2024/2982

4.12.2024

REGULAMENTO DE EXECUÇÃO (UE) 2024/2982 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 aos protocolos e às interfaces que devem ser suportados pelo Regime Europeu para a 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-A, n.º 23,

Considerando o seguinte:

(1) O Regime Europeu para a Identidade Digital, instituído pelo Regulamento (UE) n.º 910/2014, é uma 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 das pessoas singulares e coletivas aos serviços em todos os Estados-Membros, assegurando simultaneamente a proteção dos dados pessoais e da privacidade.

(2) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]) e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([3]) aplicam-se a todas as atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

(3) O artigo 5.º-A, n.º 23, do Regulamento (UE) n.º 910/2014 incumbe a Comissão, se necessário, de estabelecer as especificações e os procedimentos pertinentes. Tal é alcançado através de quatro regulamentos de execução, que abordam os protocolos e as interfaces: Regulamento de Execução (UE) 2024/2982 da Comissão ([4]), a integridade e as funcionalidades essenciais: Regulamento de Execução (UE) 2024/2979 da Comissão ([5]), os dados de identificação pessoal e os certificados eletrónicos de atributos: Regulamento de Execução (UE) 2024/2977 da Comissão ([6]), bem como as notificações à Comissão: Regulamento de Execução (UE) 2024/2980 da Comissão ([7]). O presente regulamento estabelece os requisitos pertinentes para os protocolos e as interfaces.

([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]) 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).

([4]) Regulamento de Execução (UE) 2024/2982 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 aos protocolos e às interfaces que devem ser suportados pelo Regime Europeu para a Identidade Digital (JO L, 2024/2982, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2982/oj).

([5]) Regulamento de Execução (UE) 2024/2979 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 integridade e às funcionalidades essenciais das carteiras europeias de identidade digital (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

([6]) Regulamento de Execução (UE) 2024/2977 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 aos dados de identificação pessoal e aos certificados eletrónicos de atributos emitidos para carteiras europeias de identidade digital (JO L, 2024/2977, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2977/oj).

([7]) Regulamento de Execução (UE) 2024/2980 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 às notificações à Comissão relativas ao ecossistema da carteira europeia de identidade digital (JO L, 2024/2980, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2980/oj).

(4) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou 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 com base na 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 ([8]) e, em especial, na arquitetura e no quadro de referência. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([9]), a Comissão deve rever e atualizar o presente regulamento de execução, se necessário, a fim de assegurar que o mesmo acompanha a evolução mundial, a arquitetura e o regime de referência e de seguir as boas práticas no mercado interno.

(5) A fim de assegurar a transparência e a fiabilidade dos utilizadores de carteiras face aos utentes das carteiras, os protocolos e as interfaces utilizados pelas soluções de carteiras devem proporcionar aos utentes de carteiras um mecanismo fiável para autenticar os utilizadores de carteiras e outras unidades de carteira. Inversamente, os fornecedores de carteiras devem disponibilizar um mecanismo para autenticar e validar unidades de carteira, de modo que os utilizadores possam receber garantias no que diz respeito à fiabilidade e autenticidade das unidades de carteira. Além disso, a infraestrutura técnica das carteiras deve também ser concebida de modo a assegurar a transferência apenas da quantidade mínima de dados necessária unicamente para os utilizadores autorizados, mantendo simultaneamente a ausência de associação entre as diferentes transações. A fim de facilitar a emissão de dados de identificação pessoal e de certificados eletrónicos de atributos, todas as soluções de carteiras devem suportar um conjunto mínimo de protocolos e interfaces.

(6) A fim de assegurar a facilidade de utilização das soluções de carteiras em todos os Estados-Membros, todas as soluções de carteiras devem suportar a aplicação das especificações técnicas comuns quando os dados de identificação pessoal e os certificados eletrónicos de atributos são apresentados a utilizadores através das carteiras, tanto em cenários à distância como de proximidade. Além disso, as unidades de carteira podem suportar outros protocolos e interfaces para casos de utilização específicos.

