REGULAMENTO DE EXECUÇÃO (UE) 2025/847 DA COMISSÃO

de 6 de maio de 2025

que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante às reações a violações da segurança das carteiras europeias de identidade digital

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE ([1]), nomeadamente o artigo 5.º-E, n.º 5,

Considerando o seguinte:

(1) O Regime Europeu para a Identidade Digital («regime»), instituído pelo Regulamento (UE) n.º 910/2014, é um componente crucial da criação de um ecossistema de identidade digital seguro e interoperável em toda a União. Tendo como pedra angular as carteiras europeias de identidade digital («carteiras»), o regime visa facilitar o acesso aos serviços em todos os Estados-Membros, assegurando simultaneamente a proteção dos dados pessoais e da privacidade.

(2) Os Regulamentos (UE) 2016/679 ([2]), (UE) 2018/1725 ([3]) do Parlamento Europeu e do Conselho e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([4]) aplicam-se às atividades de tratamento de dados pessoais ao abrigo do presente regulamento. As regras relativas à avaliação e prestação de informações estabelecidas ao abrigo do presente regulamento não prejudicam a obrigação de notificar as violações de dados pessoais à autoridade de controlo competente, se for caso disso, nos termos do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725, nem a obrigação de comunicar as violações de dados pessoais aos titulares dos dados, se for caso disso, por força dos mesmos regulamentos.

(3) A Comissão avalia periodicamente as novas tecnologias, práticas, normas e especificações técnicas. A fim de assegurar o mais elevado nível de harmonização entre os Estados-Membros para o desenvolvimento e a certificação das carteiras, as especificações técnicas estabelecidas no presente regulamento baseiam-se nos trabalhos realizados nos termos da Recomendação (UE) 2021/946 da Comissão ([5]) e, em especial, na arquitetura e no regime de referência que dela fazem parte. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([6]), a Comissão deve rever e, se necessário, atualizar o presente regulamento, para assegurar que o mesmo acompanha a evolução mundial e a arquitetura e o regime de referência, bem como para seguir as boas práticas no mercado interno.

([1]) JO L 257 de 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([3]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39, ELI: http://data. europa.eu/eli/reg/2018/1725/oj).

([4]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([5]) Recomendação (UE) 2021/946 da Comissão, de 3 de junho de 2021, relativa a um conjunto de instrumentos comuns a nível da União para uma abordagem coordenada do quadro europeu para a identidade digital (JO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([6]) Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho, de 11 de abril de 2024, que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação do Regime Europeu para a Identidade Digital (JO L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

(4) Em caso de violação ou comprometimento da segurança das soluções de carteiras ou dos mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014, ou do sistema de identificação eletrónica ao abrigo do qual as soluções de carteiras são fornecidas, as reações a essas violações e comprometimentos da segurança têm de ocorrer de forma rápida, coordenada e segura em todos os Estados-Membros, a fim de proteger os utentes e de preservar a confiança no ecossistema de identidade digital. O que precede não prejudica o disposto na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([7]) e nos Regulamentos (UE) 2019/881 ([8]) e (UE) 2024/2847 ([9]) do Parlamento Europeu e do Conselho, em particular no que respeita ao tratamento de incidentes ou vulnerabilidades e a sua classificação como violações da segurança. Por conseguinte, os Estados-Membros devem garantir a suspensão atempada do fornecimento e da utilização das carteiras afetadas por uma violação ou um comprometimento da segurança ou, se for caso disso, a sua retirada.

