Publicatieblad
van de Europese Unie

NL
L-serie

2025/847

7.5.2025

UITVOERINGSVERORDENING (EU) 2025/847 VAN DE COMMISSIE

van 6 mei 2025

tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad inzake de reactie op inbreuken op de beveiliging van Europese portemonnees voor digitale identiteit

DE EUROPESE COMMISSIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG ([1]), en met name artikel 5 sexies, lid 5,

Overwegende hetgeen volgt:

(1) Het bij Verordening (EU) nr. 910/2014 vastgestelde Europees kader voor digitale identiteit ("het kader") is een cruciaal onderdeel van de totstandbrenging van een veilig en interoperabel ecosysteem voor digitale identiteit in de hele Unie. Met de Europese portemonnee voor digitale identiteit ("de portemonnee") als hoeksteen heeft het kader tot doel de toegang tot diensten in alle lidstaten te vergemakkelijken en de bescherming van persoonsgegevens en de persoonlijke levenssfeer te waarborgen.

(2) Verordeningen (EU) 2016/679 ([2]) en (EU) 2018/1725 ([3]) van het Europees Parlement en de Raad en, in voorkomend geval, Richtlijn 2002/58/EG van het Europees Parlement en de Raad ([4]) zijn van toepassing op de activiteiten betreffende de verwerking van persoonsgegevens uit hoofde van deze verordening. De bij deze verordening vastgestelde regels inzake de beoordeling en de verstrekking van informatie doen geen afbreuk aan de verplichting om inbreuken in verband met persoonsgegevens te melden aan de bevoegde toezichthoudende autoriteit, indien van toepassing uit hoofde van Verordening (EU) 2016/679 of Verordening (EU) 2018/1725, noch aan de verplichting om inbreuken in verband met persoonsgegevens aan de betrokkenen mee te delen, indien van toepassing uit hoofde van deze verordeningen.

(3) De Commissie voert regelmatig beoordelingen uit van nieuwe technologieën, praktijken, normen en technische specificaties. Om het hoogste niveau van harmonisatie tussen de lidstaten te waarborgen voor de ontwikkeling en de certificering van de portemonnees, berusten de in deze uitvoeringsverordening vastgestelde technische specificaties op de werkzaamheden op basis van Aanbeveling (EU) 2021/946 van de Commissie ([5]), en met name de architectuur en het referentiekader die daar deel van uitmaken. Overeenkomstig overweging 75 van Verordening (EU) 2024/1183 van het Europees Parlement en de Raad ([6]) moet de Commissie deze uitvoeringsverordening evalueren en in voorkomend geval actualiseren om deze in overeenstemming te houden met de mondiale ontwikkelingen en de architectuur en het referentiekader en om de beste praktijken op de interne markt te volgen.

([1]) PB L 257 van 28.8.2014, blz. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB L 119 van 4.5.2016, blz. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Verordening (EU) 2018/1725 van het Europees Parlement en de Raad van 23 oktober 2018 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de instellingen, organen en instanties van de Unie en betreffende het vrije verkeer van die gegevens, en tot intrekking van Verordening (EG) nr. 45/2001 en Besluit nr. 1247/2002/EG (PB L 295 van 21.11.2018, blz. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([4]) Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB L 201 van 31.7.2002, blz. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Aanbeveling (EU) 2021/946 van de Commissie van 3 juni 2021 betreffende een gemeenschappelijke EU-toolbox voor een gecoördineerde aanpak ten behoeve van een Europees kader voor digitale identiteit (PB L 210 van 14.6.2021, blz. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Verordening (EU) 2024/1183 van het Europees Parlement en de Raad van 11 april 2024 tot wijziging van Verordening (EU) nr. 910/2014, wat betreft de vaststelling van het Europees kader voor digitale identiteit (PB L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) In geval van een beveiligingsinbreuk of -aantasting van de portemonneeoplossingen of van de valideringsmechanismen als bedoeld in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014, of van het stelsel voor elektronische identificatie op grond waarvan de portemonneeoplossingen worden verstrekt, moet er in alle lidstaten snel, gecoördineerd en veilig op dergelijke beveiligingsinbreuken of aantastingen worden gereageerd om de gebruikers te beschermen en het vertrouwen in het ecosysteem voor digitale identiteit in stand te houden. Dit laat Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad ([7]) en Verordeningen (EU) 2019/881 ([8]) en (EU) 2024/2847 ([9]) van het Europees Parlement en de Raad onverlet, in het bijzonder ten aanzien van de aanpak van incidenten en kwetsbaarheden en de vraag of die als beveiligingsinbreuken moeten worden beschouwd. Daarom moeten de lidstaten waarborgen dat de verstrekking en het gebruik van door een beveiligingsinbreuk of aantasting getroffen portemonnees tijdig worden opgeschort, of, in voorkomend geval, worden ingetrokken.

