2025/2532

17.12.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/2532 DA COMISSÃO

de 16 de dezembro de 2025

que estabelece as regras de execução do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho no respeitante às normas de referência e especificações para serviços qualificados de arquivo eletrónico

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-J, n.º 2,

Considerando o seguinte:

(1) Por força do Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho ([2]), foi introduzida no Regulamento (UE) n.º 910/2014 uma lista de novos serviços de confiança e de serviços de confiança qualificados, incluindo o serviço qualificado de arquivo eletrónico. Importa que a Comissão estabeleça uma lista de normas de referência e, se necessário, especificações para esses serviços.

(2) O arquivo eletrónico é um serviço para a receção, o armazenamento, a recuperação e a supressão de dados eletrónicos e de documentos eletrónicos, a fim de assegurar a sua durabilidade e legibilidade, bem como de preservar a sua integridade, confidencialidade e prova de origem durante todo o período de preservação. Os serviços qualificados de arquivo eletrónico desempenham um papel crucial no ambiente empresarial digital ao promoverem a transição dos processos tradicionais em suporte papel para equivalentes eletrónicos. Para assegurar que os dados eletrónicos e os documentos eletrónicos preservam a presunção da sua integridade e da sua origem durante o período de preservação pelo prestador qualificado de serviços de confiança e alcançar um nível elevado de transparência e confiança entre todos os participantes no ciclo de vida da informação, é necessário estabelecer um conjunto comum de especificações para os serviços qualificados de arquivo eletrónico.

(3) A fim de aumentar o valor probatório, a segurança e a fiabilidade dos serviços qualificados de arquivo eletrónico, sempre que sejam utilizadas assinaturas eletrónicas, selos eletrónicos ou selos temporais para criar, assinar, selar ou atestar a data e a hora, por exemplo, de provas de arquivo, de registos de provas, de registos de eventos, de registos da correta aplicação de procedimentos ou de relatórios de confirmação de arquivo, devem ser utilizados serviços de confiança qualificados.

(4) A presunção de conformidade prevista no artigo 45.º-J, n.º 2, do Regulamento (UE) n.º 910/2014 só deve aplicar-se se os serviços qualificados de arquivo eletrónico cumprirem os requisitos estabelecidos no presente regulamento. As normas de referência para os serviços qualificados de arquivo eletrónico devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Devem igualmente ser adaptadas de modo a incluir controlos adicionais que garantam a segurança e a fiabilidade dos serviços qualificados de arquivo eletrónico.

(5) Se um prestador de serviços de confiança cumprir os requisitos estabelecidos no presente regulamento, as entidades supervisoras devem presumir a conformidade com os requisitos pertinentes do Regulamento (UE) n.º 910/2014 e ter devidamente em conta essa presunção para conceder ou confirmar o estatuto de qualificado do serviço de confiança. No entanto, um prestador qualificado de serviços de confiança pode continuar a invocar outras práticas para demonstrar o cumprimento dos requisitos do Regulamento (UE) n.º 910/2014.

(6) A fim de preservar a integridade e a prova de origem dos dados eletrónicos e dos documentos eletrónicos que contenham uma ou mais assinaturas ou selos eletrónicos qualificados, os serviços qualificados de arquivo eletrónico devem utilizar procedimentos e tecnologias capazes de prolongar a fiabilidade dessas assinaturas e selos eletrónicos para além do período de validade tecnológica, pelo menos durante todo o período de preservação.

([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).

(7) A Comissão avalia periodicamente as novas tecnologias, práticas, normas ou especificações técnicas. Em conformidade com o considerando 75 do Regulamento (UE) 2024/1183, a Comissão deve rever e, se necessário, atualizar o presente regulamento, a fim de assegurar que o mesmo acompanha a evolução mundial, as novas tecnologias, práticas, normas ou especificações técnicas e de seguir as boas práticas no mercado interno.

(8) 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]) aplicam-se às atividades de tratamento de dados pessoais ao abrigo do presente regulamento.