(5) A fim de garantir reações adequadas a uma violação ou comprometimento da segurança, os Estados-Membros devem avaliar se uma violação ou comprometimento da segurança de uma solução de carteira, dos mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014, ou do sistema de identificação eletrónica ao abrigo do qual é fornecida uma solução de carteira afeta a fiabilidade dessa solução de carteira ou das demais soluções de carteiras. Essa avaliação deve basear-se em critérios uniformes, como o número e a categoria dos utentes das carteiras, das pessoas singulares e dos utilizadores de carteiras afetados, a natureza dos dados afetados, a duração do comprometimento ou da violação da segurança, a disponibilidade limitada de um serviço e as perdas financeiras, bem como o potencial comprometimento de dados pessoais. Estes critérios devem dar aos Estados-Membros flexibilidade e poder discricionário para determinar de forma proporcionada se a fiabilidade de uma solução de carteira é afetada e se a suspensão ou, se a gravidade da violação ou do comprometimento o justificar, a retirada da solução da carteira é adequada. Estes critérios não devem desencadear a retirada automática de uma solução de carteira ou a suspensão automática do fornecimento e da utilização de uma solução de carteira, mas devem ser devidamente ponderados pelos Estados-Membros ao decidirem se é necessário retirar ou suspender o fornecimento e a utilização de uma solução de carteira.

(6) Devido ao impacto e aos inconvenientes causados pela suspensão da utilização de soluções de carteiras, os Estados-Membros terão de avaliar se a revogação dos certificados de unidades de carteira ou quaisquer outras medidas adicionais são necessárias para reagir adequadamente à violação ou ao comprometimento da segurança.

(7) Para manter os utentes de carteiras informados sobre o estado das suas carteiras, estes devem receber informações adequadas sobre violações ou comprometimentos da segurança que as afetem. Uma vez que os utilizadores de carteiras registados na União também podem ser afetados por violações e comprometimentos da segurança, as informações pertinentes sobre violações e comprometimentos da segurança também devem ser partilhadas com eles.

(8) Para reforçar a transparência e a confiança no ecossistema de identidade digital, as informações sobre as violações ou os comprometimentos da segurança e sobre as suas consequências devem, no mínimo, incluir as informações exigidas por força do presente regulamento. As informações relativas a violações ou comprometimentos da segurança partilhadas com utentes e utilizadores de carteiras devem, no entanto, ser cuidadosamente avaliadas, para prevenir e minimizar o risco de serem exploradas por atacantes.

([7]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80, ELI: https://data.europa.eu/eli/dir/2022/2555/oj).

([8]) Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Para permitir que os utentes voltem a aceder às suas unidades de carteira depois de uma violação ou um comprometimento da segurança ter sido sanado, o Estado-Membro que forneceu as soluções de carteiras terá de restabelecer o fornecimento e a utilização dessas soluções de carteiras sem demora injustificada. Pode fazê-lo restabelecendo as unidades da carteira, emitindo unidades de carteira fornecidas ao abrigo da nova versão das soluções de carteiras ou reemitindo novos certificados de unidades de carteira válidos. Os utentes de carteiras afetados, os utilizadores de carteiras, os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014 e a Comissão devem ser informados em conformidade.

(10) Para garantir a retirada das carteiras sempre que uma violação ou comprometimento da segurança não tenha sido sanado no prazo de três meses a contar da suspensão ou sempre que a gravidade da violação ou do comprometimento da segurança o justifique, o Estado-Membro deve garantir que os certificados de unidades de carteira pertinentes sejam revogados, que o seu estado de validade não possa ser restaurado, e que não possam ser emitidos ou fornecidos a unidades de carteira existentes. Além disso, não devem ser fornecidas novas unidades de carteira ao abrigo da solução de carteira afetada. Para efeitos de transparência, os utentes, os utilizadores, os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014 e a Comissão têm de ser informados da retirada. Esta informação inclui uma descrição dos potenciais impactos nos utentes das carteiras e, nomeadamente, na gestão dos certificados emitidos, ou nos utilizadores das carteiras.

