2026/1735

22.7.2026

REGULAMENTO DE EXECUÇÃO (UE) 2026/1735 DA COMISSÃO

de 15 de julho de 2026

que altera o Regulamento de Execução (UE) 2025/1569 no respeitante às normas e especificações aplicáveis

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 45.º-D, n.º 5, o artigo 45.º-E, n.º 2, e o artigo 45.º-F, n.ºs 6 e 7,

Considerando o seguinte:

(1) A fim de assegurar o mais elevado nível de harmonização entre os Estados-Membros para o desenvolvimento das carteiras europeias de identidade digital, as especificações técnicas das carteiras baseiam-se nos trabalhos realizados nos termos da Recomendação (UE) 2021/946 da Comissão ([2]) e, em especial, na arquitetura e no regime de referência. Uma vez que ambos evoluíram significativamente desde a adoção do Regulamento de Execução (UE) 2025/1569 da Comissão ([3]), este deve agora ser alterado em conformidade de forma a estar alinhado com as novas normas e especificações.

(2) Em conformidade com os objetivos do Regulamento (UE) n.º 910/2014, foram selecionadas várias normas para cumprir os requisitos aplicáveis à emissão, gestão e verificação de certificados eletrónicos de atributos. Estas normas devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Sempre que necessário, devem ser adaptadas ou complementadas de modo a assegurar um elevado nível de segurança e integridade dos certificados eletrónicos de atributos, facilitando simultaneamente a interoperabilidade transfronteiriça e o bom funcionamento do mercado interno. Em consonância com este objetivo, o presente regulamento atualiza os requisitos aplicáveis à emissão e revogação de certificados eletrónicos qualificados de atributos e certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome e introduz os requisitos para a aposição de assinaturas e selos nos resultados da verificação por confronto com fontes autênticas.

(3) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([4]) e, se for caso disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([5]) aplicam-se a todas as atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

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

([2]) 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).

([3]) Regulamento de Execução (UE) 2025/1569 da Comissão, de 29 de julho de 2025, que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante aos certificados eletrónicos qualificados de atributos e aos certificados eletrónicos de atributos fornecidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) 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).

([5]) 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) 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 ([6]) e emitiu parecer em 17 de abril de 2026 ([7]).

(5) 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

Alterações do Regulamento de Execução (UE) 2025/1569

O Regulamento de Execução (UE) 2025/1569 é alterado do seguinte modo:

1) No artigo 3.º, o n.º 2 passa a ter a seguinte redação:

«2. Sempre que os fornecedores de certificados eletrónicos qualificados de atributos e os fornecedores de certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome emitem certificados eletrónicos de atributos que são incluídos em sistemas registados no catálogo de sistemas de certificação de atributos, devem cumprir os requisitos do sistema correspondente de certificação de atributos. A avaliação da conformidade estabelecida no Regulamento (UE) n.º 910/2014 deve abranger as políticas e os procedimentos estabelecidos pelos emitentes de certificados a fim de cumprir os requisitos dos sistemas de certificação de atributos.».

2) O artigo 4.º é alterado do seguinte modo:

a) É suprimido o n.º 1;

b) O n.º 3 passa a ter a seguinte redação:

«3. Sempre que esses certificados sejam emitidos com um período de validade superior a 24 horas, os fornecedores de certificados eletrónicos qualificados de atributos e os fornecedores de certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome devem revogá-los, pelo menos, nas seguintes circunstâncias:

a) Mediante pedido da pessoa a quem foi emitido o certificado eletrónico de atributos ou, quando aplicável, da pessoa que é objeto do certificado;

b) Se o fornecedor tomar conhecimento de que houve um comprometimento da segurança ou da fiabilidade dos certificados eletrónicos qualificados de atributos ou dos certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome;

c) Noutras situações em que tal seja exigido pelo direito da União ou pelo direito nacional.»;

c) O n.º 4 passa a ter a seguinte redação:

«4. Os fornecedores de certificados eletrónicos qualificados de atributos e os fornecedores de certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome devem instituir técnicas de revogação e métodos de gestão que preservem a privacidade e impeçam a associação ou rastreabilidade. As técnicas de revogação devem cumprir os requisitos estabelecidos no anexo II.».

([6]) 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).

([7]) *EDPS Formal comments on the draft Commission Implementing Regulation as regards applicable standards and specifications for the registration of wallet-relying parties* | Autoridade Europeia para a Proteção de Dados.

3) O artigo 9.º é alterado do seguinte modo:

a) A seguir ao n.º 2, é inserido um novo n.º 2-A com a seguinte redação:

«2-A. O mecanismo de verificação deve cumprir as especificações estabelecidas no anexo IV.»;

b) O n.º 4 passa a ter a seguinte redação:

«4. O resultado da verificação deve indicar se o atributo foi ou não verificado e especificar o organismo do setor público responsável pela fonte autêntica ou, se for caso disso, o organismo do setor público designado para atuar em nome da fonte autêntica com base na qual o atributo foi verificado.

