Jornal Oficial
da União Europeia

PT
Série L

2025/1567

30.7.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1567 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 à gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e de dispositivos qualificados de criação de selos eletrónicos à distância enquanto serviços de confiança qualificados

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 29.º-A, n.º 2, e o artigo 39.º-A,

Considerando o seguinte:

(1) Os serviços de confiança qualificados para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância desempenham um papel crucial no ambiente empresarial digital ao promoverem a transição dos processos tradicionais em suporte papel para equivalentes eletrónicos. Esses serviços de confiança qualificados contribuem para uma gestão segura e fiável dos referidos dispositivos à distância em nome dos signatários e criadores de selos, de uma forma que garanta o cumprimento das condições aplicáveis às assinaturas eletrónicas qualificadas e aos selos eletrónicos qualificados.

(2) A fim de reforçar a segurança jurídica e a fiabilidade dos serviços de confiança qualificados para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e dos serviços de confiança qualificados para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância, os prestadores qualificados de serviços de confiança que prestam esses serviços qualificados devem cumprir as normas estabelecidas no presente regulamento.

(3) Estas normas devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Devem ser adaptadas de modo a incluir controlos para garantir a segurança e a fiabilidade dos serviços de confiança qualificados, bem como para assegurar que os signatários têm o controlo exclusivo, com um elevado nível de confiança, da utilização dos seus dados para a criação de assinaturas eletrónicas e que os criadores de selos controlam a utilização dos seus dados para a criação de selos eletrónicos, respetivamente.

(4) A fim de assegurar um prazo adequado para a auditoria dos prestadores de serviços de confiança no que diz respeito ao cumprimento dos novos requisitos, este deve ser aplicável 24 meses após a sua entrada em vigor.

(5) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou especificações técnicas. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([2]), a Comissão deve rever e atualizar o presente regulamento, se necessário, a fim de assegurar que o mesmo acompanha a evolução mundial, novas tecnologias, normas ou especificações técnicas e de 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) 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).

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

(7) 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 ([5]) e emitiu parecer em 6 de junho de 2025.

(8) 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

Normas de referência e especificações

As normas de referência e especificações aplicáveis à gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e de dispositivos qualificados de criação de selos eletrónicos à distância enquanto serviços de confiança qualificados a que se referem o artigo 29.º-A, n.º 2, e o artigo 39.º-A do Regulamento (UE) n.º 910/2014 constam do anexo do presente regulamento.

Artigo 2.º

Entrada em vigor e aplicabilidade

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

O presente regulamento é aplicável a partir de 19 de agosto de 2027.

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

Feito em Bruxelas, em 29 de julho de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

([3]) 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).

([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]) 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).

ANEXO

Lista de normas de referência e especificações aplicáveis à gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e de dispositivos qualificados de criação de selos eletrónicos à distância

A norma ETSI TS 119 431-1 V1.3.1 (2024-12) («ETSI TS 119 431-1») é aplicável para efeitos de avaliação da conformidade com a política «EU Server Signing Application Service v2» (política do serviço de aplicação de assinatura em servidor da UE), em conformidade com o anexo A dessa norma, com as seguintes adaptações:

1) 2.1 Referências normativas

— [1] ETSI EN 319 401 V3.1.1 (2024-06): «Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers» (Assinaturas eletrónicas e infraestruturas de confiança; requisitos de política geral para os prestadores de serviços de confiança);

— [7] 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) ([1]).

2) 6.1 Responsabilidades em matéria de publicação e criação de repositórios

— OVR-6.1-04: as informações identificadas no OVR-6.1-01 devem estar disponíveis pública e internacionalmente.

3) 6.4.4 Controlos do pessoal

— OVR-6.4.4-02: os prestadores de serviços de aplicação de assinatura em servidor (SSASP) devem empregar pessoal em funções de confiança e, se aplicável, subcontratantes em funções de confiança, que possuam os conhecimentos especializados, a experiência e as qualificações necessários adquiridos por meio de formação formal e credenciais, de experiência, ou de uma combinação de ambas;

— OVR-6.4.4-03: a conformidade com o OVR-6.4.4-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

4) 6.4.9 Cessação do serviço do SSASP

— OVR-6.4.9-02: o plano de cessação do SSASP deve ser conforme com os atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014 [i.1].

5) 6.5.5 Controlos de segurança da rede

— OVR-6.5.5-02: a análise das vulnerabilidades solicitada pelo REQ-7.8-13 da norma ETSI EN 319 401 [1] deve ser efetuada pelo menos uma vez por trimestre;

— OVR-6.5.5-03: as barreiras de segurança devem ser configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do prestador de serviços de confiança.

6) 6.8.5 Controlos criptográficos

— OVR-6.8.5-01: devem ser implementados controlos de segurança adequados para a gestão de quaisquer técnicas criptográficas do SSASP ao longo do seu ciclo de vida;

— OVR-6.8.5-02: no que diz respeito ao OVR-6.8.5-01, o SSASP 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 [7].

7) Anexo A, secção A.3 Requisitos gerais

— OVR-A.3-02 [EUSPv2]: a declaração de práticas do prestador de serviços de confiança deve incluir a referência à certificação do dispositivo qualificado de criação de assinaturas empregado em conformidade com os requisitos do Regulamento (UE) n.º 910/2014 [i.1], anexo II.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.