(11) O período de três meses a contar da suspensão do fornecimento e da utilização de uma solução de carteira, e durante o qual deve ser sanada a violação ou comprometimento da segurança conducente a essa suspensão, deve constituir o prazo após o qual a solução de carteira deve ser retirada a menos que tenha sido aplicada uma medida corretiva adequada. No entanto, os Estados-Membros são livres de exigir que a violação ou o comprometimento da segurança sejam sanados num prazo inferior a três meses, tendo em conta, em particular e se for caso disso, a extensão, a duração e as consequências dessa violação ou comprometimento da segurança. Se a violação ou o comprometimento da segurança não forem ou não puderem ser sanados no prazo fixado pelo Estado-Membro, este pode exigir que a solução de carteira seja retirada antes do termo do período de três meses. Os Estados-Membros devem usar o prazo durante o qual a violação ou comprometimento da segurança conducente à suspensão do fornecimento e da utilização de uma solução de carteira têm de ser sanados para preparar a possível retirada dessa solução de carteira e as comunicações conexas.

(12) A fim de reduzir os encargos administrativos para os Estados-Membros no que diz respeito às informações a prestar, em conformidade com o presente regulamento, à Comissão e a outros Estados-Membros, os Estados-Membros devem utilizar os instrumentos de notificação existentes, como o Sistema de Comunicação e Análise de Incidentes de Cibersegurança (CIRAS) gerido pela Agência da União Europeia para a Cibersegurança (ENISA). No que diz respeito aos canais ou meios alternativos a utilizar para informar os utentes de carteiras afetados por uma violação ou comprometimento da segurança e os utilizadores das carteiras, os Estados-Membros devem garantir que as informações pertinentes são prestadas de forma clara, exaustiva e facilmente acessível. Os canais previstos para a prestação dessas informações aos utentes de carteiras afetados e aos utilizadores de carteiras devem incluir soluções adequadas para a difusão Web, o seguimento em tempo real das atualizações dos sítios Web e a agregação de notícias.

(13) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 e emitiu parecer em 31 de janeiro de 2025.

(14) As medidas previstas no presente regulamento estão em conformidade com o parecer do comité instituído pelo artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento estabelece regras relativas às reações a violações da segurança das carteiras, dos mecanismos de validação referidos no artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014 e do sistema de identificação eletrónica ao abrigo do qual as carteiras são fornecidas.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Solução de carteira», uma combinação de *software*, *hardware*, serviços, definições e configurações, incluindo instâncias de carteiras, uma ou várias aplicações criptográficas seguras de carteiras e um ou vários dispositivos criptográficos seguros de carteiras;

2) «Utente da carteira», um utente que controla a unidade de carteira;

3) «Utilizador de carteira», um utilizador que tenciona recorrer a unidades de carteira para a prestação de serviços públicos ou privados por meio de interação digital;

4) «Instância de carteira», a aplicação instalada e configurada no dispositivo ou ambiente do utente de uma carteira, que faz parte de uma unidade de carteira e que o utente da carteira utiliza para interagir com a unidade de carteira;

5) «Aplicação criptográfica segura de carteiras», uma aplicação que gere ativos críticos através da ligação e da utilização das funções criptográficas e não criptográficas disponibilizadas pelo dispositivo criptográfico seguro de carteiras;

6) «Dispositivo criptográfico seguro de carteiras», um dispositivo inviolável que disponibiliza um ambiente ligado à aplicação criptográfica segura de carteiras e que esta utiliza para proteger ativos críticos e assegurar funções criptográficas para a execução segura de operações críticas;

7) «Fornecedor de carteiras», uma pessoa singular ou coletiva que disponibiliza soluções de carteiras;

8) «Unidade de carteira», uma configuração única de uma solução de carteira que inclui instâncias de carteiras, aplicações criptográficas seguras de carteiras e dispositivos criptográficos seguros de carteiras disponibilizada pelo fornecedor de uma carteira a um utente individual da carteira;

9) «Ativos críticos», ativos dentro de uma unidade de carteira ou relacionados com a mesma, que se revestem de uma importância de tal forma extraordinária que o comprometimento da sua disponibilidade, confidencialidade ou integridade teria um efeito debilitante muito grave na capacidade de recorrer à unidade de carteira;

10) «Certificado de unidade de carteira», um objeto de dados que descreve os componentes da unidade de carteira ou permite a autenticação e validação desses componentes.