(7) A fim de assegurar a proteção de dados desde a conceção e por defeito, as carteiras devem dispor de várias funcionalidades de reforço da privacidade, de modo a impedir que os fornecedores de meios de identificação eletrónica e de certificados eletrónicos de atributos combinem dados pessoais obtidos aquando da prestação de outros serviços com os dados pessoais tratados para prestar os serviços abrangidos pelo âmbito de aplicação do Regulamento (UE) n.º 910/2014. Conforme estabelecido no Regulamento (UE) n.º 910/2014, os utilizadores não devem solicitar aos utentes que facultem quaisquer dados para além dos indicados durante o processo de registo para a utilização prevista das carteiras. Os utentes das carteiras devem poder verificar os dados de registo dos utilizadores a qualquer momento. Além disso, as unidades de carteira devem poder apresentar certificados de registo de utilizador de carteira aos utentes, quando disponíveis, no âmbito de um pedido de atributos. Tal deverá permitir aos utentes da carteira verificar se os atributos solicitados pelo utilizador de carteira estão abrangidos pelo âmbito dos atributos por este registados, dando garantias de que o pedido é legítimo e fiável.

(8) A fim de proteger os dados dos utentes das carteiras, os fornecedores de carteiras devem assegurar que as unidades de carteira validam os pedidos dos utilizadores de carteiras ou de outras unidades de carteira antes de disponibilizarem quaisquer dados. Pela mesma razão e em conformidade com o artigo 5.º-A, n.º 4, alínea d), subalínea ii), do Regulamento (UE) n.º 910/2014, os fornecedores de carteiras devem assegurar que as unidades de carteira permitem aos utentes das carteiras apresentarem pedidos de apagamento de dados aos utilizadores de carteiras.

(9) A fim de permitir reações rápidas em caso de preocupações em matéria de proteção de dados relacionadas com o artigo 5.º-A, n.º 4, alínea d), subalínea iii), do Regulamento (UE) n.º 910/2014, os fornecedores de carteiras devem assegurar que as soluções de carteiras proporcionam mecanismos de comunicação de um utilizador à autoridade nacional responsável pela proteção de dados. Os fornecedores de carteiras e as autoridades de proteção de dados devem dispor de flexibilidade adequada na criação de mecanismos adequados para interagir com as autoridades de proteção de dados dos Estados-Membros.

(10) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([10]) e emitiu o seu parecer em 30 de setembro de 2024.

([8]) JO L 210 de 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj.

([9]) 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).

([10]) 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).

(11) As medidas previstas no presente regulamento estão em conformidade com o parecer do Comité referido no artigo 48.º do Regulamento (UE) n.º 910/2014,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto e âmbito de aplicação

O presente regulamento estabelece regras relativas aos protocolos e interfaces das soluções de carteiras para:

1) A emissão de dados de identificação pessoal e certificados eletrónicos de atributos para unidades de carteira;

2) A apresentação de atributos de dados de identificação pessoal e certificados eletrónicos de atributos aos utilizadores de carteiras e a outras unidades de carteira;

3) A comunicação de pedidos de apagamento de dados aos utilizadores de carteiras;

4) A comunicação de utilizadores de carteiras às autoridades de controlo estabelecidas nos termos do artigo 51.º do Regulamento (UE) 2016/679;

a atualizar periodicamente, a fim de acompanhar a evolução da tecnologia e das normas, bem como os trabalhos realizados com base na Recomendação (UE) 2021/946, em especial a arquitetura e o quadro de referência.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «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;

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

3) «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;

4) «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;

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

6) «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;

7) «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;

8) «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;

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 acesso de utilizador de carteira», um certificado de assinaturas ou selos eletrónicos que autenticam e validam o utilizador de carteira, emitido por um fornecedor de certificados de acesso de utilizadores de carteiras;

11) «Fornecedor de certificados de acesso de utilizadores de carteiras», uma pessoa singular ou coletiva mandatada por um Estado-Membro para emitir certificados de acesso de utilizadores de carteiras a utilizadores de carteiras registados nesse Estado-Membro;

12) «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;

13) «Política de divulgação incorporada», um conjunto de regras, incorporadas num certificado eletrónico de atributos pelo seu fornecedor, que indicam as condições que um utilizador de carteira tem de cumprir para aceder ao certificado eletrónico de atributos;

14) «Certificado de registo de utilizador de carteira», um objeto de dados que indica os atributos que o utilizador registou tendo em vista a sua solicitação aos utentes;

15) «Fornecedor de dados de identificação pessoal», uma pessoa singular ou coletiva responsável pela emissão e revogação dos dados de identificação pessoal e pela garantia de que os dados de identificação pessoal de um utente estão criptograficamente vinculados a uma unidade de carteira;

16) «Vinculação criptográfica», o método para associar dados de identificação pessoal ou certificados eletrónicos de atributos a unidades de carteira por meios criptográficos.