(5) Om passend op een beveiligingsinbreuk of aantasting te kunnen reageren, moeten de lidstaten beoordelen of een beveiligingsinbreuk of -aantasting van een portemonnee, van de in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde valideringsmechanismen, of van het stelsel voor elektronische identificatie op grond waarvan een portemonneeoplossing wordt verstrekt, de betrouwbaarheid van die portemonneeoplossing of van andere portemonneeoplossingen beïnvloedt. Die beoordeling moet gebaseerd zijn op uniforme criteria, zoals het aantal en de categorie van getroffen portemonneegebruikers, natuurlijke personen en op portemonnees vertrouwende partijen, de aard van de getroffen gegevens, de duur van de aantasting of beveiligingsinbreuk, de beperkte beschikbaarheid van een dienst en financiële verliezen, en de mogelijke aantasting van persoonsgegevens. Op basis van die criteria moeten de lidstaten voldoende flexibel en discretionair kunnen bepalen of de betrouwbaarheid van een portemonneeoplossing is aangetast en of de opschorting of, indien gerechtvaardigd door de ernst van de inbreuk of de aantasting, de intrekking van de portemonneeoplossing passend is. Die criteria mogen niet leiden tot een automatische intrekking van een portemonneeoplossing of een automatische opschorting van de verstrekking en het gebruik van een portemonneeoplossing, maar moeten door de lidstaten zorgvuldig worden overwogen bij hun beslissing of de intrekking of de opschorting van de verstrekking en het gebruik van een portemonneeoplossing nodig is.

(6) Vanwege de gevolgen en het ongemak ten gevolge van de opschorting van het gebruik van portemonneeoplossingen, moeten de lidstaten beoordelen of de intrekking van portemonnee-eenheidsattesteringen of andere aanvullende maatregelen nodig zijn als adequate reactie op de beveiligingsinbreuk of -aantasting.

(7) Om portemonneegebruikers op de hoogte te houden van de status van hun portemonnees, moeten zij adequate informatie krijgen over beveiligingsinbreuken of aantastingen die hun portemonnees raken. Aangezien ook in de Unie geregistreerde op portemonnees vertrouwende partijen door beveiligingsinbreuken en aantastingen kunnen worden getroffen, moet relevante informatie over beveiligingsinbreuken en aantastingen ook met hen worden gedeeld.

(8) Met het oog op transparantie en een groter vertrouwen in het ecosysteem voor digitale identiteit moet de informatie over de beveiligingsinbreuken of -aantastingen, en over de gevolgen daarvan, ten minste de overeenkomstig deze verordening vereiste informatie bevatten. De informatie over beveiligingsinbreuken of aantastingen die met portemonneegebruikers en met op portemonnees vertrouwende partijen worden gedeeld, moet echter zorgvuldig worden beoordeeld, zodat het risico van misbruik door aanvallers wordt voorkomen en geminimaliseerd.

([7]) Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972, en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-Richtlijn) (PB L 333 van 27.12.2022, blz. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (PB L 151 van 7.6.2019, blz. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (PB L, 2024/2847 van 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Om gebruikers opnieuw toegang te geven tot hun portemonnees nadat een beveiligingsinbreuk of -aantasting is verholpen, moet de lidstaat die de portemonneeoplossingen heeft verstrekt, de verstrekking en het gebruik van die portemonneeoplossingen onverwijld herstellen. Dit kan geschieden door de portemonnee-eenheden te herstellen, door portemonnee-eenheden af te geven op grond van een nieuwe versie van de portemonneeoplossingen of door weer nieuwe geldige attesteringen van de portemonnee-eenheid af te geven. Getroffen portemonneegebruikers, op portemonnees vertrouwende partijen, de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) 910/2014 aangeduide centrale contactpunten en de Commissie moeten daarvan in kennis worden gesteld.

(10) Om te waarborgen dat de portemonnees worden ingetrokken indien een beveiligingsinbreuk of -aantasting niet binnen drie maanden na de opschorting is verholpen of indien de ernst van de beveiligingsinbreuk of de aantasting daartoe noopt, moet de lidstaat ervoor zorgen dat de desbetreffende attesteringen van de portemonnee-eenheid worden ingetrokken en niet naar een geldige staat kunnen terugkeren en evenmin aan bestaande portemonnee-eenheden kunnen worden afgegeven of verstrekt. Bovendien mogen geen nieuwe portemonnee-eenheden worden verstrekt op grond van de getroffen portemonneeoplossing. Met het oog op de transparantie moeten gebruikers, op portemonnees vertrouwende partijen, de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) nr. 910/2014 aangeduide centrale contactpunten en de Commissie van de intrekking in kennis worden gesteld. Dit omvat een beschrijving van de mogelijke gevolgen voor de portemonneegebruikers en met name het beheer van afgegeven attesteringen, of voor op portemonnees vertrouwende partijen.