Artigo 3.º

Determinação da existência de uma violação ou comprometimento da segurança

1. Sem prejuízo do disposto na Diretiva (UE) 2022/2555 e nos Regulamentos (UE) 2019/881 e (UE) 2024/2847, os Estados-Membros devem ter devidamente em conta os critérios estabelecidos no anexo I do presente regulamento para avaliar se uma violação ou comprometimento da segurança de uma solução de carteira, dos mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014, ou do sistema de identificação eletrónica ao abrigo do qual a solução de carteira é fornecida, está a afetar a sua fiabilidade ou a fiabilidade das demais soluções de carteiras.

2. Se um Estado-Membro determinar, com base na avaliação prevista no n.º 1, que uma violação ou um comprometimento da segurança está a afetar a fiabilidade de uma solução de carteira e suspender o fornecimento e a utilização dessa solução de carteira, deve tomar as medidas previstas nos artigos 4.º e 5.º. Se um Estado-Membro retirar a solução de carteira, deve tomar as medidas previstas nos artigos 8.º e 9.º.

3. Sempre que um Estado-Membro tome conhecimento de informações relativas a uma eventual violação ou comprometimento da segurança que possa afetar a fiabilidade de uma ou mais soluções de carteiras fornecidas por outro Estado-Membro, esse Estado-Membro deve comunicar esse facto, sem demora injustificada, à Comissão e aos pontos de contacto único dos Estados-Membros afetados designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014. A comunicação deve incluir as informações a que se refere o artigo 5.º, n.º 2.

4. O Estado-Membro que recebe informações prestadas nos termos do n.º 3 deve tomar as medidas previstas nos n.ºs 1 e 2 sem demora injustificada.

Artigo 4.º

Suspensão do fornecimento e da utilização de carteiras e outras medidas corretivas

1. Os Estados-Membros devem assegurar que não são fornecidas, utilizadas nem ativadas unidades de carteira ao abrigo da solução de carteira suspensa.

2. Os Estados-Membros devem avaliar se é necessário revogar certificados de unidades de carteira das unidades de carteira afetadas pela suspensão de uma solução de carteira, ou aplicar qualquer outra medida corretiva adicional, para reagir adequadamente à violação ou comprometimento da segurança.

3. As medidas previstas nos n.ºs 1 e 2 devem ser tomadas sem demora injustificada e, em qualquer caso, o mais tardar 24 horas após a suspensão do fornecimento e da utilização da solução de carteira afetada pela violação ou comprometimento da segurança.

4. As medidas previstas nos n.ºs 1 e 2 não devem impedir os utentes de carteiras afetados de exercerem o seu direito à portabilidade dos dados previsto no artigo 5.º-A, n.º 4, alínea g), do Regulamento (UE) n.º 910/2014. Esta disposição está sujeita à condição de os utentes de carteiras poderem exercer o direito sem comprometer a segurança dos ativos críticos das unidades de carteira afetadas, tendo em conta, nomeadamente, os motivos da suspensão e a necessidade de assegurar a proteção eficaz desses ativos contra a utilização abusiva.

Artigo 5.º

Informações sobre suspensões e medidas corretivas

1. Devem ser prestadas informações sobre a suspensão do fornecimento e da utilização de uma solução de carteira de forma clara, exaustiva e facilmente acessível, sem demora injustificada e o mais tardar 24 horas após a suspensão do fornecimento e da utilização da solução de carteira:

a) Aos pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014;

b) À Comissão;

c) Aos utentes de carteiras afetados;

d) Aos utilizadores de carteiras registados em conformidade com o artigo 5.º-B do Regulamento (UE) n.º 910/2014.

