela, mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, lub systemu identyfikacji elektronicznej, w ramach którego zapewnia się rozwiązanie w zakresie portfela, wpływa na niezawodność tego rozwiązania lub innych rozwiązań w zakresie portfela. Taka ocena powinna opierać się na jednolitych kryteriach, takich jak liczba i kategoria użytkowników portfela, osób fizycznych i stron ufających portfela, których to dotyczy, charakter danych, których to dotyczy, czas trwania kompromitacji lub naruszenia bezpieczeństwa, ograniczona dostępność usługi i straty finansowe oraz potencjalna kompromitacja danych osobowych. Kryteria te powinny zapewniać państwom członkowskim elastyczność i swobodę w ustaleniu, w sposób proporcjonalny, czy wystąpił negatywny wpływ na wiarygodność rozwiązania w zakresie portfela oraz czy zawieszenie lub, jeżeli jest to uzasadnione wagą naruszenia lub kompromitacji, wycofanie rozwiązania w zakresie portfela jest właściwe. Kryteria te nie powinny powodować automatycznego wycofania rozwiązania w zakresie portfela lub automatycznego zawieszenia dostarczania i stosowania rozwiązania w zakresie portfela, lecz powinny one być należycie uwzględniane przez państwa członkowskie przy podejmowaniu decyzji, czy konieczne jest wycofanie lub zawieszenie dostarczania i stosowania rozwiązania w zakresie portfela.

(6) Ze względu na skutki i niedogodności spowodowane zawieszeniem stosowania rozwiązań w zakresie portfela państwa członkowskie będą musiały ocenić, czy unieważnienie poświadczeń jednostek portfela lub jakiekolwiek inne dodatkowe środki są konieczne, aby odpowiednio zareagować na naruszenie lub kompromitację.

(7) Aby użytkowników portfela informować na bieżąco o stanie ich portfeli, należy im zapewnić odpowiednie informacje o naruszeniach bezpieczeństwa lub kompromitacjach mających wpływ na ich portfele. Ponieważ naruszenia bezpieczeństwa i kompromitacje mogą mieć również wpływ na strony ufające portfela zarejestrowane w Unii, należy im również udostępniać istotne informacje na temat naruszeń bezpieczeństwa i kompromitacji.

(8) Aby zwiększyć przejrzystość i zbudować zaufanie do ekosystemu tożsamości cyfrowej, informacje o naruszeniach bezpieczeństwa lub kompromitacjach oraz ich konsekwencji powinny co najmniej zawierać informacje wymagane na mocy niniejszego rozporządzenia. Informacje dotyczące naruszeń bezpieczeństwa lub kompromitacji udostępniane użytkownikom portfela i stronom ufającym portfela należy jednak starannie ocenić, tak aby likwidować i minimalizować ryzyko ich wykorzystania przez atakujących.

([7]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Aby umożliwić użytkownikom uzyskanie ponownego dostępu do jednostek portfela po wyeliminowaniu naruszenia lub kompromitacji, państwo członkowskie, które zapewniło rozwiązania w zakresie portfela, będzie musiało bez zbędnej zwłoki przywrócić dostarczanie i stosowanie tych rozwiązań w zakresie portfela. Można tego dokonać przez przywrócenie jednostek portfela, wydanie jednostek portfela dostarczonych w ramach nowej wersji rozwiązań w zakresie portfela lub ponowne wydanie nowych ważnych poświadczeń jednostki portfela. Należy odpowiednio poinformować użytkowników portfela, strony ufające portfela, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1 rozporządzenia (UE) nr 910/2014 oraz Komisję.

(10) Aby zapewnić wycofanie portfeli, w przypadku gdy naruszenie bezpieczeństwa lub kompromitacja nie zostaną wyeliminowane w terminie trzech miesięcy od zawieszenia lub jeżeli jest to uzasadnione wagą naruszenia bezpieczeństwa lub kompromitacji, państwo członkowskie powinno zapewnić, aby odpowiednie poświadczenia jednostki portfela zostały unieważnione i aby ich ważność nie została przywrócona, a także aby nie mogły być wydane lub dostarczone istniejącym jednostkom portfela. Ponadto w ramach danego rozwiązania w zakresie portfela nie należy dostarczać żadnych nowych jednostek portfela. Do celów przejrzystości o wycofaniu należy informować użytkowników, strony ufające, pojedyncze punkty kontaktowe wyznaczone zgodnie z art. 46c ust. 1 rozporządzenia (UE) nr 910/2014 i Komisję. Obejmuje to opis potencjalnego wpływu na użytkowników portfela, w szczególności na zarządzanie wydanymi poświadczeniami, lub na strony ufające portfela.