(11) De periode van drie maanden na de opschorting van de levering en het gebruik van een portemonnee-oplossing en waarin de beveiligingsinbreuk of -aantasting die tot die opschorting heeft geleid, moet worden verholpen, moet een termijn bevatten waarna de portemonneeoplossing moet worden ingetrokken, tenzij een passende oplossing is geïmplementeerd. Het staat de lidstaten echter vrij om verlangen dat de beveiligingsinbreuk of -aantasting binnen een termijn van minder dan drie maanden wordt verholpen, waarbij in het bijzonder en in voorkomend geval de omvang, de duur en de gevolgen van die beveiligingsinbreuk of -aantasting in aanmerking worden genomen. Indien de beveiligingsinbreuk of -aantasting niet binnen de door de lidstaat vastgestelde termijn wordt of kan worden verholpen, kan de lidstaat verlangen dat de portemonnee-oplossing vóór het verstrijken van de termijn van drie maanden wordt ingetrokken. De lidstaten moeten die termijn voor het verhelpen van een beveiligingsinbreuk of -aantasting die heeft geleid tot de opschorting van de levering en het gebruik van een portemonnee-oplossing, gebruiken om de mogelijke intrekking van die portemonnee-oplossing en de daaruit voortvloeiende mededelingen voor te bereiden.

(12) Om de administratieve lasten voor de lidstaten met betrekking tot de overeenkomstig deze verordening aan de Commissie en aan andere lidstaten te verzenden informatie te verminderen, moeten de lidstaten gebruikmaken van bestaande kennisgevingsinstrumenten, zoals het systeem voor de melding en analyse van cyberincidenten ("CIRAS"), dat wordt beheerd door het Agentschap van de Europese Unie voor cyberbeveiliging ("Enisa"). Met betrekking tot alternatieve kanalen of middelen om door een beveiligingsinbreuk of -aantasting getroffen portemonneegebruikers en op portemonnees vertrouwende partijen te informeren, moeten de lidstaten waarborgen dat de relevante informatie op een duidelijke, volledige en eenvoudig toegankelijke wijze wordt verstrekt. De kanalen om die informatie te verstrekken aan getroffen portemonneegebruikers en op portemonnees vertrouwende partijen moeten passende oplossingen omvatten voor websiteuitzendingen, realtime tracking van website-updates en nieuwsaggregatie.

(13) De Europese Toezichthouder voor gegevensbescherming is overeenkomstig artikel 42, lid 1, van Verordening (EU) 2018/1725 geraadpleegd en heeft op 31 januari 2025 een advies uitgebracht.

(14) De in deze verordening vervatte maatregelen zijn in overeenstemming met het advies van het bij artikel 48 van Verordening (EU) nr. 910/2014 ingestelde comité,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Onderwerp

Deze verordening stelt regels vast voor de reactie op inbreuken op de beveiliging van de portemonnees, van de in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde valideringsmechanismen en van het stelsel voor elektronische identificatie op grond waarvan de portemonnees worden verstrekt.

Artikel 2

Definities

Voor de doelstellingen van deze verordening, zijn de volgende definities van toepassing:

1) "portemonneeoplossing": een combinatie van software, hardware, diensten, instellingen en configuraties, met inbegrip van portemonnee-instanties, een of meer beveiligde cryptografische toepassingen voor portemonnees en een of meer beveiligde cryptografische middelen voor portemonnees;

2) "portemonneegebruiker": een gebruiker die de controle heeft over de portemonnee-eenheid;

3) "op portemonnees vertrouwende partij": een vertrouwende partij die voornemens is portemonnee-eenheden te gebruiken voor het verlenen van publieke of private diensten door middel van digitale interactie;

4) "portemonnee-instantie": de toepassing die is geïnstalleerd en geconfigureerd op het apparaat of in de omgeving van een gebruiker van de portemonnee, die deel uitmaakt van een portemonnee-eenheid, en die de portemonnee-gebruiker gebruikt voor de interactie met de portemonnee-eenheid;

5) "beveiligde cryptografische toepassing voor portemonnees": een toepassing die kritieke activa beheert door middel van koppeling aan en gebruikmaking van de cryptografische en niet-cryptografische functies van het beveiligd cryptografisch middel voor portemonnees;