2. As informações prestadas em conformidade com o n.º 1 devem incluir, pelo menos, os seguintes elementos:

a) O nome do fornecedor da solução de carteira cujo fornecimento e utilização foram suspensos;

b) O nome e o identificador de referência dessa solução de carteira, tal como consta da lista de carteiras certificadas elaborada nos termos do artigo 5.º-D do Regulamento (UE) n.º 910/2014 e, se for caso disso, as versões em causa;

c) A data e a hora em que foi detetada a violação ou o comprometimento da segurança;

d) Se conhecida, a data e a hora em que a violação ou o comprometimento da segurança se tornou efetivo, com base nos registos da rede ou do sistema ou noutras fontes de dados;

e) A data e a hora da suspensão da solução de carteira;

f) Dados de contacto, incluindo, pelo menos, um endereço de correio eletrónico e um número de telefone do Estado-Membro notificante e, se diferentes, do fornecedor de carteiras a que se refere a alínea a);

g) Uma descrição da violação ou do comprometimento da segurança;

h) Uma descrição dos dados comprometidos, incluindo, se for caso disso, as categorias de dados pessoais, conforme definidas no artigo 9.º, n.º 1, e no artigo 10.º do Regulamento (UE) 2016/679;

i) Sempre que possível, uma estimativa do número aproximado de utentes de carteiras afetados e de outras pessoas singulares afetadas;

j) Uma descrição dos potenciais impactos nos utilizadores de carteiras ou nos utentes de carteiras e, neste último caso, se pertinente, a indicação de medidas que os utentes de carteiras podem tomar para os atenuar;

k) Uma descrição das medidas tomadas ou planeadas para sanar a violação ou o comprometimento da segurança, juntamente com um plano e um prazo para essa correção;

l) Se aplicável e adequado, uma descrição das medidas tomadas ou planeadas para transitar os utentes de carteiras afetados para soluções ou serviços de carteira alternativos.

Artigo 6.º

Restabelecimento do fornecimento e da utilização de carteiras

Sempre que necessário para assegurar o restabelecimento do fornecimento, a ativação e a utilização de uma solução de carteira, os Estados-Membros devem, sem demora injustificada:

1) Restabelecer o fornecimento e a utilização das unidades de carteira fornecidas ao abrigo dessa solução de carteira, emitindo uma unidade de carteira fornecida ao abrigo de uma nova versão da solução de carteira para todos os utentes afetados;

2) Emitir novos certificados de unidades de carteira para novas unidades de carteira ou, se for caso disso, para unidades de carteira emitidas anteriormente, desde que essas unidades de carteira cumpram os requisitos de segurança em vigor após a violação ou o comprometimento da segurança terem sido sanados;

3) Revogar qualquer medida aplicada nos termos do artigo 4.º que impeça o fornecimento de novas unidades de carteira ao abrigo da solução de carteira afetada, se essa medida estiver relacionada apenas com a violação ou o comprometimento da segurança já sanado.

Artigo 7.º

Informações sobre o restabelecimento

Se um Estado-Membro restabelecer uma solução de carteira, deve assegurar que:

1) São informadas desse facto, sem demora injustificada, todas as partes que tenham recebido informações sobre a suspensão do fornecimento e da utilização dessa solução de carteira nos termos do artigo 5.º, n.º 1.

2) As informações prestadas em conformidade com o ponto 1 incluem, pelo menos, os elementos referidos no artigo 5.º, n.º 2, alíneas a), b) e f) a h), bem como os seguintes elementos:

   a) A data e a hora em que foi sanada a violação ou o comprometimento da segurança;

   b) A data e a hora do restabelecimento da solução de carteira afetada e, se for caso disso, das unidades de carteira afetadas fornecidas ao abrigo dessa solução de carteira;

   c) Uma descrição das medidas tomadas para sanar a violação ou o comprometimento da segurança;

   d) Uma descrição dos potenciais impactos residuais nos utilizadores de carteiras ou nos utentes de carteiras e, neste último caso, se pertinente, a indicação de medidas que os utentes de carteiras podem tomar para os atenuar.