(11) Okres trzech miesięcy od zawieszenia dostarczania i zastosowania rozwiązania w zakresie portfela, w trakcie którego należy usunąć naruszenie bezpieczeństwa lub kompromitację, które doprowadziły do tego zawieszenia, powinien przewidywać termin, po upływie którego rozwiązanie w zakresie portfela ma zostać wycofane, chyba że wdrożono odpowiedni środek zaradczy. Państwa członkowskie mają jednak swobodę żądania usunięcia naruszenia bezpieczeństwa lub kompromitacji w terminie krótszym niż trzy miesiące, biorąc pod uwagę, w szczególności i w stosownych przypadkach, zakres, czas trwania i konsekwencje tego naruszenia bezpieczeństwa lub kompromitacji. W przypadku gdy naruszenie bezpieczeństwa lub kompromitacja nie zostały lub nie mogą zostać usunięte w terminie określonym przez państwo członkowskie, państwo członkowskie może zażądać wycofania rozwiązania w zakresie portfela przed upływem okresu trzech miesięcy. Państwa członkowskie powinny wykorzystać ten okres, w którym należy usunąć naruszenie bezpieczeństwa lub kompromitację, które doprowadziły do zawieszenia świadczenia i stosowania rozwiązania w zakresie portfela, w celu przygotowania ewentualnego wycofania tego rozwiązania w zakresie portfela i wynikających z tego powiadomień.

(12) Aby zmniejszyć obciążenie administracyjne państw członkowskich związane z informacjami, które mają być przekazywane Komisji i innym państwom członkowskim zgodnie z niniejszym rozporządzeniem, państwa członkowskie powinny korzystać z istniejących narzędzi notyfikacji, takich jak system zgłaszania i analizy cyberincydentów („CIRAS") obsługiwany przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa („ENISA"). W odniesieniu do alternatywnych kanałów lub środków, które mają być wykorzystywane do informowania użytkowników portfela, których dotyczy naruszenie bezpieczeństwa lub kompromitacja, oraz stron ufających portfela, państwa członkowskie powinny zapewnić, aby odpowiednie informacje były przekazywane w sposób jasny, wyczerpujący i łatwo dostępny. Kanały przekazywania takich informacji użytkownikom portfela, których to dotyczy, i stronom ufającym portfela powinny obejmować odpowiednie rozwiązania w zakresie transmisji za pomocą strony internetowej, śledzenia w czasie rzeczywistym aktualizacji stron internetowych i agregacji wiadomości.

(13) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię dnia 31 stycznia 2025 r.

(14) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

W niniejszym rozporządzeniu ustanawia się przepisy dotyczące reakcji na naruszenia bezpieczeństwa portfeli, mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, oraz systemu identyfikacji elektronicznej, w ramach którego dostarczane są portfele.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „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;

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

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

4) „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;

5) „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;

6) „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;

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

8) „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;

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

Artykuł 3

Stwierdzenie naruszenia bezpieczeństwa lub kompromitacji

1. Bez uszczerbku dla dyrektywy (UE) 2022/2555 i rozporządzeń (UE) 2019/881 i (UE) 2024/2847 państwa członkowskie należycie uwzględniają kryteria określone w załączniku I do niniejszego rozporządzenia, aby ocenić, czy naruszenie bezpieczeństwa lub kompromitacja rozwiązania w zakresie portfela, mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, lub systemu identyfikacji elektronicznej, w ramach którego dostarcza się rozwiązanie w zakresie portfela, ma wpływ na ich wiarygodność lub wiarygodność innych rozwiązań w zakresie portfela.

2. Jeżeli państwo członkowskie ustali, na podstawie oceny określonej w ust. 1, że naruszenie bezpieczeństwa lub kompromitacja wpływają na wiarygodność rozwiązania w zakresie portfela i zawiesza stosowanie tego rozwiązania w zakresie portfela, państwo to stosuje środki określone w art. 4 i 5. Jeżeli państwo członkowskie wycofuje rozwiązanie w zakresie portfela, stosuje ono środki określone w art. 8 i 9.