Artigo 3.º

Disposições gerais

No que diz respeito aos protocolos e interfaces a que se referem os artigos 4.º e 5.°, os fornecedores de carteiras devem assegurar que as unidades de carteira:

1) Autenticam e validam os certificados de acesso de utilizadores de carteiras caso interajam com utilizadores de carteiras;

2) Autenticam e validam os certificados de unidades de carteira de outras unidades de carteira caso interajam com outras unidades de carteira;

3) Autenticam e validam os pedidos apresentados utilizando certificados de acesso de utilizadores de carteiras ou certificados de unidades de carteira de outras unidades de carteira, se for caso disso;

4) Autenticam e validam o certificado de registo de utilizador de carteira, se for caso disso;

5) Apresentam aos utentes das carteiras as informações contidas nos certificados de acesso de utilizadores de carteiras ou nos certificados de unidades de carteira;

6) Apresentam aos utentes das carteiras, se for caso disso, os atributos que são convidados a apresentar;

7) Apresentam aos utentes da carteira, se for caso disso, as informações contidas no certificado de registo de utilizador de carteira;

8) Apresentam certificados de unidades de carteira da unidade de carteira aos utilizadores de carteiras ou às unidades de carteira que os solicitem;

9) Não apresentam quaisquer atributos solicitados a utilizadores de carteiras ou unidades de carteira até que estejam preenchidos os seguintes requisitos:

   a) Verificar que a aplicação criptográfica segura de carteiras autenticou a identidade do utente da carteira;

   b) Verificar que as políticas de divulgação incorporadas foram processadas na unidade de carteira em conformidade com o artigo 11.º do Regulamento de Execução (UE) 2024/2979, se for caso disso;

   c) Verificar que os utentes das carteiras aprovaram parcial ou integralmente a apresentação;

10) Permitem técnicas de preservação da privacidade que assegurem a ausência de associação caso os certificados eletrónicos de atributos não exijam a identificação do utente da carteira, ao apresentar certificados ou dados de identificação pessoal a diferentes utilizadores de carteiras.

Artigo 4.º

Emissão de dados de identificação pessoal e certificados eletrónicos de atributos para unidades de carteira

1. Os fornecedores de carteiras devem assegurar que as soluções de carteiras suportam protocolos e interfaces para a emissão de dados de identificação pessoal e certificados eletrónicos de atributos para unidades de carteira.

2. Os fornecedores de carteiras devem assegurar que as unidades de carteira solicitam a emissão de dados de identificação pessoal e certificados eletrónicos de atributos apenas a utilizadores que dispõem de um certificado de acesso de utilizador de carteira autêntico e válido que os certifique como:

a) Um fornecedor de dados de identificação pessoal;

b) Um fornecedor de um certificado eletrónico de atributos qualificado;

c) Um fornecedor de um certificado eletrónico de atributos emitido por ou em nome de um organismo do setor público responsável por uma fonte autêntica; ou

d) Um fornecedor de certificados eletrónicos de atributos não qualificados.

3. No que diz respeito à emissão de dados de identificação pessoal e de certificados eletrónicos de atributos para uma unidade de carteira, os fornecedores de carteiras devem assegurar que são cumpridos os seguintes requisitos:

a) Caso os utentes das carteiras utilizem a sua unidade de carteira para solicitar a emissão de dados de identificação pessoal ou de certificados eletrónicos de atributos a fornecedores de dados de identificação pessoal ou fornecedores de certificados eletrónicos de atributos que permitam a emissão dos referidos dados ou certificados em mais do que um formato, a unidade de carteira deve solicitá-la em todos os formatos a que se refere o artigo 8.º do Regulamento de Execução (UE) 2024/2979 que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 no respeitante à integridade e às funcionalidades essenciais das carteiras europeias de identidade digital;