Artigo 8.º

Retirada de carteiras

1. Se uma violação ou um comprometimento da segurança conducente à suspensão do fornecimento e da utilização de uma solução de carteira não forem sanados no prazo de três meses a contar da data de suspensão do fornecimento e da utilização dessa solução de carteira, o Estado-Membro que fornece essa solução de carteira deve garantir que a solução de carteira afetada é retirada e que a sua validade é revogada, sem demora injustificada e, em todo o caso, no prazo de 72 horas após o termo do prazo de três meses.

2. Se um Estado-Membro retirar uma solução de carteira deve assegurar que:

a) Os certificados de unidades de carteira da unidade de carteira da solução de carteira afetada são revogados;

b) Não é possível restaurar o estado de validade dos certificados de unidades de carteira;

c) Não pode ser emitido um novo certificado de unidade de carteira para unidades de carteira existentes fornecidas ao abrigo da solução de carteira afetada;

d) Não podem ser fornecidas novas unidades de carteira ao abrigo da solução de carteira afetada.

3. As medidas previstas nos n.os 1 e 2 não devem impedir os utentes de carteiras afetados de exercerem o seu direito à portabilidade dos dados previsto no artigo 5.º-A, n.º 4, alínea g), do Regulamento (UE) n.º 910/2014. Esta disposição está sujeita à condição de os utentes de carteiras poderem exercer o direito sem comprometer a segurança dos ativos críticos das unidades de carteira afetadas, tendo em conta, nomeadamente, os motivos da retirada e a necessidade de assegurar a proteção eficaz desses ativos contra a utilização abusiva.

Artigo 9.º

Informações sobre a retirada

1. Devem ser prestadas informações sobre a retirada de uma solução de carteira de forma clara, exaustiva e facilmente acessível, sem demora injustificada e o mais tardar 24 horas após a retirada da solução de carteira:

a) Aos pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014;

b) À Comissão;

c) Aos utentes de carteiras afetados;

d) Aos utilizadores de carteiras registados em conformidade com o artigo 5.º-B do Regulamento (UE) n.º 910/2014.

2. As informações prestadas em conformidade com o n.º 1 devem incluir, pelo menos, os seguintes elementos:

a) O nome do fornecedor da solução de carteira retirada;

b) O nome e o identificador de referência dessa solução de carteira, tal como consta da lista de carteiras certificadas elaborada nos termos do artigo 5.º-D do Regulamento (UE) n.º 910/2014 e, se for caso disso, as versões em causa;

c) A data e a hora da deteção da violação ou do comprometimento da segurança que, devido à sua gravidade ou ao facto de não ter sido sanado no prazo de três meses, levou à retirada da solução de carteira afetada;

d) Se conhecida, a data e a hora em que a violação ou o comprometimento da segurança se tornou efetivo, com base nos registos da rede ou do sistema ou noutras fontes de dados;

e) A data e a hora da retirada da solução de carteira e da revogação efetiva dos certificados de unidades de carteira das unidades de carteira fornecidas ao abrigo da solução de carteira;

f) Se a retirada resulta da gravidade da violação ou do comprometimento da segurança ou se é consequência da não correção da violação ou do comprometimento da segurança;

g) Dados de contacto, incluindo, pelo menos, um endereço de correio eletrónico e um número de telefone do Estado-Membro notificante e, se diferentes, do fornecedor de carteiras a que se refere a alínea a);

h) Uma descrição da violação ou do comprometimento da segurança;

i) Uma descrição dos dados comprometidos, incluindo, se for caso disso, as categorias de dados pessoais, conforme especificadas no artigo 9.º, n.º 1, e no artigo 10.º do Regulamento (UE) 2016/679;

j) Sempre que possível, uma estimativa do número aproximado de utentes de carteiras afetados e de outras pessoas singulares afetadas;

k) Uma descrição dos potenciais impactos nos utilizadores de carteiras ou nos utentes de carteiras e, neste último caso, se pertinente, a indicação de medidas que os utentes de carteiras podem tomar para os atenuar;

l) Uma descrição das medidas tomadas ou planeadas para transitar os utentes de carteiras afetados para soluções de carteiras alternativas ou, se aplicável e adequado, serviços alternativos.

