Amtsblatt
der Europäischen Union

DE
Reihe L

2025/847

7.5.2025

DURCHFÜHRUNGSVERORDNUNG (EU) 2025/847 DER KOMMISSION

vom 6. Mai 2025

zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Reaktion auf Sicherheitsverletzungen europäischer Brieftaschen für die digitale Identität

DIE EUROPÄISCHE KOMMISSION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union,

gestützt auf die Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG ([1]), insbesondere auf Artikel 5e Absatz 5,

in Erwägung nachstehender Gründe:

(1) Der durch die Verordnung (EU) Nr. 910/2014 festgelegte europäische Rahmen für die digitale Identität (im Folgenden „Rahmen“) ist eine unverzichtbare Komponente für die Schaffung eines sicheren und interoperablen Ökosystems für die digitale Identität in der gesamten Union. Mit den europäischen Brieftaschen für die digitale Identität (im Folgenden „Brieftaschen“) als Eckpfeiler soll der Rahmen den Zugang zu Diensten in allen Mitgliedstaaten erleichtern und gleichzeitig den Schutz personenbezogener Daten und der Privatsphäre gewährleisten.

(2) Die Verordnungen (EU) 2016/679 ([2]) und (EU) 2018/1725 ([3]) des Europäischen Parlaments und des Rates und, sofern anwendbar, die Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates ([4]) gelten für die Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung. Die in dieser Verordnung festgelegten Vorschriften für die Bewertung und Bereitstellung von Informationen lassen die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten gegebenenfalls gemäß der Verordnung (EU) 2016/679 oder der Verordnung (EU) 2018/1725 der zuständigen Aufsichtsbehörde zu melden, und die Verpflichtung, die betroffenen Personen von Verletzungen des Schutzes personenbezogener Daten zu benachrichtigen, soweit dies nach diesen Verordnungen anwendbar ist, unberührt.

(3) Die Kommission bewertet regelmäßig neue Technologien, Praktiken, Normen und technische Spezifikationen. Um ein Höchstmaß an Harmonisierung zwischen den Mitgliedstaaten bei der Entwicklung und Zertifizierung der Brieftaschen zu gewährleisten, beruhen die in dieser Verordnung festgelegten technischen Spezifikationen auf den Arbeiten, die im Zuge der Empfehlung (EU) 2021/946 der Kommission ([5]) durchgeführt wurden, insbesondere auf der Architektur und dem dazugehörigen Referenzrahmen. Nach Erwägungsgrund 75 der Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates ([6]) sollte die Kommission diese Verordnung überprüfen und gegebenenfalls aktualisieren, damit sie mit globalen Entwicklungen, der Architektur und dem Referenzrahmen Schritt hält und den bewährten Verfahren des Binnenmarkts folgt.

([1]) ABl. L 257 vom 28.8.2014, S. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität (ABl. L 210 vom 14.6.2021, S. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität (ABl. L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Im Falle einer Sicherheitsverletzung oder Beeinträchtigung der Brieftaschenlösungen oder der Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder des elektronischen Identifizierungssystems, in dessen Rahmen die Brieftaschenlösungen bereitgestellt werden, muss in allen Mitgliedstaaten in rascher, koordinierter und sicherer Weise auf solche Sicherheitsverletzungen und Beeinträchtigungen reagiert werden, um die Nutzer zu schützen und das Vertrauen in das Ökosystem der digitalen Identität zu bewahren. Dies gilt unbeschadet der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates ([7]) und der Verordnungen (EU) 2019/881 ([8]) und (EU) 2024/2847 ([9]) des Europäischen Parlaments und des Rates, insbesondere bezüglich der Behandlung von Sicherheitsvorfällen oder Schwachstellen und ihrer Einstufung als Sicherheitsverletzungen. Deshalb sollten die Mitgliedstaaten für die zeitnahe Aussetzung der Bereitstellung und Nutzung der Brieftaschen sorgen, die von einer Sicherheitsverletzung oder -beeinträchtigung betroffen sind, oder gegebenenfalls für deren Zurückziehung.

(5) Um angemessene Reaktionen auf eine Sicherheitsverletzung oder -beeinträchtigung zu gewährleisten, sollten die Mitgliedstaaten prüfen, ob sich eine Sicherheitsverletzung oder -beeinträchtigung einer Brieftaschenlösung, der Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder des elektronischen Identifizierungssystems, in dessen Rahmen eine Brieftaschenlösung bereitgestellt wird, auf die Zuverlässigkeit dieser Brieftaschenlösung oder anderer Brieftaschenlösungen auswirkt. Eine solche Prüfung sollte auf einheitliche Kriterien gestützt werden, wie z. B. die Anzahl und Kategorie der betroffenen Brieftaschennutzer, natürlichen Personen und auf Brieftaschen vertrauenden Beteiligten, die Art der betroffenen Daten, die Dauer der Beeinträchtigung oder Sicherheitsverletzung, die eingeschränkte Verfügbarkeit eines Dienstes und finanzielle Verluste sowie die potenzielle Beeinträchtigung des Schutzes personenbezogener Daten. Diese Kriterien sollten den Mitgliedstaaten Flexibilität und Ermessensspielraum geben, damit sie auf verhältnismäßige Weise feststellen können, ob die Zuverlässigkeit einer Brieftaschenlösung beeinträchtigt ist und ob die Aussetzung oder — falls dies wegen der Schwere der Sicherheitsverletzung oder -beeinträchtigung gerechtfertigt ist — die Zurückziehung der Brieftaschenlösung angemessen ist. Diese Kriterien sollten nicht zu einer automatischen Zurückziehung einer Brieftaschenlösung oder einer automatischen Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung führen, aber sie sollten von den Mitgliedstaaten gebührend berücksichtigt werden, wenn sie entscheiden, ob eine Zurückziehung oder Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung erforderlich ist.