6) "beveiligd cryptografisch middel voor portemonnees": een manipulatiebestendig apparaat dat een omgeving biedt die gekoppeld is aan en wordt gebruikt door de beveiligde cryptografische toepassing voor portemonnees om kritieke activa te beschermen en cryptografische functies te bieden voor de veilige uitvoering van kritieke activiteiten;

7) "aanbieder van portemonnees": een natuurlijke of rechtspersoon die portemonneeoplossingen aanbiedt;

8) "portemonnee": een unieke configuratie van een portemonneeoplossing die bestaat uit portemonnee-instanties, beveiligde cryptografische toepassingen voor portemonnees en beveiligde cryptografische middelen voor portemonnees die door een aanbieder van portemonnees aan een individuele portemonneegebruiker worden verstrekt;

9) "kritieke activa": activa in of met betrekking tot een portemonnee-eenheid die van dermate groot belang zijn dat, als de beschikbaarheid, de authenticiteit of de integriteit ervan in gevaar zou komen, dat een zeer ernstig, verzwakkend effect zou hebben op het vermogen om de portemonnee-eenheid te kunnen gebruiken;

10) "portemonnee-eenheidsattestering": een gegevensobject dat de componenten van de portemonnee-eenheid beschrijft en authenticatie en validering van die componenten mogelijk maakt.

Artikel 3

Vaststelling van een beveiligingsinbreuk of -aantasting

1. Onverminderd Richtlijn (EU) 2022/2555 en Verordeningen (EU) 2019/881 en (EU) 2024/2847 nemen de lidstaten bij de beoordeling of een beveiligingsinbreuk of -aantasting van een portemonneeoplossing, van de in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde valideringsmechanismen of van het stelsel voor elektronische identificatie op grond waarvan de portemonneeoplossing is verstrekt, gevolgen heeft voor de betrouwbaarheid ervan of voor de betrouwbaarheid van andere portemonneeoplossingen, de in bijlage I vastgestelde criteria in aanmerking.

2. Indien een lidstaat op basis van de beoordeling in lid 1 vaststelt dat een beveiligingsinbreuk of -aantasting de betrouwbaarheid van een portemonneeoplossing aantast en hij de verstrekking en het gebruik van die portemonnee-oplossing opschort, treft die lidstaat de in de artikelen 4 en 5 genoemde maatregelen. Indien een lidstaat de portemonnee-oplossing intrekt, treft hij de in de artikelen 8 en 9 genoemde maatregelen.

3. Indien een lidstaat kennis krijgt van informatie over een mogelijke beveiligingsinbreuk of -aantasting die de betrouwbaarheid van een of meer door een andere lidstaat verstrekte portemonneeoplossingen kan aantasten, stelt die lidstaat de Commissie en de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) nr. 910/2014 aangewezen centrale contactpunten van de getroffen lidstaten onverwijld daarvan in kennis. Die mededeling bevat de uit hoofde van artikel 5, lid 2, bedoelde informatie.

4. De lidstaat die informatie op grond van lid 3 ontvangt, treft onverwijld de in de leden 1 en 2 genoemde maatregelen.

Artikel 4

Opschorting van de verstrekking en het gebruik van portemonnees en andere maatregelen

1. De lidstaten waarborgen dat geen portemonnees worden verstrekt, gebruikt of geactiveerd op grond van de opgeschorte portemonneeoplossing.

2. De lidstaten beoordelen of de intrekking van attesteringen van de portemonnee-eenheid van de door de opschorting van een portemonneeoplossing getroffen portemonnee-eenheden of een andere aanvullende maatregel nodig is om adequaat op de beveiligingsinbreuk of -aantasting te reageren.

3. De in de leden 1 en 2 genoemde maatregelen worden onverwijld getroffen, en in ieder geval uiterlijk 24 uur na de opschorting van de verstrekking en het gebruik van de door de beveiligingsinbreuk of -aantasting getroffen portemonnee-oplossing.

4. De in de leden 1 en 2 genoemde maatregelen beletten niet dat de getroffen portemonneegebruikers hun rechten op gegevensoverdraagbaarheid overeenkomstig artikel 5 bis, lid 4, punt g), van Verordening (EU) nr. 910/2014 uitoefenen. Dit is onder de voorwaarde dat de portemonneegebruikers dit recht kunnen uitoefenen zonder afbreuk te doen aan de beveiliging van de kritieke activa van de getroffen portemonnee-eenheden, met name gezien de redenen voor de opschorting en de noodzaak om een doeltreffende bescherming van die activa tegen misbruik te waarborgen.