Artigo 10.º

Sistema de informação

Os Estados-Membros devem enviar as informações previstas nos artigos 3.º, 5.°, 7.° e 9.° à Comissão e aos pontos de contacto único dos Estados-Membros designados nos termos do artigo 46.º-C, n.º 1, do Regulamento (UE) n.º 910/2014, através do CIRAS gerido pela ENISA ou de um sistema equivalente acordado pelos Estados-Membros e pela Comissão.

Artigo 11.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros, com exceção do artigo 10.º, que é aplicável a partir de 7 de maio de 2026.

Feito em Bruxelas, em 6 de maio de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

Critérios para a avaliação de uma violação ou comprometimento da segurança

1. Os Estados-Membros devem basear a sua avaliação de uma violação ou comprometimento da segurança nos seguintes critérios:

   a) A violação ou comprometimento causou ou pode causar a morte de uma pessoa singular ou danos consideráveis à saúde de uma pessoa singular;

   b) Ocorreu ou pode ocorrer um acesso bem-sucedido, presumivelmente malicioso ou não autorizado aos sistemas de rede e informação de um fornecedor de carteiras, de um fornecedor de mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014, ou de um fornecedor do sistema de identificação eletrónica ao abrigo do qual é fornecida uma solução de carteira («entidades em causa»), passível de causar graves perturbações operacionais, e esses sistemas são componentes críticos da solução de carteira afetada, dos mecanismos de validação afetados a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014 ou do sistema de identificação eletrónica afetado ao abrigo do qual é fornecida uma solução de carteira;

   c) Uma solução de carteira, um mecanismo de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014, ou um sistema de identificação eletrónica ao abrigo do qual é fornecida uma solução de carteira, ou parte deles:

      — está totalmente indisponível, ou prevê-se que esteja totalmente indisponível, para os utentes ou utilizadores de carteiras, durante mais de 12 horas consecutivas,

      — está indisponível, ou prevê-se que esteja indisponível, para os utentes ou utilizadores de carteiras, durante mais de 16 horas calculadas de acordo com uma semana de calendário;

   d) Suspeita-se que mais de 1 % dos utentes ou utilizadores de carteiras sejam afetados, ou prevê-se que sejam afetados, pela disponibilidade limitada da solução de carteira, ou dos serviços prestados pelas entidades em causa no que diz respeito à solução da carteira;

   e) Existe uma capacidade de comprometimento ou houve um comprometimento do acesso físico restrito ao pessoal de confiança das entidades em causa, ou da proteção do acesso físico, a um ou mais locais dos sistemas de rede e informação que apoiam a solução da carteira, a disponibilização dos mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, do Regulamento (UE) n.º 910/2014 associados a uma solução de carteira, ou o sistema de identificação eletrónica ao abrigo do qual é fornecida uma solução de carteira;

   f) A privacidade, a integridade, a confidencialidade ou a autenticidade dos dados armazenados, transmitidos ou tratados na solução da carteira foi comprometida, ou pode ser comprometida, de uma ou mais das seguintes formas:

      — com impacto em mais de 1 % dos utentes de carteiras da solução de carteira afetada ou em mais de 100 000 desses utentes, consoante o número que for menor,

      — é o resultado de uma atividade presumivelmente maliciosa bem-sucedida,

      — é o resultado ou é suscetível de ser o resultado de uma ou mais vulnerabilidades conhecidas, incluindo as tratadas em conformidade com o Regulamento de Execução (UE) 2024/2981 da Comissão ([1]),

      — é suscetível de afetar dados pessoais de uma forma passível de resultar num risco para os direitos e liberdades das pessoas singulares em causa e, em particular, em caso de violação de dados pessoais na aceção do artigo 9.º, n.º 1, e do artigo 10.º do Regulamento (UE) 2016/679,