(6) Angesichts der Auswirkungen und Unannehmlichkeiten, die sich aus der Aussetzung der Nutzung von Brieftaschenlösungen ergeben, sollten die Mitgliedstaaten prüfen, ob der Widerruf von Einzelbrieftaschenbescheinigungen oder andere zusätzliche Maßnahmen als angemessene Reaktion auf die Sicherheitsverletzung oder -beeinträchtigung erforderlich sind.

(7) Um die Brieftaschennutzer über den Status ihrer Brieftaschen auf dem Laufenden zu halten, müssen ihnen geeignete Informationen über Sicherheitsverletzungen oder -beeinträchtigungen, die ihre Brieftaschen betreffen, gegeben werden. Da in der Union registrierte auf Brieftaschen vertrauende Beteiligte ebenfalls von Sicherheitsverletzungen und -beeinträchtigungen betroffen sein können, müssen auch sie einschlägige Informationen über Sicherheitsverletzungen oder -beeinträchtigungen erhalten.

(8) Um die Transparenz zu erhöhen und Vertrauen in das Ökosystem der digitalen Identität aufzubauen, sollten die Informationen über Sicherheitsverletzungen oder -beeinträchtigungen und deren Folgen zumindest die nach dieser Verordnung erforderlichen Informationen enthalten. Informationen über Sicherheitsverletzungen oder -beeinträchtigungen, die Brieftaschennutzern und auf Brieftaschen vertrauenden Beteiligten gegeben werden, sollten jedoch zuvor sorgfältig geprüft werden, damit das Risiko ihrer Ausnutzung durch Angreifer vermieden bzw. so gering wie möglich gehalten wird.

([7]) Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80, , ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Verordnung (EU) 2024/2847 des Europäischen Parlaments und des Rates vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen (EU) Nr. 168/2013 und (EU) 2019/1020 und der Richtlinie (EU) 2020/1828 (Cyberresilienz-Verordnung) (ABl. L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Damit die Nutzer nach der Behebung einer Sicherheitsverletzung oder -beeinträchtigung erneut auf ihre Einzelbrieftaschen zugreifen können, muss der Mitgliedstaat, der die Brieftaschenlösungen bereitgestellt hat, die Bereitstellung und Nutzung dieser Brieftaschenlösungen unverzüglich wiederherstellen. Dies kann durch die Wiederherstellung der Einzelbrieftaschen, die Ausstellung von Einzelbrieftaschen im Rahmen einer neuen Version der Brieftaschenlösungen oder die Neuausstellung neuer gültiger Einzelbrieftaschenbescheinigungen erfolgen. Betroffene Brieftaschennutzer sowie auf Brieftaschen vertrauende Beteiligte, gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannte einheitliche Anlaufstellen und die Kommission sind entsprechend zu informieren.

(10) Damit Brieftaschen zurückgezogen werden, wenn eine Sicherheitsverletzung oder -beeinträchtigung nicht innerhalb von drei Monaten nach der Aussetzung behoben wurde oder wenn dies wegen der Schwere der Sicherheitsverletzung oder -beeinträchtigung gerechtfertigt ist, sollte der Mitgliedstaat sicherstellen, dass die betroffenen Einzelbrieftaschenbescheinigungen zurückgezogen werden und weder in einen gültigen Status zurückgesetzt noch für bestehende Einzelbrieftaschen ausgestellt oder bereitgestellt werden können. Außerdem sollten keine neuen Einzelbrieftaschen im Rahmen der betroffenen Brieftaschenlösung bereitgestellt werden. Im Interesse der Transparenz sind betroffene Brieftaschennutzer sowie auf Brieftaschen vertrauende Beteiligte, gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannte einheitliche Anlaufstellen und die Kommission über die Zurückziehung zu informieren. Dies schließt auch eine Beschreibung der potenziellen Auswirkungen auf die Brieftaschennutzer und insbesondere auf die Verwaltung der ausgestellten Bescheinigungen oder auf die auf Brieftaschen vertrauenden Beteiligten ein.