3. W przypadku gdy państwo członkowskie uzyska informacje o ewentualnym naruszeniu bezpieczeństwa lub kompromitacji, które mogą mieć wpływ na wiarygodność co najmniej jednego rozwiązania w zakresie portfela dostarczonego przez inne państwo członkowskie, państwo to bez zbędnej zwłoki powiadamia o tym fakcie Komisję i pojedyncze punkty kontaktowe państw członkowskich, których to dotyczy, wyznaczone zgodnie z art. 46c ust. 1 rozporządzenia (UE) nr 910/2014. Takie powiadomienie musi zawierać informacje wyszczególnione w art. 5 ust. 2.

4. Państwo członkowskie otrzymujące informacje przekazywane zgodnie z ust. 3 stosuje środki określone w ust. 1 i 2 bez zbędnej zwłoki.

Artykuł 4

Zawieszenie dostarczania i stosowania portfeli oraz inne środki zaradcze

1. Państwa członkowskie zapewniają, aby nie dostarczano, nie stosowano ani nie aktywowano jednostek portfela w ramach zawieszonego rozwiązania w zakresie portfela.

2. Państwa członkowskie oceniają, czy unieważnienie poświadczeń jednostek portfela, których dotyczy zawieszenie rozwiązania w zakresie portfela lub jakikolwiek inny dodatkowy środek zaradczy, są konieczne, aby odpowiednio zareagować na naruszenie bezpieczeństwa lub kompromitację.

3. Środki określone w ust. 1 i 2 wprowadza się bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny po zawieszeniu dostarczania i stosowania rozwiązania w zakresie portfela, na które naruszenie bezpieczeństwa lub kompromitacja miały wpływ.

4. Środki określone w ust. 1 i 2 nie utrudniają użytkownikom portfela, których to dotyczy korzystania z prawa do przenoszenia danych określonego w art. 5a ust. 4 lit. g) rozporządzenia (UE) nr 910/2014. Jest to możliwe, pod warunkiem że użytkownicy portfela mogą korzystać z tego prawa bez uszczerbku dla bezpieczeństwa aktywów krytycznych odnośnych jednostek portfela, w szczególności biorąc pod uwagę przyczyny zawieszenia i potrzebę zapewnienia skutecznej ochrony tych aktywów przed niewłaściwym wykorzystaniem.

Artykuł 5

Informacje o zawieszeniach i środkach zaradczych

1. Jasne, wyczerpujące i łatwo dostępne informacje o zawieszeniu dostarczania i stosowania rozwiązania w zakresie portfela przekazuje się, bez zbędnej zwłoki i nie później niż 24 godziny po zawieszeniu dostarczania i stosowania rozwiązania w zakresie portfela, do:

a) pojedynczych punktów kontaktowych wyznaczonych na podstawie art. 46c ust. 1 rozporządzenia (UE) nr 910/2014;

b) Komisji;

c) użytkowników portfela, których to dotyczy;

d) stron ufających portfela zarejestrowanych zgodnie z art. 5b rozporządzenia (UE) nr 910/2014.

2. Informacje przekazywane zgodnie z ust. 1 muszą zawierać co najmniej następujące elementy:

a) nazwę dostawcy rozwiązania w zakresie portfela, którego dostarczanie i stosowanie zostało zawieszone;

b) nazwę i identyfikator referencyjny tego rozwiązania w zakresie portfela wskazany w wykazie certyfikowanych portfeli sporządzonym zgodnie z art. 5d rozporządzenia (UE) nr 910/2014 oraz, w stosownych przypadkach, odnośną wersję;

c) datę i godzinę wykrycia naruszenia bezpieczeństwa lub kompromitacji;

d) datę i godzinę zaistnienia naruszenia bezpieczeństwa lub kompromitacji, jeżeli są znane, na podstawie dzienników sieciowych lub systemowych lub innych źródeł danych;

e) datę i godzinę zawieszenia rozwiązania w zakresie portfela;

f) dane kontaktowe, w tym co najmniej adres e-mail i numer telefonu w przypadku notyfikującego państwa członkowskiego, a gdy są one różne, w przypadku dostawcy portfela, o którym mowa w lit. a);

g) opis naruszenia bezpieczeństwa lub kompromitacji;