([1]) Regulamento de Execução (UE) 2024/2981 da Comissão, de 28 de novembro de 2024, que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante à certificação das carteiras europeias de identidade digital (JO L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— é suscetível de afetar as comunicações eletrónicas pessoais,

— é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares,

— é suscetível de afetar pessoas singulares vulneráveis;

g) A certificação da solução de carteira foi cancelada ou prevê-se que seja cancelada;

h) A violação ou o comprometimento causou ou é suscetível de causar a uma entidade em causa perdas financeiras diretas superiores a 500 000 EUR ou, se for caso disso, a 5 % do seu volume de negócios anual total ao longo do exercício financeiro anterior, consoante o que for mais baixo.

2. Os Estados-Membros não devem ter em conta as consequências previstas de uma operação de manutenção realizada pelas entidades em causa ou em seu nome, desde que essa operação de manutenção:

a) Tenha sido previamente notificada aos utentes de carteiras potencialmente afetados, aos utilizadores de carteiras e às entidades supervisoras competentes;

b) Não satisfaça nenhum dos critérios estabelecidos no n.º 1 do presente anexo.

3. No que diz respeito ao n.º 1, alínea c), a duração de um incidente que afete a disponibilidade deve ser medida a partir do momento em que a prestação adequada do serviço afetado é perturbada até ao momento em que o serviço é restabelecido e fica novamente operacional. Se uma entidade em causa for incapaz de determinar o momento em que a perturbação teve início, a duração do incidente deve ser medida a partir do momento em que o incidente foi detetado, ou a partir do momento em que o incidente foi registado nos registos da rede ou do sistema ou noutras fontes de dados, consoante o que ocorrer primeiro. A indisponibilidade total de um serviço deve ser medida desde o momento em que o serviço fica totalmente indisponível para os utentes até ao momento em que é restabelecido, no que toca às atividades ou operações regulares, o nível de serviço prestado antes do incidente. Se uma entidade em causa for incapaz de determinar em que momento teve início a indisponibilidade total de um serviço, a indisponibilidade deve ser medida a partir do momento em que foi detetada por essa entidade.

4. No que diz respeito ao n.º 1, alínea d), considera-se que existe uma disponibilidade limitada de um serviço, nomeadamente, quando o tempo de resposta de um serviço é consideravelmente superior à média ou quando não estejam disponíveis todas as funcionalidades do serviço em questão. Sempre que possível, com vista a avaliar os atrasos no tempo de resposta, devem ser utilizados critérios objetivos baseados nos tempos médios de resposta dos serviços.

5. Para determinar as perdas financeiras diretas resultantes de uma violação ou um comprometimento a que se refere o n.º 1, alínea h), as entidades em causa devem ter em conta todas as perdas financeiras em que incorreram em resultado do incidente, tais como os custos de substituição ou relocalização de *software*, *hardware* ou infraestruturas, os custos com pessoal, incluindo os custos associados à substituição ou relocalização do pessoal, ao recrutamento de pessoal suplementar, à remuneração de horas extraordinárias e ao restabelecimento de competências perdidas ou comprometidas, as taxas por incumprimento de obrigações contratuais, os custos de reparação e indemnização dos clientes, os prejuízos causados pela perda de receitas, os custos associados à comunicação interna e externa, os custos de consultoria, incluindo custos associados a aconselhamento jurídico, a serviços forenses e a serviços de recurso. Os custos necessários para o funcionamento corrente da empresa, incluindo os custos de manutenção geral de infraestruturas, equipamentos, *hardware* e *software*, melhorias e iniciativas de avaliação dos riscos e prémios de seguros, não devem ser considerados perdas financeiras resultantes de um incidente. As entidades em causa devem calcular os montantes das perdas financeiras com base nos dados disponíveis e, caso não seja possível determinar os montantes reais das perdas financeiras, devem estimar esses montantes.