(11) Nach Ablauf des Dreimonatszeitraums nach der Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung, in dem die Sicherheitsverletzung oder -beeinträchtigung, die diese Aussetzung zur Folge hatte, behoben werden muss, sollte die Brieftaschenlösung zurückgezogen werden müssen, wenn innerhalb dieser Frist keine angemessene Abhilfe geschaffen wurde. Es steht den Mitgliedstaaten jedoch frei zu verlangen, dass die Sicherheitsverletzung oder -beeinträchtigung innerhalb einer Frist von weniger als drei Monaten behoben wird, wobei insbesondere und soweit relevant das Ausmaß, die Dauer und die Folgen dieser Sicherheitsverletzung oder -beeinträchtigung zu berücksichtigen sind. Sofern die Sicherheitsverletzung oder -beeinträchtigung nicht innerhalb der von dem Mitgliedstaat gesetzten Frist behoben wird oder behoben werden kann, kann der Mitgliedstaat verlangen, dass die Brieftaschenlösung vor Ablauf des Dreimonatszeitraums zurückgezogen wird. Die Mitgliedstaaten sollten diesen Zeitraum, in dem eine Sicherheitsverletzung oder -beeinträchtigung, die die Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung zur Folge hatte, behoben werden muss, nutzen, um die mögliche Zurückziehung dieser Brieftaschenlösung und die entsprechende Kommunikation vorzubereiten.

(12) Um den Verwaltungsaufwand der Mitgliedstaaten durch die gemäß dieser Verordnung an die Kommission und an andere Mitgliedstaaten bereitzustellenden Informationen zu verringern, sollten die Mitgliedstaaten dafür bestehende Notifizierungsinstrumente wie das von der Agentur der Europäischen Union für Cybersicherheit (ENISA) betriebene Melde- und Analysesystem für Cybervorfälle (CIRAS) verwenden. In Bezug auf alternative Kanäle oder Mittel, die zur Information der von einer Sicherheitsverletzung oder -beeinträchtigung betroffenen Brieftaschennutzer und der auf Brieftaschen vertrauenden Beteiligten zu verwenden sind, sollten die Mitgliedstaaten dafür sorgen, dass die betreffenden Informationen in klarer, umfassender und leicht zugänglicher Weise bereitgestellt werden. Die Kanäle für die Bereitstellung solcher Informationen für betroffene Brieftaschennutzer und auf Brieftaschen vertrauende Beteiligte sollten geeignete Lösungen für die Verbreitung über Websites, die Nachverfolgung von Website-Aktualisierungen in Echtzeit und Nachrichtenaggregationsdienste umfassen.

(13) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 angehört und gab am 31. Januar 2025 seine Stellungnahme ab.

(14) Die in dieser Verordnung vorgesehenen Maßnahmen entsprechen der Stellungnahme des gemäß Artikel 48 der Verordnung (EU) Nr. 910/2014 eingesetzten Ausschusses —

HAT FOLGENDE VERORDNUNG ERLASSEN:

Artikel 1

Gegenstand

Diese Verordnung enthält Vorschriften für die Reaktion auf Sicherheitsverletzungen der Brieftaschen, der Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 und des elektronischen Identifizierungssystems, in dessen Rahmen die Brieftaschen bereitgestellt werden.

Artikel 2

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Brieftaschenlösung“ eine Kombination aus Software, Hardware, Diensten, Einstellungen und Konfigurationen, einschließlich Brieftascheninstanzen, einer oder mehreren sicheren Kryptoanwendungen für Brieftaschen und einem oder mehreren sicheren Kryptomodulen für Brieftaschen;

2. „Brieftaschennutzer“ einen Nutzer, der die Kontrolle über die Einzelbrieftasche hat;

3. „auf Brieftaschen vertrauender Beteiligter“ einen vertrauenden Beteiligten, der beabsichtigt, zur Erbringung öffentlicher oder privater Dienste mittels digitaler Interaktion auf Einzelbrieftaschen zu vertrauen;

4. „Brieftascheninstanz“ die Anwendung, die als Bestandteil einer Einzelbrieftasche auf dem Gerät oder in der Umgebung eines Brieftaschennutzers installiert und konfiguriert ist und die der Brieftaschennutzer verwendet, um mit der Brieftasche zu interagieren;

5. „sichere Kryptoanwendung für Brieftaschen“ (*Wallet Secure Cryptographic Application*) eine Anwendung, die kritische Werte verwaltet und dabei mit den kryptografischen und nicht-kryptografischen Funktionen eines sicheren Kryptomoduls für Brieftaschen verknüpft ist und diese nutzt;

6. „sicheres Kryptomodul für Brieftaschen“ (*Wallet Secure Cryptographic Device*) eine manipulationssichere Vorrichtung, die eine Umgebung bietet, die mit der sicheren Kryptoanwendung für Brieftaschen verknüpft ist und von dieser genutzt wird, um kritische Werte zu schützen und kryptografische Funktionen für die sichere Ausführung kritischer Vorgänge bereitzustellen;

7. „Brieftaschenanbieter“ eine natürliche oder juristische Person, die Brieftaschenlösungen bereitstellt;

8. „Einzelbrieftasche“ eine einzigartige Konfiguration einer Brieftaschenlösung, die Brieftascheninstanzen, sichere Kryptoanwendungen für Brieftaschen und sichere Kryptomodule für Brieftaschen umfasst, die einem einzelnen Brieftaschennutzer von einem Brieftaschenanbieter bereitgestellt werden;

9. „kritische Werte“ Werte bzw. Daten innerhalb oder im Zusammenhang mit einer Einzelbrieftasche, die so außerordentlich wichtig sind, dass die Beeinträchtigung ihrer Verfügbarkeit, Vertraulichkeit oder Integrität eine sehr schwerwiegende, beeinträchtigende Wirkung auf die verlässliche Verwendbarkeit der Einzelbrieftasche hätte;

10. „Einzelbrieftaschenbescheinigung“ ein Datenobjekt, das die Komponenten der Einzelbrieftasche beschreibt oder die Authentifizierung und Validierung dieser Komponenten ermöglicht.