h) opis danych objętych kompromitacją, w tym, w stosownych przypadkach, kategorii danych osobowych zdefiniowanych w art. 9 ust. 1 i art. 10 rozporządzenia (UE) 2016/679;

i) w miarę możliwości szacunkową, przybliżoną liczbę użytkowników portfela, których to dotyczy, oraz innych osób fizycznych, których to dotyczy;

j) opis potencjalnego wpływu na strony ufające portfela lub na użytkowników portfela, a w tym drugim przypadku, odpowiednio, wszelkie wskazania dotyczące środków, które użytkownicy portfela mogą przedsięwziąć w celu złagodzenia tych potencjalnych skutków;

k) opis środków zaradczych zastosowanych lub planowanych w celu wyeliminowania naruszenia bezpieczeństwa lub kompromitacji, wraz z planem i terminem zastosowania takich środków zaradczych;

l) w miarę możliwości i w stosownych przypadkach, opis środków zastosowanych lub planowanych w celu przejścia użytkowników portfela, których to dotyczy, na alternatywne rozwiązania w zakresie portfela lub alternatywne usługi.

Artykuł 6

Przywrócenie dostarczania i stosowania portfeli

W przypadku gdy jest to konieczne do zapewnienia przywrócenia dostarczania, aktywacji i stosowania rozwiązania w zakresie portfela, państwa członkowskie bez zbędnej zwłoki:

1) przywracają dostarczanie i stosowanie jednostek portfela zapewnianych w ramach tego rozwiązanie w zakresie portfela poprzez wydanie wszystkim użytkownikom, których to dotyczy, jednostki portfela dostarczanej w ramach nowej wersji rozwiązania w zakresie portfela;

2) wydają nowe poświadczenia jednostek portfela nowym jednostkom portfela lub, w stosownych przypadkach, wcześniej wydanym jednostkom portfela, pod warunkiem że te jednostki portfela spełniają obowiązujące wymogi bezpieczeństwa po usunięciu naruszenia bezpieczeństwa lub kompromitacji;

3) uchylają wszelkie środki wdrożone na podstawie art. 4 utrudniające dostarczanie nowych jednostek portfela w ramach rozwiązania w zakresie portfela, którego to dotyczy, w przypadku gdy środki te były związane wyłącznie z obecnie usuniętymi naruszeniem bezpieczeństwa lub kompromitacją.

Artykuł 7

Informacje o przywróceniu

W przypadku gdy państwo członkowskie przywraca rozwiązanie w zakresie portfela, państwo to zapewnia, aby:

1) informacje o tym fakcie przekazuje się bez zbędnej zwłoki wszystkim stronom, które otrzymały informacje o zawieszeniu dostarczania i stosowania tego rozwiązania w zakresie portfela zgodnie z art. 5 ust. 1;

2) informacje przekazywane zgodnie z pkt 1 muszą zawierać co najmniej elementy, o których mowa w art. 5 ust. 2 lit. a), b) i f)–h), oraz następujące elementy:

   a) datę i godzinę wyeliminowania naruszenia bezpieczeństwa lub kompromitacji;

   b) datę i godzinę przywrócenia rozwiązania w zakresie portfela, którego to dotyczy, oraz, w stosownych przypadkach, jednostek portfela, których to dotyczy, przewidzianych w tym rozwiązaniu w zakresie portfela;

   c) opis środków zaradczych wprowadzonych w celu wyeliminowania naruszenia bezpieczeństwa lub kompromitacji;

   d) opis potencjalnego wpływu rezydualnego na strony ufające portfela lub na użytkowników portfela, a w tym drugim przypadku, odpowiednio, wszelkie wskazania dotyczące środków, które użytkownicy portfela mogą przedsięwziąć w celu złagodzenia tych potencjalnych skutków;

Artykuł 8

Wycofanie portfeli

1. Jeżeli naruszenie bezpieczeństwa lub kompromitacja, które doprowadziły do zawieszenia dostarczania i stosowania rozwiązania w zakresie portfela, nie zostaną wyeliminowane w terminie trzech miesięcy od daty zawieszenia dostarczania i stosowania rozwiązania w zakresie portfela, państwo członkowskie zapewniające to rozwiązanie zakresie portfela dopilnowuje, aby dane rozwiązanie zostało wycofane i unieważnione bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od upływu trzymiesięcznego okresu.