O resultado da verificação deve ser assinado ou selado pelo organismo do setor público responsável por uma fonte autêntica, ou pelo intermediário designado reconhecido a nível nacional, utilizando, pelo menos, uma assinatura eletrónica avançada baseada num certificado qualificado de assinaturas eletrónicas ou um selo eletrónico avançado baseado num certificado qualificado de selos eletrónicos, respetivamente.».

4) O anexo I é substituído pelo texto que consta do anexo I do presente regulamento.

5) O anexo II é substituído pelo texto que consta do anexo II do presente regulamento.

6) O texto que consta do anexo III do presente regulamento é aditado como anexo IV.

Artigo 2.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 artigo 1.º, n.º 3, é aplicável a partir de 1 de janeiro de 2027.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 15 de julho de 2026.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

«*ANEXO I*

Lista das normas de referência e especificações a que se refere o artigo 3.º

Aplica-se a norma ETSI TS 119 471 V1.1.1 (2025-05) com as seguintes adaptações:

1) 2.1 Referências normativas:

[1] ETSI EN 319 401 V3.2.1 (2026-01): "Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers" [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política geral para os prestadores de serviços de confiança].

[2] Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia: "Agreed Cryptographic Mechanisms" (Mecanismos criptográficos acordados), publicado pela Agência da União Europeia para a Cibersegurança (ENISA).

[3] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules" (Requisitos de segurança para módulos criptográficos).

[4] Regulamento de Execução (UE) 2024/482 da Comissão ([1]).

[5] Regulamento de Execução (UE) 2024/3144 da Comissão ([2]).

[6] ISO/IEC 15408:2022 (partes 1 a 5): "Information security, cybersecurity and privacy protection — Evaluation criteria for IT security" [Segurança da informação, cibersegurança e proteção da privacidade — Critérios de avaliação da segurança informática].

2) 3.1 Termos:
É aditado o seguinte termo:

— dispositivo criptográfico seguro: dispositivo que detém a chave privada do utente, a protege contra o risco de comprometimento e executa funções de assinatura ou decifragem em nome do utente.

3) 4. Serviços de confiança dos certificados eletrónicos de atributos (EAA)

— A cláusula 4.2.2.2 "Verification of attributes against authentic sources" (Verificação de atributos por confronto com fontes autênticas) não é aplicável.

— REQ-EAASP-4.2.2.3-02: o prestador de serviços de certificados eletrónicos de atributos (EAASP) deve autenticar-se junto da instância da carteira europeia de identidade digital, implementando mecanismos de autenticação mútua que utilizem um certificado de acesso válido.

— REQ-EAASP-4.2.2.3-03: o EAASP deve validar a unidade da carteira europeia de identidade digital e verificar *se a instância da carteira foi revogada.*

— A cláusula *4.3.2 "EUDIW Specific" (Requisitos específicos para a carteira europeia de identidade digital) não é aplicável.*

4) 6.1 Declaração de práticas dos serviços de certificados eletrónicos de atributos (EAAS):

— REQ-EAASP-6.1-02: o EAASP deve documentar o mecanismo de revogação na declaração de práticas dos EAAS.

5) 6.3 Política de segurança da informação:

— REQ-EAASP-6.3-02: o EAASP deve estabelecer procedimentos para notificar a entidade supervisora sobre quaisquer alterações na prestação do serviço de confiança de certificação eletrónica de atributos e a intenção de cessar essas atividades, em conformidade com os requisitos operacionais e as disposições legislativas e regulamentares aplicáveis, nomeadamente nos termos dos requisitos dos atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014. O EAASP deve notificar a entidade supervisora pelo menos:

— um mês antes da implementação de qualquer alteração,

— três meses antes da cessação prevista da prestação de um serviço de confiança.

([1]) Regulamento de Execução (UE) 2024/482 da Comissão, de 31 de janeiro de 2024, que estabelece regras de execução do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho no respeitante à adoção do sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Regulamento de Execução (UE) 2024/3144 da Comissão, de 18 de dezembro de 2024, que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6) 7.5 Controlos criptográficos:

— REQ-EAASP-7.5.2-05: nulo e sem efeito.

— REQ-EAASP-7.5.2-06: nulo e sem efeito.

— REQ-EAASP-7.5.3-01A: devem existir controlos de segurança adequados para a gestão de quaisquer chaves criptográficas, algoritmos criptográficos e dispositivos criptográficos ao longo do respetivo ciclo de vida, seguindo, se for caso disso, uma abordagem de agilidade criptográfica.

— REQ-EAASP-7.5.3-01B: para efeitos da prestação dos respetivos serviços de confiança, o EAASP deve selecionar e utilizar técnicas criptográficas adequadas conformes com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [2].