Artikel 3

Feststellung einer Sicherheitsverletzung oder -beeinträchtigung

(1) Unbeschadet der Richtlinie (EU) 2022/2555 und der Verordnungen (EU) 2019/881 und (EU) 2024/2847 berücksichtigen die Mitgliedstaaten bei der Prüfung, ob sich eine Sicherheitsverletzung oder -beeinträchtigung einer Brieftaschenlösung, der Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder des elektronischen Identifizierungssystems, in dessen Rahmen die Brieftaschenlösung bereitgestellt wird, auf deren Zuverlässigkeit oder die Zuverlässigkeit anderer Brieftaschenlösungen auswirkt, gebührend die in Anhang I der vorliegenden Verordnung festgelegten Kriterien.

(2) Stellt ein Mitgliedstaat auf der Grundlage der in Absatz 1 genannten Prüfung fest, dass sich eine Sicherheitsverletzung oder -beeinträchtigung auf die Zuverlässigkeit einer Brieftaschenlösung auswirkt, und setzt er die Bereitstellung und Nutzung dieser Brieftaschenlösung aus, so ergreift er die in den Artikeln 4 und 5 genannten Maßnahmen. Wenn ein Mitgliedstaat die Brieftaschenlösung zurückzieht, ergreift er die in den Artikeln 8 und 9 genannten Maßnahmen.

(3) Erlangt ein Mitgliedstaat Kenntnis von Informationen über eine mögliche Sicherheitsverletzung oder -beeinträchtigung, die sich auf die Zuverlässigkeit einer oder mehrerer von einem anderen Mitgliedstaat bereitgestellter Brieftaschenlösungen auswirken könnte, so meldet er dies unverzüglich der Kommission und den gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannten einheitlichen Anlaufstellen der betroffenen Mitgliedstaaten. Diese Meldung enthält die in Artikel 5 Absatz 2 genannten Angaben.

(4) Der Mitgliedstaat, der die nach Absatz 3 bereitgestellten Informationen erhält, ergreift unverzüglich die in den Absätzen 1 und 2 genannten Maßnahmen.

Artikel 4

Aussetzung der Bereitstellung und Nutzung von Brieftaschen und andere Abhilfemaßnahmen

(1) Die Mitgliedstaaten stellen sicher, dass im Rahmen der ausgesetzten Brieftaschenlösung keine Einzelbrieftaschen bereitgestellt, genutzt oder aktiviert werden.

(2) Die Mitgliedstaaten prüfen, ob der Widerruf von Einzelbrieftaschenbescheinigungen der von der Aussetzung einer Brieftaschenlösung betroffenen Einzelbrieftaschen oder andere zusätzliche Abhilfemaßnahmen als angemessene Reaktion auf die Sicherheitsverletzung oder -beeinträchtigung erforderlich sind.

(3) Die in den Absätzen 1 und 2 genannten Maßnahmen werden unverzüglich, jedenfalls aber spätestens 24 Stunden nach der Aussetzung der Bereitstellung und Nutzung der von der Sicherheitsverletzung oder -beeinträchtigung betroffenen Brieftaschenlösung ergriffen.

(4) Die in den Absätzen 1 und 2 genannten Maßnahmen dürfen die Brieftaschennutzer nicht an der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Artikel 5a Absatz 4 Buchstabe g der Verordnung (EU) Nr. 910/2014 hindern. Dies gilt unter der Bedingung, dass dieses Recht von Brieftaschennutzern ausgeübt werden kann, ohne die Sicherheit der kritischen Werte der betroffenen Einzelbrieftaschen zu beeinträchtigen, insbesondere unter Berücksichtigung der Gründe für die Aussetzung und der Notwendigkeit, den wirksamen Schutz dieser Werte vor Missbrauch zu gewährleisten.

Artikel 5

Informationen über Aussetzungen und Abhilfemaßnahmen

(1) Informationen über die Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung werden unverzüglich, spätestens aber 24 Stunden nach der Aussetzung der Bereitstellung und Nutzung der Brieftaschenlösung in klarer, umfassender und leicht zugänglicher Weise für folgende Empfänger bereitgestellt:

a) die gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannte einheitliche Anlaufstelle,

b) die Kommission,

c) die betroffenen Brieftaschennutzer,

d) die gemäß Artikel 5b der Verordnung (EU) Nr. 910/2014 registrierten auf Brieftaschen vertrauenden Beteiligten.