Artikel 5

Informatie over opschortingen en maatregelen

1. Informatie over de opschorting van de verstrekking en het gebruik van een portemonneeoplossing wordt op duidelijke, volledige en eenvoudig toegankelijke wijze, onverwijld en uiterlijk 24 uur na de opschorting van de verstrekking en het gebruik van de portemonneeoplossing verstrekt aan:

a) de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) nr. 910/2014 aangewezen centrale contactpunten;

b) de Commissie;

c) de getroffen portemonneegebruikers;

d) de overeenkomstig artikel 5 ter van Verordening (EU) nr. 910/2014 geregistreerde op portemonnees vertrouwende partijen.

2. De overeenkomstig lid 1 verstrekte informatie omvat in ieder geval de volgende elementen:

a) de naam van de aanbieder van de portemonneeoplossing waarvan de verstrekking en het gebruik is opgeschort;

b) de naam en de referentie van die portemonneeoplossing, zoals vermeld op de overeenkomstig artikel 5 quinquies van Verordening (EU) nr. 910/2014 opgestelde lijst van gecertificeerde portemonnees, en, in voorkomend geval, de betrokken versies;

c) de datum en het tijdstip waarop de beveiligingsinbreuk of -aantasting is vastgesteld;

d) indien bekend, de datum en het tijdstip waarop de beveiligingsinbreuk of -aantasting zich heeft voorgedaan, op basis van netwerk- of systeemlogbestanden of andere gegevensbronnen;

e) de datum en het tijdstip van de opschorting van de portemonneeoplossing;

f) de contactgegevens, waaronder ten minste een e-mailadres en een telefoonnummer voor de kennisgevende lidstaat, en, indien verschillend, voor de in punt (a) bedoelde portemonneeaanbieder;

g) een beschrijving van de beveiligingsinbreuk of -aantasting;

h) een beschrijving van de aangetaste gegevens, met inbegrip van, in voorkomend geval, de categorieën persoonsgegevens in de zin van artikel 9, lid 1, en artikel 10 van Verordening (EU) 2016/679;

i) indien mogelijk, een raming van het aantal getroffen portemonneegebruikers en van andere getroffen natuurlijke personen;

j) een beschrijving van de mogelijke gevolgen voor op portemonnees vertrouwende partijen of voor portemonneegebruikers, en in het laatste geval, in voorkomend geval, aanwijzingen voor maatregelen die gebruikers van portemonnees kunnen treffen om die mogelijke gevolgen te beperken;

k) een beschrijving van de maatregelen die zijn getroffen of gepland om de beveiligingsinbreuk of -aantasting te verhelpen, met een planning en een uiterste termijn voor die oplossing;

l) een beschrijving van de maatregelen die zijn getroffen of gepland om de getroffen portemonneegebruikers naar alternatieve portemonneeoplossingen of diensten over te brengen, waar passend en van toepassing.

Artikel 6

Herstel van de verstrekking en het gebruik van portemonnees

Indien nodig om de verstrekking, de activering en het gebruik van een portemonneeoplossing te doen herstellen, zullen de lidstaten onverwijld:

1. de verstrekking en het gebruik van de op grond van die portemonneeoplossing verstrekte portemonnee-eenheden herstellen door aan alle getroffen gebruikers een portemonnee-eenheid af te geven op basis van een nieuwe versie van de portemonneeoplossing;

2. nieuwe attesteringen van de portemonnee-eenheid afgeven aan nieuwe portemonnee-eenheden of, indien van toepassing, aan eerder afgegeven portemonnee-eenheden, mits die portemonnee-eenheden voldoen aan de beveiligingseisen die van toepassing zijn nadat de inbreuk of de aantasting is verholpen;

3. de maatregelen intrekken die overeenkomstig artikel 4 zijn uitgevoerd en die de verstrekking van nieuwe portemonnee-eenheden op grond van de getroffen portemonneeoplossing verhinderen, indien die maatregel uitsluitend verband hield met de nu voor alsdan verholpen beveiligingsinbreuk of -aantasting.

Artikel 7

Informatie over herstel

Indien een lidstaat een portemonneeoplossing herstelt, waarborgt hij dat:

1. informatie over dat feit onverwijld wordt verstrekt aan alle partijen die informatie over de opschorting van de levering en het gebruik van die portemonnee-oplossing overeenkomstig artikel 5, lid 1 hebben ontvangen.

2. De overeenkomstig punt 1. verstrekte informatie omvat ten minste de in artikel 5, lid 2, punten a), b) en f) tot en met h), bedoelde elementen en de volgende:

   a) de datum en het tijdstip waarop de beveiligingsinbreuk of -aantasting is verholpen;

   b) de datum en het tijdstip van het herstel van de getroffen portemonneeoplossing en, in voorkomend geval, van de getroffen portemonnee-eenheden die op grond van die portemonneeoplossing worden verstrekt;

   c) een beschrijving van de maatregelen om de beveiligingsinbreuk of -aantasting te verhelpen;

   d) een beschrijving van de mogelijke resterende gevolgen voor op portemonnees vertrouwende partijen of voor portemonneegebruikers, en in het laatste geval, in voorkomend geval, aanwijzingen voor maatregelen die gebruikers van portemonnees kunnen treffen om die mogelijke resterende gevolgen te beperken.