— REQ-EAASP-7.5.3-02: o EAASP deve assegurar que o dispositivo criptográfico seguro utilizado para a assinatura ou selo digital do EAA é um dispositivo qualificado de criação de assinaturas ou de selos e que todas as outras assinaturas ou selos digitais utilizados para prestar o serviço de confiança de certificação eletrónica de atributos correspondente, ou de parte do mesmo, são criados através de um dispositivo criptográfico seguro que seja um sistema fiável certificado em conformidade com:

a) Os Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, estabelecidos nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão 3.1 (CC3.1) até 31.8.2027, ou na versão CC:2022, partes 1 a 5, publicados pelos participantes no Acordo de Reconhecimento de Certificados de Critérios Comuns no domínio da Segurança das TI, ou estabelecidos pela norma ISO/IEC 15408 [6], e certificado com o nível EAL 4 ou superior; ou

b) O sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns (EUCC) [4] [5] e certificado de acordo com o nível EAL 4 ou superior; ou

c) A FIPS-140-2 nível 3 a utilizar até 31.8.2027 para sistemas certificados existentes ou a FIPS PUB 140-3 [3] nível 3 até 31.12.2030.

Esta certificação refere-se a uma meta de segurança ou a um perfil de proteção, ou a uma documentação de segurança e conceção de módulos, que cumpra os requisitos do presente documento, com base numa análise de risco e tendo em conta as medidas de segurança físicas e outras medidas de segurança não técnicas.

Se o dispositivo criptográfico seguro possuir uma certificação EUCC [4] [5], deve ser configurado e utilizado em conformidade com essa certificação.

— REQ-EAASP-7.5.5-01: nulo e sem efeito.

— REQ-EAASP-7.5.5-02: nulo e sem efeito.

— REQ-EAASP-7.5.5-04: nulo e sem efeito.

7) 7.9 Vulnerabilidades e gestão de incidentes:

— REQ-EAASP-7.9-02: as atividades de monitorização devem ter em conta a sensibilidade das informações recolhidas ou analisadas.

8) 7.12 Cessação e planos de cessação do EAASP e dos EAAS:

— REQ-EAASP-7.12-04: o plano de cessação do EAASP deve cumprir os requisitos estabelecidos nos atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014 [i.1].».

ANEXO II

«*ANEXO II*

Especificações técnicas a que se referem os artigos 3.º e 4.º

Os fornecedores de certificados eletrónicos qualificados de atributos e os fornecedores de certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome devem emitir os seus certificados em conformidade com, pelo menos, uma das normas enumeradas no anexo II do Regulamento de Execução (UE) 2024/2979 da Comissão ([1]) e aplicar as técnicas de revogação pertinentes, igualmente enumeradas no anexo II desse regulamento.».

([1]) 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).

ANEXO III

«ANEXO IV

Lista das normas e especificações técnicas a que se refere o artigo 9.º

Os mecanismos de verificação referidos no artigo 9.º devem cumprir um ou ambos os seguintes elementos:

a) As especificações técnicas enumeradas na cláusula 6.1.1 da norma ETSI TS 119 478 V1.1.1 (2026-01) — "Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources" [Assinaturas eletrónicas e infraestruturas de confiança (ESI); especificação de interfaces relacionadas com fontes autênticas];

— REQ-ASIP-6.1.1.2-04-01 [CONDICIONAL]: se o attributeVerificationResult for http://uri.etsi.org/19478/VerificationResult/Match ou http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, o attributeVerificationResult pode conter um elemento attributeValue,

— REQ-ASIP-6.1.1.2-04-02 [CONDICIONAL]: se o attributeVerificationResult devolvido for http://uri.etsi.org/19478/VerificationResult/Match e o attributeVerificationResult contiver um elemento attributeValue, este elemento deve conter o valor indicado no pedido.

— REQ-ASIP-6.1.1.2-04-03 [CONDICIONAL]: se o attributeVerificationResult devolvido for http://uri.etsi.org/19478/VerificationResult/MatchWithVariation e o attributeVerificationResult contiver um elemento attributeValue, este elemento deve conter o valor do atributo, tal como armazenado na fonte autêntica.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDICIONAL]: se o fragmentVerificationResult for http://uri.etsi.org/19478/VerificationResult/Match ou http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, attributeVerificationResult pode conter um elemento fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDICIONAL]: se o fragmentVerificationResult devolvido for http://uri.etsi.org/19478/VerificationResult/Match e o attributeVerificationResult contiver um elemento fragmentValue, este elemento deve conter o valor indicado no pedido.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDICIONAL]: se o fragmentVerificationResult devolvido for http://uri.etsi.org/19478/VerificationResult/MatchWithVariation e o attributeVerificationResult contiver um elemento fragmentValue, este elemento deve conter o valor do fragmento do atributo, tal como armazenado na fonte autêntica.

b) As especificações técnicas enumeradas na cláusula 6.2.3 da norma ETSI TS 119 478 V1.1.1 (2026-01) — "Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources" [Assinaturas eletrónicas e infraestruturas de confiança (ESI); especificação de interfaces relacionadas com fontes autênticas];

— REQ-ASIP-6.2.3.2.1-08-04: o elemento AttributeVerificationResponse pode incluir exatamente um sub-elemento à escolha entre TextValue, XMLValue ou AttributeProperties.».