(2) Die nach Absatz 1 bereitgestellten Informationen umfassen zumindest Folgendes:

a) Name des Anbieters der Brieftaschenlösung, deren Bereitstellung und Nutzung ausgesetzt wurde,

b) Name und Referenzkennung dieser Brieftaschenlösung nach der gemäß Artikel 5d der Verordnung (EU) Nr. 910/2014 erstellten Liste der zertifizierten Brieftaschen und gegebenenfalls die betroffenen Versionen,

c) Datum und Uhrzeit der Erkennung der Sicherheitsverletzung oder -beeinträchtigung,

d) Datum und Uhrzeit des Wirksamwerdens der Sicherheitsverletzung oder -beeinträchtigung anhand von Netz- oder Systemprotokollen oder anderen Datenquellen, sofern bekannt,

e) Datum und Uhrzeit der Aussetzung der Brieftaschenlösung,

f) Kontaktdaten, zumindest mit einer E-Mail-Adresse und einer Telefonnummer für den meldenden Mitgliedstaat und — sofern davon abweichend — für den in Buchstabe a genannten Brieftaschenanbieter,

g) Beschreibung der Sicherheitsverletzung oder -beeinträchtigung,

h) Beschreibung der beeinträchtigten Daten, gegebenenfalls einschließlich der Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 und Artikel 10 der Verordnung (EU) 2016/679,

i) Schätzung der ungefähren Zahl der betroffenen Brieftaschennutzer und anderer betroffener natürlicher Personen, soweit möglich,

j) Beschreibung der potenziellen Auswirkungen auf die auf Brieftaschen vertrauenden Beteiligten oder Brieftaschennutzer und im letzteren Fall gegebenenfalls Hinweise auf Maßnahmen, die Brieftaschennutzer ergreifen können, um diese potenziellen Auswirkungen abzumildern,

k) Beschreibung der ergriffenen oder geplanten Maßnahmen zur Behebung der Sicherheitsverletzung oder -beeinträchtigung, mit einer Planung und Fristen für diese Abhilfemaßnahmen,

l) soweit zutreffend und angemessen, Beschreibung der ergriffenen oder geplanten Maßnahmen zur Umstellung der betroffenen Brieftaschennutzer auf alternative Brieftaschenlösungen oder -dienste.

Artikel 6

Wiederherstellung der Bereitstellung und Nutzung von Brieftaschen

Soweit dies zur Wiederherstellung der Bereitstellung, der Aktivierung und der Nutzung einer Brieftaschenlösung erforderlich ist, müssen die Mitgliedstaaten unverzüglich

1. die Bereitstellung und Nutzung der im Rahmen dieser Brieftaschenlösung bereitgestellten Einzelbrieftaschen wiederherstellen, indem sie allen betroffenen Brieftaschennutzern eine Einzelbrieftasche ausstellen, die im Rahmen einer neuen Version der Brieftaschenlösung bereitgestellt wird;

2. neue Einzelbrieftaschenbescheinigungen für neue Einzelbrieftaschen oder gegebenenfalls für zuvor ausgestellte Einzelbrieftaschen ausstellen, sofern diese Einzelbrieftaschen die nach der Behebung der Sicherheitsverletzung oder -beeinträchtigung geltenden Sicherheitsanforderungen erfüllen;

3. alle gemäß Artikel 4 ergriffenen Maßnahmen aufheben, die die Bereitstellung neuer Einzelbrieftaschen im Rahmen der betroffenen Brieftaschenlösung verhindern, falls sich solche Maßnahmen ausschließlich auf die nunmehr behobene Sicherheitsverletzung oder -beeinträchtigung bezogen.

Artikel 7

Informationen über die Wiederherstellung

Wenn ein Mitgliedstaat eine Brieftaschenlösung wiederherstellt, stellt er sicher, dass

1. Informationen hierüber unverzüglich allen Beteiligten, die Informationen über die Aussetzung der Bereitstellung und Nutzung dieser Brieftaschenlösung gemäß Artikel 5 Absatz 1 erhalten haben, zur Verfügung gestellt werden,

2. gemäß Nummer 1 bereitgestellte Informationen zumindest die in Artikel 5 Absatz 2 Buchstaben a, b und f bis h genannten Angaben sowie folgende Angaben enthalten:

   a) Datum und Uhrzeit der Behebung der Sicherheitsverletzung oder -beeinträchtigung,

   b) Datum und Uhrzeit der Wiederherstellung der betroffenen Brieftaschenlösung und gegebenenfalls der betroffenen, im Rahmen dieser Brieftaschenlösung bereitgestellten Einzelbrieftaschen,

   c) Beschreibung der Maßnahmen, die ergriffen wurden, um die Sicherheitsverletzung oder -beeinträchtigung zu beheben,

   d) Beschreibung der potenziellen verbleibenden Auswirkungen auf die auf Brieftaschen vertrauenden Beteiligten oder Brieftaschennutzer und im letzteren Fall gegebenenfalls Hinweise auf Maßnahmen, die Brieftaschennutzer ergreifen können, um diese potenziellen Auswirkungen abzumildern.