Artikel 8

Intrekking van portemonnees

1. Indien een beveiligingsinbreuk of -aantasting die tot de opschorting van de verstrekking en het gebruik van een portemonneeoplossing heeft geleid, niet binnen drie maanden na de datum van opschorting van de verstrekking en het gebruik van die portemonneeoplossing wordt verholpen, zorgt de lidstaat die die portemonnee verstrekt ervoor dat de getroffen portemonneeoplossing en de geldigheid ervan onverwijld en in ieder geval uiterlijk 72 uur na verloop van de termijn van drie maanden wordt ingetrokken.

2. Indien een lidstaat een portemonneeoplossing intrekt, waarborgt hij dat:

a) de attesteringen van de portemonnee-eenheid van de getroffen portemonneeoplossing worden ingetrokken;

b) de attesteringen van de portemonnee-eenheid niet naar een geldige staat kunnen terugkeren;

c) op grond van de getroffen portemonneeoplossing geen nieuw attesteringen van de portemonnee-eenheid kunnen worden afgegeven aan bestaande portemonnee-eenheden;

d) geen nieuwe portemonnee-eenheden kunnen worden verstrekt op grond van de getroffen portemonneeoplossing.

3. De in de leden 1 en 2 genoemde maatregelen beletten niet dat de getroffen portemonneegebruikers hun rechten op gegevensoverdraagbaarheid overeenkomstig artikel 5 bis, lid 4, punt g), van Verordening (EU) nr. 910/2014 uitoefenen. Dit is onder de voorwaarde dat de portemonneegebruikers dit recht kunnen uitoefenen zonder afbreuk te doen aan de beveiliging van de kritieke activa van de getroffen portemonnee-eenheden, met name gezien de redenen voor de intrekking en de noodzaak om een doeltreffende bescherming van die activa tegen misbruik te waarborgen.

Artikel 9

Informatie over intrekking

1. Informatie over de intrekking van een portemonneeoplossing wordt op duidelijke, volledige en eenvoudig toegankelijke wijze, onverwijld en uiterlijk 24 uur na de intrekking van de portemonneeoplossing verstrekt aan:

a) de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) nr. 910/2014 aangewezen centrale contactpunten;

b) de Commissie;

c) de getroffen portemonneegebruikers;

d) de overeenkomstig artikel 5 ter van Verordening (EU) nr. 910/2014 geregistreerde op portemonnees vertrouwende partijen.

2. De overeenkomstig lid 1 verstrekte informatie omvat in ieder geval de volgende elementen:

a) de naam van de aanbieder van de portemonneeoplossing die is ingetrokken;

b) de naam en de referentie van die portemonneeoplossing, zoals vermeld op de overeenkomstig artikel 5 quinquies van Verordening (EU) nr. 910/2014 opgestelde lijst van gecertificeerde portemonnees, en, in voorkomend geval, de betrokken versies;

c) de datum en het tijdstip van de ontdekking van de beveiligingsinbreuk of -aantasting die heeft geleid tot de intrekking van de getroffen portemonneeoplossing vanwege de ernst ervan of omdat die niet binnen drie maanden is verholpen;

d) indien bekend, de datum en het tijdstip waarop de beveiligingsinbreuk of -aantasting zich heeft voorgedaan, op basis van netwerk- of systeemlogbestanden of andere gegevensbronnen;

e) de datum en het tijdstip van de intrekking van de portemonneeoplossing en van de daadwerkelijke intrekking van de attesteringen van de portemonnee-eenheid van de op grond van die portemonneeoplossing verstrekte portemonnee-eenheden;

f) of de intrekking het gevolg is van de ernst van de beveiligingsinbreuk of -aantasting, of van het feit dat de beveiligingsinbreuk of -aantasting niet is verholpen;

g) de contactgegevens, waaronder ten minste een e-mailadres en een telefoonnummer voor de kennisgevende lidstaat, en, indien verschillend, voor de in punt a) bedoelde portemonneeaanbieder;

h) een beschrijving van de beveiligingsinbreuk of -aantasting;

i) een beschrijving van de aangetaste gegevens, met inbegrip van, in voorkomend geval, de categorieën persoonsgegevens in de zin van artikel 9, lid 1, en artikel 10 van Verordening (EU) 2016/679;

j) indien mogelijk, een raming van het aantal getroffen portemonneegebruikers en van andere getroffen natuurlijke personen;

k) een beschrijving van de mogelijke gevolgen voor op portemonnees vertrouwende partijen of voor portemonneegebruikers, en in het laatste geval, in voorkomend geval, aanwijzingen voor maatregelen die gebruikers van portemonnees kunnen treffen om die mogelijke gevolgen te beperken;

l) een beschrijving van de maatregelen die zijn getroffen of gepland om de getroffen portemonneegebruikers naar alternatieve portemonneeoplossingen of alternatieve diensten over te brengen, waar passend en van toepassing.