2. W przypadku gdy państwo członkowskie wycofuje rozwiązanie w zakresie portfela, państwo to zapewnia, aby:

a) poświadczenia jednostki portfela w ramach tego rozwiązania w zakresie portfela zostały unieważnione;

b) przywrócenie ważności poświadczeń jednostki portfela nie było możliwe;

c) w ramach tego rozwiązania w zakresie portfela nie było możliwe wydanie nowych poświadczeń jednostki portfela istniejącym jednostkom portfela;

d) w ramach tego rozwiązania w zakresie portfela nie było możliwe zapewnienie nowych jednostek portfela.

3. Środki określone w ust. 1 i 2 nie utrudniają użytkownikom portfela, których to dotyczy korzystania z prawa do przenoszenia danych określonego w art. 5a ust. 4 lit. g) rozporządzenia (UE) nr 910/2014. Jest to możliwe, pod warunkiem że użytkownicy portfela mogą korzystać z tego prawa bez uszczerbku dla bezpieczeństwa aktywów krytycznych odnośnych jednostek portfela, w szczególności biorąc pod uwagę przyczyny wycofania i potrzebę zapewnienia skutecznej ochrony tych aktywów przed niewłaściwym wykorzystaniem.

Artykuł 9

Informacje o wycofaniu

1. Jasne, wyczerpujące i łatwo dostępne informacje o wycofaniu rozwiązania w zakresie portfela wysyła się bez zbędnej zwłoki i nie później niż 24 godziny po wycofaniu rozwiązania w zakresie portfela do:

a) pojedynczych punktów kontaktowych wyznaczonych na podstawie art. 46c ust. 1 rozporządzenia (UE) nr 910/2014;

b) Komisji;

c) użytkowników portfela, których to dotyczy;

d) stron ufających portfela zarejestrowanych zgodnie z art. 5b rozporządzenia (UE) nr 910/2014.

2. Informacje przekazywane zgodnie z ust. 1 muszą zawierać co najmniej następujące elementy:

a) nazwę dostawcy rozwiązania w zakresie portfela, które zostało wycofane;

b) nazwę i identyfikator referencyjny tego rozwiązania w zakresie portfela wskazany w wykazie certyfikowanych portfeli sporządzonym zgodnie z art. 5d rozporządzenia (UE) nr 910/2014 oraz, w stosownych przypadkach, odnośną wersję;

c) datę i godzinę wykrycia naruszenia bezpieczeństwa lub kompromitacji, które doprowadziły do wycofania danego rozwiązania w zakresie portfela ze względu na ich wagę lub fakt, że nie wyeliminowano ich w ciągu trzech miesięcy;

d) datę i godzinę zaistnienia naruszenia bezpieczeństwa lub kompromitacji, jeżeli są znane, na podstawie dzienników sieciowych lub systemowych lub innych źródeł danych;

e) datę i godzinę wycofania rozwiązania w zakresie portfela oraz skutecznego unieważnienia poświadczeń jednostki portfela jednostek portfela dostarczonych w ramach rozwiązania w zakresie portfela;

f) informację, czy wycofanie jest wynikiem wagi naruszenia bezpieczeństwa lub kompromitacji, czy jest konsekwencją naruszenia bezpieczeństwa lub kompromitacji, których nie wyeliminowano;

g) dane kontaktowe, w tym co najmniej adres e-mail i numer telefonu w przypadku notyfikującego państwa członkowskiego, a gdy są one różne, w przypadku dostawcy portfela, o którym mowa w lit. a);

h) opis naruszenia bezpieczeństwa lub kompromitacji;

i) opis danych objętych kompromitacją, w tym, w stosownych przypadkach, kategorii danych osobowych określonych w art. 9 ust. 1 i art. 10 rozporządzenia (UE) 2016/679;

j) w miarę możliwości szacunkową, przybliżoną liczbę użytkowników portfela, których to dotyczy, oraz innych osób fizycznych, których to dotyczy;

k) opis potencjalnego wpływu na strony ufające portfela lub na użytkowników portfela, a w tym drugim przypadku, odpowiednio, wszelkie wskazania dotyczące środków, które użytkownicy portfela mogą przedsięwziąć w celu złagodzenia tych potencjalnych skutków;

l) opis środków zastosowanych lub planowanych w celu przejścia użytkowników portfela, których to dotyczy, na alternatywne rozwiązania w zakresie portfela lub, w miarę możliwości i w stosownych przypadkach, alternatywne usługi.