b) Caso os utentes das carteiras utilizem a sua unidade de carteira para interagir com fornecedores de dados de identificação pessoal ou certificados eletrónicos de atributos, as unidades de carteira devem permitir a autenticação e a validação dos componentes da unidade de carteira, apresentando os certificados de unidades de carteira a esses fornecedores, a seu pedido;

c) As soluções de carteiras devem suportar mecanismos que permitam aos fornecedores de dados de identificação pessoal verificar a emissão, a entrega e a ativação em conformidade com os requisitos de nível de garantia elevado estabelecidos no Regulamento de Execução (UE) 2015/1502 da Comissão ([11]);

d) As unidades de carteira devem verificar a autenticidade e a validade dos dados de identificação pessoal e dos certificados eletrónicos de atributos.

Artigo 5.º

Apresentação de atributos a utilizadores de carteiras

1. Os fornecedores de carteiras devem assegurar que as soluções de carteiras suportam protocolos e interfaces para a apresentação de atributos a utilizadores de carteiras, à distância e, se for caso disso, em situação de proximidade, nos termos das normas estabelecidas no anexo.

2. Os fornecedores de carteiras devem assegurar que, a pedido dos utentes, as unidades de carteira respondem aos pedidos devidamente autenticados e validados dos utilizadores de carteiras a que se refere o artigo 3.º, nos termos das normas estabelecidas no anexo.

3. Os fornecedores de carteiras devem assegurar que as unidades de carteira suportam a prova da posse de chaves privadas correspondentes a chaves públicas utilizadas em vinculação criptográfica.

([11]) Regulamento de Execução (UE) 2015/1502 da Comissão, de 8 de setembro de 2015, que estabelece as especificações técnicas mínimas e os procedimentos para a atribuição dos níveis de garantia dos meios de identificação eletrónica, nos termos do artigo 8.º, n.º 3, do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno (JO L 235 de 9.9.2015, p. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

4. Os fornecedores de carteiras devem assegurar que as soluções de carteiras suportam a divulgação seletiva de atributos de dados de identificação pessoal e de certificados eletrónicos de atributos.

5. Os n.os 1 a 4 aplicam-se, *mutatis mutandis*, às interações entre duas unidades de carteira em situação de proximidade.

Artigo 6.º

Comunicação de pedidos de apagamento de dados

1. Os fornecedores de carteiras devem assegurar que as unidades de carteira suportam protocolos e interfaces que permitam aos utentes das carteiras solicitar aos utilizadores de carteiras com os quais interagiram por meio dessas unidades de carteira o apagamento dos seus dados pessoais facultados através dessas unidades de carteira, em conformidade com o artigo 17.º do Regulamento (UE) 2016/679.

2. Os protocolos e interfaces a que se refere o n.º 1 devem permitir aos utentes das carteiras selecionar os utilizadores de carteiras aos quais os pedidos de apagamento de dados devem ser apresentados.

3. As unidades de carteira devem apresentar ao utente da carteira os pedidos de apagamento de dados anteriormente realizados através dessas unidades de carteira.

Artigo 7.º

Comunicação de utilizadores de carteiras às autoridades de controlo estabelecidas nos termos do artigo 51.º do Regulamento (UE) 2016/679

1. Os fornecedores de carteiras devem assegurar que as unidades de carteira permitem que os utentes das carteiras comuniquem facilmente os utilizadores de carteiras às autoridades de controlo estabelecidas nos termos do artigo 51.º do Regulamento (UE) 2016/679.

2. Os fornecedores de carteiras devem implementar os protocolos e interfaces para comunicar os utilizadores de carteiras, em conformidade com o direito processual nacional dos Estados-Membros.

3. Os fornecedores de carteiras devem assegurar que as unidades de carteira permitem aos utentes das carteiras fundamentarem as comunicações, nomeadamente anexando informações pertinentes para identificar os utilizadores de carteiras, bem como as alegações dos utentes das carteiras, em formato legível por máquina.

Artigo 8.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.

Feito em Bruxelas, em 28 de novembro de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

NORMAS A QUE SE REFERE O ARTIGO 5.º, N.os 1 E 2

— ISO/IEC 18013-5:2021

— ISO/IEC TS 18013-7:2024