Artikel 10

Informatiesysteem

De lidstaten zenden de in de artikelen 3, 5, 7 en 9 bedoelde informatie toe aan de Commissie en de overeenkomstig artikel 46 quater, lid 1, van Verordening (EU) nr. 910/2014 aangewezen centrale contactpunten van de lidstaten via het door Enisa beheerde CIRAS, of een gelijkwaardig systeem dat door de lidstaten en de Commissie is overeengekomen.

Artikel 11

Inwerkingtreding

Deze verordening treedt in werking op de twintigste dag na die van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat, met uitzondering van artikel 10, dat van toepassing is met ingang van 7 mei 2026.

Gedaan te Brussel, 6 mei 2025.

Voor de Commissie
De voorzitter
Ursula VON DER LEYEN

BIJLAGE

Criteria ter beoordeling van een beveiligingsinbreuk of -aantasting

1. De lidstaten baseren hun beoordeling van een beveiligingsinbreuk of -aantasting op de onderstaande criteria:

a) de beveiligingsinbreuk of -aantasting heeft aanzienlijke schade aan de gezondheid of de dood van een natuurlijke persoon veroorzaakt of kan dit veroorzaken;

b) er heeft zich met succes een vermoedelijk kwaadwillige of ongeoorloofde toegang tot de netwerk- en informatiesystemen van een portemonneeaanbieder, een aanbieder van in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde valideringsmechanismen, of een aanbieder van het stelsel voor elektronische identificatie op grond waarvan een portemonneeoplossing wordt verstrekt ("betrokken entiteiten") voorgedaan of die kan zich voordoen, op een wijze die ernstige operationele verstoringen kan veroorzaken, en die systemen zijn kritieke onderdelen van de getroffen portemonneeoplossing, van de in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde getroffen valideringsmechanismen of van het getroffen stelsel voor elektronische identificatie op grond waarvan een portemonneeoplossing is verstrekt;

c) een portemonneeoplossing, een in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoeld valideringsmechanisme of een stelsel voor elektronische identificatie op grond waarvan een portemonneeoplossing is verstrekt, of een deel daarvan:

— is meer dan 12 opeenvolgende uren volledig niet-beschikbaar of naar verwachting volledig niet-beschikbaar voor portemonneegebruikers of op portemonnees vertrouwende partijen;

— is meer dan 16 opeenvolgende uren per kalenderweek niet-beschikbaar of naar verwachting niet-beschikbaar voor portemonneegebruikers of op portemonnees vertrouwende partijen;

d) er is een vermoeden dat meer dan 1 % van de portemonneegebruikers of op portemonnees vertrouwende partijen gevolgen ondervindt of naar verwachting zal ondervinden van de beperkte beschikbaarheid van de portemonneeoplossing of van door betrokken entiteiten verleende diensten met betrekking tot de portemonneeoplossing;

e) er heeft zich een aantasting van de (tot betrouwbaar personeel van de betrokken entiteiten beperkte) fysieke toegang voorgedaan of die kan zich voordoen met betrekking tot een of meer locaties van de netwerk- en informatiesystemen die de portemonneeoplossing ondersteunen, van de verstrekking van de in artikel 5 bis, lid 8, van Verordening (EU) nr. 910/2014 bedoelde valideringsmechanismen in verband met een portemonnee-oplossing, of van het systeem voor elektronische identificatie op grond waarvan een portemonneeoplossing wordt verstrekt;

f) de privacy, de integriteit, de vertrouwelijkheid of de authenticiteit van in de portemonnee-oplossing opgeslagen, verzonden of verwerkte gegevens is op een of meer van de volgende manieren aangetast, of kan dat worden:

— er zijn gevolgen voor meer dan 1 % van de getroffen portemonneegebruikers of voor meer dan 100 000 van die portemonneegebruikers, afhankelijk van welk aantal het kleinste is;

— het is het gevolg van een succesvolle, vermoedelijk kwaadwillig activiteit;

— het is een gevolg of waarschijnlijk een gevolg van een of meer bekende kwetsbaarheden, met inbegrip van overeenkomstig Uitvoeringsverordening (EU) 2024/2981 van de Commissie behandelde kwetsbaarheden ([1]);