Artykuł 10

System informacyjny

Państwa członkowskie przesyłają informacje określone w art. 3, 5, 7 i 9 Komisji i pojedynczym punktom kontaktowym państw członkowskich wyznaczonym zgodnie z art. 46c ust. 1 rozporządzenia (UE) nr 910/2014 za pośrednictwem systemu CIRAS obsługiwanego przez ENISA lub równoważnego systemu uzgodnionego przez państwa członkowskie i Komisję.

Artykuł 11

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, z wyjątkiem art. 10, który stosuje się od dnia 7 maja 2026 r.

Sporządzono w Brukseli dnia 6 maja 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK

Kryteria oceny naruszenia bezpieczeństwa lub kompromitacji

1. Państwa członkowskie oceniają naruszenie bezpieczeństwa lub kompromitację według następujących kryteriów:

   a) naruszenie lub kompromitacja spowodowały lub mogą spowodować śmierć osoby fizycznej lub znaczną szkodę dla zdrowia tej osoby fizycznej;

   b) skuteczny, prawdopodobnie złośliwy lub nieuprawniony dostęp do sieci i systemów informatycznych dostawcy portfela, dostawcy mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, dostawcy systemów identyfikacji elektronicznej, w ramach których zapewnia się rozwiązanie w zakresie portfela („zainteresowane podmioty") miał miejsce lub może nastąpić w sposób, który może spowodować poważne zakłócenia operacyjne, a systemy te są kluczowymi elementami rozwiązania w zakresie portfela, mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, lub systemu identyfikacji elektronicznej, których to dotyczy, w ramach którego zapewniono rozwiązanie w zakresie portfela;

   c) rozwiązanie w zakresie portfela, mechanizm walidacji, o którym mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014 lub system identyfikacji elektronicznej, w ramach którego zapewnia się rozwiązanie w zakresie portfela lub ich część:

      — są lub przewiduje się, że będą całkowicie niedostępne dla użytkowników portfela lub stron ufających portfela przez ponad 12 kolejnych godzin;

      — są lub przewiduje się, że będą niedostępne dla użytkowników portfela lub stron ufających portfela przez ponad 16 godzin w tygodniu kalendarzowym;

   d) podejrzewa się, że ograniczona dostępność rozwiązania w zakresie portfela lub usług świadczonych przez dane podmioty w odniesieniu do rozwiązania w zakresie portfela ma wpływ na ponad 1 % użytkowników portfela lub stron ufających portfela;

   e) istnieje możliwość kompromitacji lub nastąpiła kompromitacja fizycznego dostępu ograniczonego do zaufanego personelu danych podmiotów lub ochrony takiego fizycznego dostępu w co najmniej jednej lokalizacji sieci i systemów informatycznych wspierających rozwiązanie w zakresie portfela, zapewnianie mechanizmów walidacji, o których mowa w art. 5a ust. 8 rozporządzenia (UE) nr 910/2014, związanych z rozwiązaniem w zakresie portfela, lub system identyfikacji elektronicznej, w ramach którego dostarcza się rozwiązanie w zakresie portfela;

   f) kompromitacja prywatności, integralności, poufności lub autentyczności danych przechowywanych, przekazywanych lub przetwarzanych w rozwiązaniu w zakresie portfela nastąpiła lub może nastąpić w co najmniej jeden z następujących sposobów:

      — ma ona wpływ na ponad 1 % użytkowników portfela rozwiązania w zakresie portfela, którego to dotyczy, lub na ponad 100 000 użytkowników portfela, w zależności od tego, która z tych liczb jest mniejsza;

      — wynika ze skutecznego, prawdopodobnie złośliwego działania;

      — jest wynikiem lub może być wynikiem co najmniej jednej znanej podatności, w tym podatności usuniętych zgodnie z rozporządzeniem wykonawczym Komisji (UE) 2024/2981 ([1]);

      — możliwy wpływ na dane osobowe w sposób, który może powodować ryzyko naruszenia praw i wolności zainteresowanych osób fizycznych, w szczególności w przypadku naruszenia danych osobowych zdefiniowanych w art. 9 ust. 1 i art. 10 rozporządzenia (UE) 2016/679;