Artikel 8

Zurückziehung von Brieftaschen

(1) Wird eine Sicherheitsverletzung oder -beeinträchtigung, die die Aussetzung der Bereitstellung und Nutzung einer Brieftaschenlösung zur Folge hatte, nicht innerhalb von drei Monaten nach dem Datum der Aussetzung der Bereitstellung und Nutzung dieser Brieftaschenlösung behoben, so sorgt der Mitgliedstaat, der diese Brieftaschenlösung bereitgestellt hat, unverzüglich, jedenfalls aber innerhalb von 72 Stunden nach Ablauf der Dreimonatsfrist dafür, dass die betroffene Brieftaschenlösung zurückgezogen und ihre Gültigkeit widerrufen wird.

(2) Wenn ein Mitgliedstaat eine Brieftaschenlösung zurückzieht, stellt er sicher, dass

a) die Einzelbrieftaschenbescheinigungen der Einzelbrieftaschen der betroffenen Brieftaschenlösung widerrufen werden,

b) die Einzelbrieftaschenbescheinigungen nicht in einen gültigen Status zurückgesetzt werden können,

c) an bestehende Einzelbrieftaschen, die im Rahmen der betroffenen Brieftaschenlösung bereitgestellt wurden, keine neuen Einzelbrieftaschenbescheinigungen ausgestellt werden,

d) keine neuen Einzelbrieftaschen im Rahmen der betroffenen Brieftaschenlösung bereitgestellt werden können.

(3) Die in den Absätzen 1 und 2 genannten Maßnahmen dürfen die Brieftaschennutzer nicht an der Ausübung ihres Rechts auf Datenübertragbarkeit gemäß Artikel 5a Absatz 4 Buchstabe g der Verordnung (EU) Nr. 910/2014 hindern. Dies gilt unter der Bedingung, dass dieses Recht von Brieftaschennutzern ausgeübt werden kann, ohne die Sicherheit der kritischen Werte der betroffenen Einzelbrieftaschen zu beeinträchtigen, insbesondere unter Berücksichtigung der Gründe für die Zurückziehung und der Notwendigkeit, den wirksamen Schutz dieser Werte vor Missbrauch zu gewährleisten.

Artikel 9

Informationen über die Zurückziehung

(1) Informationen über die Zurückziehung einer Brieftaschenlösung werden unverzüglich, spätestens aber 24 Stunden nach der Zurückziehung der Brieftaschenlösung in klarer, umfassender und leicht zugänglicher Weise für folgende Empfänger bereitgestellt:

a) die gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannte einheitliche Anlaufstelle,

b) die Kommission,

c) die betroffenen Brieftaschennutzer,

d) die gemäß Artikel 5b der Verordnung (EU) Nr. 910/2014 registrierten auf Brieftaschen vertrauenden Beteiligten.

(2) Die nach Absatz 1 bereitgestellten Informationen umfassen zumindest Folgendes:

a) Name des Anbieters der Brieftaschenlösung, die zurückgezogen wurde,

b) Name und Referenzkennung dieser Brieftaschenlösung nach der gemäß Artikel 5d der Verordnung (EU) Nr. 910/2014 erstellten Liste der zertifizierten Brieftaschen und gegebenenfalls die betroffenen Versionen,

c) Datum und Uhrzeit der Erkennung der Sicherheitsverletzung oder -beeinträchtigung, die zur Zurückziehung der betroffenen Brieftaschenlösung führte, und zwar wegen ihrer Schwere oder weil sie nicht innerhalb von drei Monaten behoben wurde,

d) Datum und Uhrzeit des Wirksamwerdens der Sicherheitsverletzung oder -beeinträchtigung anhand von Netz- oder Systemprotokollen oder anderen Datenquellen, sofern bekannt,

e) Datum und Uhrzeit der Zurückziehung der Brieftaschenlösung und des wirksamen Widerrufs der Einzelbrieftaschenbescheinigungen der Einzelbrieftaschen, die im Rahmen der Brieftaschenlösung bereitgestellt wurden,

f) ob die Zurückziehung auf die Schwere der Sicherheitsverletzung oder -beeinträchtigung oder darauf zurückzuführen ist, dass die Sicherheitsverletzung oder -beeinträchtigung nicht behoben worden ist,

g) Kontaktdaten, zumindest mit einer E-Mail-Adresse und einer Telefonnummer für den meldenden Mitgliedstaat und — sofern davon abweichend — für den in Buchstabe a genannten Brieftaschenanbieter,

h) Beschreibung der Sicherheitsverletzung oder -beeinträchtigung,

i) Beschreibung der beeinträchtigten Daten, gegebenenfalls einschließlich der Kategorien personenbezogener Daten gemäß Artikel 9 Absatz 1 und Artikel 10 der Verordnung (EU) 2016/679,

j) Schätzung der ungefähren Zahl der betroffenen Brieftaschennutzer und anderer betroffener natürlicher Personen, soweit möglich,

k) Beschreibung der potenziellen Auswirkungen auf die auf Brieftaschen vertrauenden Beteiligten oder Brieftaschennutzer und im letzteren Fall gegebenenfalls Hinweise auf Maßnahmen, die Brieftaschennutzer ergreifen können, um diese potenziellen Auswirkungen abzumildern,

l) Beschreibung der ergriffenen oder geplanten Maßnahmen zur Umstellung der betroffenen Brieftaschennutzer auf alternative Brieftaschenlösungen oder, soweit zutreffend und angemessen, auf alternative Dienste.