— het heeft waarschijnlijk gevolgen voor persoonsgegevens, op een wijze die een risico kan inhouden voor de rechten en vrijheden van de betrokken natuurlijke personen, en met name in geval van een inbreuk op persoonsgegevens in de zin van artikel 9, lid 1, en artikel 10 van Verordening (EU) 2016/679;

([1]) Uitvoeringsverordening (EU) 2024/2981 van de Commissie van 28 november 2024 tot vaststelling van uitvoeringsbepalingen voor Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad wat betreft de integriteit en de kernfunctionaliteiten van Europese portemonnees voor digitale identiteit (PB L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— het heeft waarschijnlijk gevolgen voor persoonlijke elektronische communicatie;

— het leidt waarschijnlijk tot een hoog risico voor de rechten en vrijheden van natuurlijke personen;

— het heeft waarschijnlijk gevolgen voor kwetsbare natuurlijke personen;

g) de certificering van de portemonneeoplossing is geannuleerd of zal naar verwachting worden geannuleerd;

h) de beveiligingsinbreuk of -aantasting heeft voor een betrokken entiteit direct financieel verlies veroorzaakt of kan verlies veroorzaken dat hoger is dan 500 000 EUR of, indien van toepassing, meer dan 5 % van de totale jaaromzet van de betrokken entiteit in het voorgaande boekjaar, indien dat lager is.

2. De lidstaten laten de geplande gevolgen van een door of namens de betrokken entiteiten uitgevoerd onderhoud buiten beschouwing, mits dat onderhoud:

a) van tevoren is aangekondigd aan mogelijk getroffen portemonneegebruikers, op portemonnees vertrouwende partijen en de bevoegde toezichthoudende organen;

b) niet aan een van de criteria van punt 1 voldoet.

3. Ten aanzien van lid 1, punt c), wordt de duur van een incident dat van invloed is op de beschikbaarheid gemeten vanaf het moment waarop de correcte verlening van de getroffen dienst wordt verstoord tot het moment waarop de dienst wordt hersteld en weer operationeel is. Wanneer een betrokken entiteit niet in staat is het tijdstip te bepalen waarop de verstoring begon, wordt de duur van het incident gemeten vanaf het moment waarop het incident werd ontdekt of vanaf het moment waarop het incident werd geregistreerd in netwerk- of systeemlogbestanden of andere gegevensbronnen, indien dat eerder is. De volledige niet-beschikbaarheid van een dienst wordt gemeten vanaf het moment waarop de dienst volledig niet-beschikbaar is voor gebruikers tot het moment waarop de reguliere werking of activiteiten zijn hersteld tot het serviceniveau dat vóór het incident werd verleend. Wanneer een betrokken entiteit niet in staat is te bepalen wanneer de volledige niet-beschikbaarheid van een dienst begon, wordt de niet-beschikbaarheid gemeten vanaf het moment dat dit door die entiteit werd gedetecteerd.

4. Ten aanzien van lid 1, punt d), wordt een dienst met name beperkt beschikbaar geacht indien een dienst aanzienlijk trager is dan de gemiddelde responstijd of indien niet alle functies van een dienst beschikbaar zijn. Waar mogelijk worden objectieve criteria op basis van de gemiddelde responstijden gebruikt om vertragingen in de responstijd te beoordelen.

5. Om de directe financiële verliezen als gevolg van een in lid 1, punt h), bedoelde inbreuk of aantasting te bepalen, houden de betrokken entiteiten rekening met alle financiële verliezen die zij als gevolg van het incident hebben geleden, zoals kosten voor de vervanging of verplaatsing van software, hardware of infrastructuur, personeelskosten, met inbegrip van kosten in verband met de vervanging of verplaatsing van personeel, de aanwerving van extra personeel, de vergoeding van overuren en het herstel van verloren of beperkte vaardigheden, vergoedingen wegens niet-naleving van contractuele verplichtingen, kosten voor schadeloosstelling en compensatie van klanten, verliezen als gevolg van gederfde inkomsten, kosten in verband met interne en externe communicatie, en advieskosten, met inbegrip van kosten in verband met juridisch advies, forensische diensten en hersteldiensten. Kosten in verband met de dagelijkse bedrijfsvoering, zoals kosten voor algemeen onderhoud van infrastructuur, apparatuur, hardware en software, verbeterings- en risicobeoordelingsinitiatieven, en verzekeringspremies, worden niet als financiële verliezen ten gevolge van een incident beschouwd. De betrokken entiteiten berekenen de bedragen van de financiële verliezen op basis van de beschikbare gegevens en wanneer de werkelijke bedragen van de financiële verliezen niet kunnen worden bepaald, ramen die entiteiten die bedragen.