([1]) Rozporządzenie wykonawcze Komisji (UE) 2024/2981 z dnia 28 listopada 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w odniesieniu do certyfikacji europejskich portfeli tożsamości cyfrowej (Dz.U. L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— może mieć wpływ na osobistą łączność elektroniczną;

— może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych;

— może mieć wpływ na osoby fizyczne podatne na zagrożenia;

g) cofnięto certyfikację rozwiązania w zakresie portfela lub przewiduje się, że zostanie ona cofnięta;

h) naruszenie lub kompromitacja spowodowały lub mogą spowodować stratę finansową dla podmiotu, którego to dotyczy, która przekracza 500 000 EUR lub, w stosownych przypadkach, 5 % całkowitego rocznego obrotu podmiotu, którego to dotyczy, w poprzednim roku obrotowym, w zależności od tego, która z tych wartości jest niższa;

2. państwa członkowskie nie biorą pod uwagę planowanych konsekwencji prac konserwacyjnych przeprowadzanych przez dane podmioty lub w ich imieniu, pod warunkiem że:

a) o pracach konserwacyjnych powiadomiono uprzednio użytkowników portfela, strony ufające portfela i odpowiednie właściwe organy nadzoru, których prace te mogą potencjalnie dotyczyć;

b) prace konserwacyjne nie spełniają żadnego z kryteriów określonych w pkt 1 niniejszego załącznika.

3. W odniesieniu do pkt 1 lit. (c) czas trwania incydentu mającego wpływ na dostępność należy mierzyć od momentu zakłócenia właściwego świadczenia danej usługi do momentu przywrócenia usługi i jej funkcjonowania. Jeżeli dany podmiot nie jest w stanie określić momentu rozpoczęcia zakłócenia, czas trwania incydentu należy mierzyć od momentu wykrycia incydentu lub od momentu jego odnotowania w rejestrze sieci lub systemu lub w innych źródłach danych, w zależności od tego, co nastąpiło wcześniej. Całkowitą niedostępność usługi należy mierzyć od momentu, w którym usługa stała się w pełni niedostępna dla użytkowników, do momentu przywrócenia regularnej działalności lub operacji do poziomu usługi świadczonej przed incydentem. Jeżeli dany podmiot nie jest w stanie ustalić, kiedy rozpoczęła się całkowita niedostępność usługi, należy ją mierzyć od momentu jej wykrycia przez ten podmiot.

4. W odniesieniu do pkt 1 lit. (d) uznaje się, że ograniczona dostępność usługi występuje w szczególności wtedy, gdy świadczenie usługi jest znacznie wolniejsze niż średni czas reakcji lub gdy nie wszystkie funkcje usługi są dostępne. W miarę możliwości do oceny opóźnień w czasie reakcji stosuje się obiektywne kryteria oparte na średnim czasie reakcji w ramach usług.

5. W celu określenia bezpośrednich strat finansowych wynikających z naruszenia lub kompromitacji, o których mowa w pkt 1 lit. (h), zainteresowane podmioty biorą pod uwagę wszystkie straty finansowe poniesione w wyniku incydentu, takie jak koszty wymiany lub przeniesienia oprogramowania, sprzętu lub infrastruktury, koszty personelu, w tym koszty związane z zastąpieniem lub przeniesieniem personelu, rekrutacją dodatkowego personelu, wynagrodzeniem za godziny nadliczbowe i przywróceniem utraconych lub obniżonych umiejętności, opłaty z tytułu nieprzestrzegania zobowiązań umownych, koszty zadośćuczynienia i odszkodowań dla klientów, straty spowodowane utratą przychodów, koszty związane z komunikacją wewnętrzną i zewnętrzną oraz koszty doradztwa, w tym koszty związane z doradztwem prawnym, usługami kryminalistycznymi i usługami zaradczymi. Kosztów niezbędnych do bieżącego prowadzenia działalności gospodarczej, takich jak koszty ogólnego utrzymania infrastruktury, wyposażenia, sprzętu i oprogramowania, ulepszeń i inicjatyw w zakresie oceny ryzyka oraz składek ubezpieczeniowych, nie uznaje się za straty finansowe wynikające z incydentu. Dane podmioty muszą obliczać kwoty strat finansowych na podstawie dostępnych danych, a gdy nie można ustalić faktycznych kwot strat finansowych, podmioty te muszą oszacować te kwoty.