Artikel 10

Informationssystem

Die Mitgliedstaaten übermitteln der Kommission und den gemäß Artikel 46c Absatz 1 der Verordnung (EU) Nr. 910/2014 benannten einheitlichen Anlaufstellen der Mitgliedstaaten die in den Artikeln 3, 5, 7 und 9 genannte Informationen über das von ENISA betriebene CIRAS oder über ein zwischen Mitgliedstaaten und Kommission vereinbartes gleichwertiges System.

Artikel 11

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat, mit Ausnahme des Artikels 10, der ab dem 7. Mai 2026 gilt.

Brüssel, den 6. Mai 2025

Für die Kommission
Die Präsidentin
Ursula VON DER LEYEN

ANHANG

Kriterien für die Bewertung einer Sicherheitsverletzung oder -beeinträchtigung

1. Die Mitgliedstaaten stützen ihre Bewertung einer Sicherheitsverletzung oder -beeinträchtigung auf folgende Kriterien:

   a) Die Sicherheitsverletzung oder -beeinträchtigung hat den Tod einer natürlichen Person oder eine schwere Schädigung der Gesundheit einer natürlichen Person verursacht oder kann diesen Tod oder diese Schädigung verursachen;

   b) ein erfolgreicher mutmaßlich böswilliger oder unbefugter Zugang zu den Netz- und Informationssystemen eines Brieftaschenanbieters, eines Anbieters von Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder eines Anbieters des elektronischen Identifizierungssystems, in dessen Rahmen eine Brieftaschenlösung bereitgestellt wird, (im Folgenden „betreffende Einrichtungen“) ist erfolgt oder kann erfolgen, und zwar in einer Weise, die geeignet ist, schwerwiegende Betriebsstörungen zu verursachen, und diese Systeme sind kritische Komponenten der betroffenen Brieftaschenlösung, der betroffenen Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder des betroffenen elektronischen Identifizierungssystems, in dessen Rahmen eine Brieftaschenlösung bereitgestellt wird;

   c) eine Brieftaschenlösung, ein Validierungsmechanismus gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 oder ein elektronisches Identifizierungssystem, in dessen Rahmen eine Brieftaschenlösung bereitgestellt wird, oder ein Teil davon, ist

      — für Brieftaschennutzer oder auf Brieftaschen vertrauende Beteiligte für mehr als zwölf aufeinanderfolgende Stunden tatsächlich oder voraussichtlich vollständig nicht verfügbar,

      — für Brieftaschennutzer oder auf Brieftaschen vertrauende Beteiligte im Laufe einer Kalenderwoche mehr als 16 Stunden lang tatsächlich oder voraussichtlich nicht verfügbar;

   d) mutmaßlich mehr als 1 % der Brieftaschennutzer oder der auf Brieftaschen vertrauenden Beteiligten ist von einer eingeschränkten Verfügbarkeit der Brieftaschenlösung oder der Dienste, die von betreffenden Einrichtungen im Zusammenhang mit der Brieftaschenlösung bereitgestellt werden, tatsächlich betroffen oder wird voraussichtlich davon betroffen sein;

   e) der auf vertrauenswürdiges Personal betreffender Einrichtungen beschränkte physische Zugang oder der Schutz eines solchen physischen Zugangs zu einem oder mehreren Standorten von Netz- und Informationssystemen, die die Brieftaschenlösung, die Bereitstellung der Validierungsmechanismen gemäß Artikel 5a Absatz 8 der Verordnung (EU) Nr. 910/2014 im Zusammenhang mit einer Brieftaschenlösung oder das elektronische Identifizierungssystem, in dessen Rahmen eine Brieftaschenlösung bereitgestellt wird, unterstützen, könnte beeinträchtigt werden oder ist tatsächlich beeinträchtigt worden;

   f) die Privatsphäre, Integrität, Vertraulichkeit oder Authentizität von in der Brieftaschenlösung gespeicherten, übermittelten oder verarbeiteten Daten ist auf eine oder mehrere der folgenden Weisen beeinträchtigt oder könnte beeinträchtigt werden:

      — dies hat Auswirkungen auf mehr als 1 % der Brieftaschennutzer der betroffenen Brieftaschenlösung oder auf mehr als 100 000 dieser Brieftaschennutzer, je nachdem, welche Zahl kleiner ist;

      — dies ist das Ergebnis einer erfolgreichen mutmaßlich böswilligen Aktivität;

      — dies ist tatsächlich oder wahrscheinlich das Ergebnis einer oder mehrerer bekannter Schwachstellen, einschließlich der gemäß der Durchführungsverordnung (EU) 2024/2981 der Kommission [1] behandelten Schwachstellen;