(9) 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 21 de outubro de 2025 ([6]).

(10) 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

Arquivo eletrónico de documentos que ostentem uma assinatura eletrónica qualificada ou um selo eletrónico qualificado

1. Ao arquivar dados eletrónicos ou documentos eletrónicos que contenham assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados, os prestadores de serviços qualificados de arquivo eletrónico devem assegurar que é mantida a fiabilidade dessas assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados, inclusive para além do seu período de validade tecnológica, e que a integridade e a exatidão da origem das assinaturas e selos eletrónicos qualificados são mantidas, pelo menos até ao termo do período de preservação legal ou contratual.

2. Para efeitos do n.º 1, os prestadores de serviços qualificados de arquivo eletrónico podem recorrer a um serviço qualificado de preservação de assinaturas eletrónicas qualificadas ou a um serviço qualificado de preservação de selos eletrónicos qualificados.

Artigo 2.º

Normas de referência e especificações para a prestação de serviços qualificados de arquivo eletrónico

As normas de referência e especificações a que se refere o artigo 45.º-J, n.º 2, do Regulamento (UE) n.º 910/2014 constam do anexo do presente regulamento.

([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).

([6]) EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services [não traduzido para português].

Artigo 3.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 16 de dezembro de 2025.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

Lista de normas de referência e especificações para serviços qualificados de arquivo eletrónico

Aplica-se a norma CEN/TS 18170:2025 («CEN/TS 18170»), com as seguintes adaptações:

a) Referências normativas (cláusula 2)

— 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 (ESI); requisitos de política geral para os prestadores de serviços de confiança];

— ETSI EN 319 421 V1.3.1 (2025-07), «Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política e de segurança para os prestadores de serviços de confiança que emitem selos temporais];

— ISO 14721:2025, «Space Data System Practices — Reference model for an open archival Information System (OAIS)» [Práticas dos sistemas de dados espaciais — Modelo de referência para um sistema aberto de arquivo de informação (OAIS)];

— Grupo Europeu para a Certificação da Cibersegurança, subgrupo para a criptografia (ACM-ECCG): «Agreed Cryptographic Mechanisms» [Mecanismos criptográficos acordados], publicado pela Agência da União Europeia para a Cibersegurança (ENISA);

— Regulamento de Execução (UE) 2024/482 da Comissão ([1]);

— Regulamento de Execução (UE) 2024/3144 da Comissão ([2]);

— 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];

— FIPS PUB 140-3 (2019), «Security Requirements for Cryptographic Modules» [Requisitos de segurança para módulos criptográficos].

b) Declaração de políticas e de práticas (cláusula 6.1)

— Aplicam-se os requisitos da norma CEN/TS 18170, cláusula 6.1;

— Aplicam-se os requisitos da norma ETSI EN 319 401, cláusula 5;

— O prestador de serviços de confiança de arquivo eletrónico (EATSP) deve estabelecer procedimentos para notificar a entidade supervisora de quaisquer alterações da prestação do serviço de confiança de arquivo eletrónico e da intenção de cessar essas atividades, em conformidade com os requisitos operacionais e as disposições legislativas e regulamentares aplicáveis, nomeadamente em conformidade com os requisitos dos atos de execução adotados nos termos do artigo 24.º, n.º 5, do Regulamento (UE) n.º 910/2014 [i.2];

— O EATSP deve notificar a entidade supervisora competente pelo menos:

  — um mês antes da implementação de qualquer alteração,

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

c) Termos e condições (cláusula 6.2)

— Aplicam-se os requisitos da norma CEN/TS 18170, cláusula 6.2;

— Os assinantes e os utilizadores do serviço de confiança de arquivo eletrónico devem ser informados, de forma clara, exaustiva e facilmente acessível, num espaço de acesso público e individualmente, dos termos e condições exatos, antes de estabelecerem uma relação contratual.