      — dies dürfte sich auf personenbezogen Daten in einer Weise auswirken, die ein Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen zur Folge hat, insbesondere im Fall einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 9 Absatz 1 und Artikel 10 der Verordnung (EU) 2016/679;

[1] Durchführungsverordnung (EU) 2024/2981 der Kommission vom 28. November 2024 zur Festlegung der Vorschriften für die Anwendung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates in Bezug auf die Integrität und die Kernfunktionen europäischer Brieftaschen für die digitale Identität (ABl. L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— dies dürfte sich auf die persönliche elektronische Kommunikation auswirken;

— dies hat voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge;

— dies dürfte sich auf schutzbedürftige natürliche Personen auswirken;

g) die Zertifizierung der Brieftaschenlösung ist aufgehoben worden oder wird voraussichtlich aufgehoben;

h) die Sicherheitsverletzung oder Beeinträchtigung hat einer betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder, falls zutreffend, von 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr — je nachdem, welcher Wert niedriger ist — verursacht oder kann einen solchen Verlust verursachen.

2. Die Mitgliedstaaten berücksichtigen keine geplanten Folgen von Wartungsarbeiten, die von oder im Auftrag der betreffenden Einrichtungen durchgeführt werden, sofern diese Wartungsarbeiten

a) den potenziell betroffenen Brieftaschennutzern, auf Brieftaschen vertrauenden Beteiligten und jeweils zuständigen Aufsichtsbehörden vorab angekündigt worden sind,

b) keines der in Nummer 1 dieses Anhangs aufgeführten Kriterien erfüllen.

3. In Bezug auf Nummer 1 Buchstabe (c) erfolgt die Messung der Dauer eines Sicherheitsvorfalls, der die Verfügbarkeit beeinträchtigt, von dem Zeitpunkt, ab dem die ordnungsgemäße Erbringung des betroffenen Dienstes gestört ist, bis zu dem Zeitpunkt, zu dem der Dienst wiederhergestellt ist und in Betrieb geht. Wenn eine betreffende Einrichtung nicht imstande ist, den Zeitpunkt des Beginns der Störung zu bestimmen, wird die Dauer des Sicherheitsvorfalls ab dem Zeitpunkt gemessen, zu dem der Sicherheitsvorfall erkannt wurde, oder ab dem Zeitpunkt, zu dem der Sicherheitsvorfall in Netz- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet wurde, je nachdem, welcher Zeitpunkt früher ist. Eine vollständige Nichtverfügbarkeit eines Dienstes wird von dem Zeitpunkt an gemessen, zu dem der Dienst für die Nutzer vollständig nicht verfügbar ist, bis zu dem Zeitpunkt, zu dem die gewöhnlichen Tätigkeiten oder Abläufe wieder das vor dem Sicherheitsvorfall bestehende Dienstniveau erreicht haben. Wenn eine betreffende Einrichtung nicht imstande ist, den Zeitpunkt des Beginns der vollständigen Nichtverfügbarkeit eines Dienstes zu bestimmen, wird die Nichtverfügbarkeit ab dem Zeitpunkt gemessen, zu dem sie von der Einrichtung festgestellt wurde.

4. In Bezug auf Nummer 1 Buchstabe (d) wird von einer eingeschränkten Verfügbarkeit eines Dienstes insbesondere dann ausgegangen, wenn ein Dienst deutlich langsamer als die durchschnittliche Antwortzeit ist oder wenn nicht alle Funktionen eines Dienstes verfügbar sind. Zur Bewertung von Verzögerungen bei der Antwortzeit sollten — soweit möglich — objektive Kriterien auf der Grundlage der durchschnittlichen Antwortzeiten von Diensten herangezogen werden.

5. Bei der Bestimmung der direkten finanziellen Verluste infolge einer in Nummer 1 Buchstabe (h) genannten Sicherheitsverletzung oder Beeinträchtigung berücksichtigen die betreffenden Einrichtungen alle finanziellen Verluste, die ihnen infolge des Sicherheitsvorfalls entstanden sind, wie etwa Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur, Personalkosten, einschließlich Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung zusätzlichen Personals, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen, Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen, Kosten für Ausgleichs- und Entschädigungszahlungen an Kunden, Verluste wegen entgangener Einnahmen, Kosten für interne und externe Kommunikation, Beratungskosten, einschließlich Kosten im Zusammenhang mit Rechtsberatung, forensischen Dienstleistungen und Behebungsdienstleistungen. Kosten, die für den laufenden Geschäftsbetrieb erforderlich sind, wie etwa Kosten für die allgemeine Wartung von Infrastruktur, Ausrüstung, Hardware und Software, für Verbesserungen und Initiativen zur Risikobewertung sowie Versicherungsprämien, werden nicht als finanzielle Verluste infolge eines Vorfalls betrachtet. Die betreffenden Einrichtungen berechnen die Höhe der finanziellen Verluste auf der Grundlage vorliegender Daten, und wenn die tatsächliche Höhe der finanziellen Verluste nicht bestimmt werden kann, schätzen die Einrichtungen solche Beträge.