([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).

d) Recursos humanos (cláusula 7.3)

— Aplicam-se os requisitos da norma CEN/TS 18170, cláusula 7.3;

— O pessoal do EATSP com funções de confiança e, se aplicável, os seus subcontratantes com funções de confiança devem ser capazes de cumprir o requisito de dispor de conhecimentos especializados, experiência e qualificações adquiridos por meio de formação formal e credenciais, de experiência ou de uma combinação de ambas. Isto inclui atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

e) Controlos criptográficos e monitorização (ponto 7.6)

— O sistema de arquivo deve garantir a confidencialidade dos dados e dos documentos ao longo do ciclo de vida do arquivo, desde o seu depósito até à sua eliminação;

— Aplicam-se os requisitos especificados na norma ETSI EN 319 401, subcláusula 7.5 «Controlos criptográficos»;

— A origem dos dados a arquivar no sistema de arquivo eletrónico é determinada pelo EATSP, sendo que se se utilizarem assinaturas eletrónicas ou selos eletrónicos para o efeito, essas assinaturas eletrónicas ou selos eletrónicos devem ser qualificados;

— Quando o EATSP assinar digitalmente (parte de) um objeto ou registo digital, a chave de assinatura privada do EATSP deve ser mantida e utilizada num dispositivo de criação de assinaturas ou selos eletrónicos qualificados ou num 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 na norma ISO/IEC 15408 ou nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, 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, e certificado com o nível EAL 4 ou superior; ou

b) O sistema europeu de certificação da cibersegurança baseado nos Critérios Comuns [Regulamento de Execução (UE) 2024/482 da Comissão e Regulamento de Execução (UE) 2024/3144 da Comissão] e certificado com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 nível 3.

— 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 [Regulamento de Execução (UE) 2024/482 da Comissão e Regulamento de Execução (UE) 2024/3144 da Comissão], deve ser configurado e utilizado em conformidade com essa certificação;

— O EATSP deve monitorizar a robustez do algoritmo criptográfico que foi e é utilizado. Caso se considere que um dos algoritmos ou parâmetros utilizados tenha deixado de ser adequado, conforme definido na gestão dos riscos, o EATSP deve atualizar a política de arquivo conexa ou criar um novo perfil de arquivo para tratar os pacotes de arquivos de informação e definir e executar as medidas adequadas;

— A avaliação dos algoritmos criptográficos e da sua utilização pelo EATSP deve estar em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA (ACM-ECCG);

— Os componentes técnicos do serviço de confiança de arquivo eletrónico (EATS) devem autenticar-se mutuamente com base em técnicas criptográficas antes de comunicarem.

f) Rede (cláusula 7.9)

— Aplicam-se os requisitos especificados na norma ETSI EN 319 401, subcláusula 7.8 «Segurança da rede»;

— A análise das vulnerabilidades solicitada pelo REQ-7.8-13 da norma ETSI EN 319 401 é efetuada, pelo menos, uma vez por trimestre;

— O teste de penetração solicitado pelo REQ-7.8-17X da norma ETSI EN 319 401 é efetuado, pelo menos, uma vez por ano;

— As barreiras de segurança são configuradas de modo a impedir todos os protocolos e acessos não necessários para a operação do EATSP.

g) Recolha de provas (cláusula 7.11)

— Aplicam-se os requisitos especificados na norma ETSI EN 319 401, subcláusula 7.10 «Recolha de provas», nomeadamente para eventos críticos e não críticos (ver subcláusula 13.2).

h) Cessação e plano de cessação do EATSP (cláusula 7.13)

— Aplicam-se os requisitos da norma CEN/TS 18170, cláusula 7.13;

— O plano de cessação do EATSP o 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) Hora fiável dos eventos (cláusula 13.3.1)

— Aplicam-se os requisitos da norma CEN/TS 18170, cláusula 13.3.1;

— Sempre que utilizar selos temporais, o EATSP deve utilizar um selo temporal qualificado.