Jornal Oficial
da União Europeia

PT
Série L

2025/1566

30.7.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1566 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 às normas de referência para a verificação da identidade e dos atributos da pessoa a quem deve ser emitido o certificado qualificado ou o certificado eletrónico qualificado de atributos

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 24.º, n.º 1-C,

Considerando o seguinte:

(1) O artigo 24.º do Regulamento (UE) n.º 910/2014 exige que os prestadores qualificados de serviços de confiança verifiquem a identidade e, se aplicável, os eventuais atributos específicos de uma pessoa singular ou coletiva ao emitirem certificados qualificados ou certificados eletrónicos qualificados de atributos a essa pessoa.

(2) A fim de assegurar a igualdade de tratamento e a capacidade de confiar no resultado do processo de verificação, aquando da emissão de um certificado qualificado ou de um certificado eletrónico qualificado de atributos, todos os prestadores qualificados de serviços de confiança devem efetuar as verificações de forma equivalente. Em conformidade com os objetivos do Regulamento (UE) n.º 910/2014, foram selecionadas várias normas para cumprir estes requisitos específicos. Estas normas devem refletir as práticas estabelecidas e ser amplamente reconhecidas nos setores pertinentes. Devem ser adaptadas de modo a incluir controlos adicionais que garantam a segurança e a fiabilidade do serviço de confiança qualificado, facilitando simultaneamente a interoperabilidade transfronteiriça e o bom funcionamento do mercado interno.

(3) Importa prever um período transitório adequado que permita aos prestadores qualificados de serviços de confiança cumprir os requisitos do Regulamento (UE) n.º 910/2014. A fim de assegurar um prazo suficiente para a auditoria dos prestadores de serviços de confiança no que diz respeito ao cumprimento dos requisitos do presente regulamento, este deve ser aplicável 24 meses após a sua entrada em vigor.

(4) 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.

(5) 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.

([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).

([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).

(6) 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.

(7) 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

As normas de referência e especificações a que se refere o artigo 24.º, n.º 1-C, do Regulamento (UE) 910/2014 constam do anexo do presente regulamento.

Artigo 2.º

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

([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

Norma de referência para a verificação da identidade e dos atributos das pessoas a quem deve ser emitido um certificado qualificado ou um certificado eletrónico qualificado de atributos

Aplica-se a norma ETSI TS 119 461 V2.1.1 (2025-02) para efeitos de conformidade com a cláusula C.3 do anexo C, 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).

2) C.3 Casos de utilização para a emissão de certificados qualificados ou certificados eletrónicos qualificados de atributos em conformidade com os artigos 24.º, n.º 1, 24.º, n.º 1-A, e 24.º, n.º 1-B, do Regulamento (UE) n.º 910/2014

— [CONDICIONAL] QTS-C3-01: Se a verificação da identidade para um certificado qualificado ou um certificado eletrónico qualificado for efetuada juntamente com a verificação da identidade para emitir elementos de prova fidedignos, esse processo de verificação da identidade deve:

— ter sido avaliado pelos pares ou certificado por um organismo de avaliação da conformidade acreditado para cumprir um nível de garantia elevado nos termos do Regulamento (UE) n.º 910/2014, ou

— cumprir os requisitos estabelecidos nas cláusulas C3.1 a C3.6.

3) C.3.4 Caso de utilização para a prova de identidade por outros meios de identificação

— QTS-C.3.4-06A: o organismo independente de avaliação da conformidade referido no [CONDICIONAL] QTS-C.3.4-06, alínea c), deve ser acreditado nos termos do artigo 3.º, n.º 18, do Regulamento (UE) n.º 910/2014 e, se todos os requisitos aplicáveis estiverem preenchidos, a avaliação deve resultar num certificado de conformidade baseado numa auditoria de certificação. Este processo de certificação formal baseia-se num processo de avaliação da segurança que remete para os níveis de garantia definidos para os meios de identificação eletrónica notificados ou as carteiras europeias de identidade digital certificadas ao abrigo do Regulamento (UE) n.º 910/2014 e inclui testes rigorosos para avaliar a resistência contra potenciais ameaças à segurança. Estas avaliações devem utilizar normas técnicas pertinentes para demonstrar a robustez face a tais ataques.

4) 9.2.3.4 Caso de utilização para operações automatizadas

— USE-9.2.3.4-04: o prestador de serviços de prova de identidade estabelece valores-alvo para a taxa de falsa aceitação e a taxa de falsa rejeição, com base numa análise de risco e no seu procedimento de informação sobre ameaças, seguindo a metodologia estabelecida no relatório da ENISA intitulado *Methodology for sectoral cybersecurity assessments* (Metodologia para as avaliações setoriais da cibersegurança) [i.28] ou uma metodologia equivalente, em processos de prova da identidade totalmente automatizados. Estes valores-alvo devem ser iguais ou inferiores aos estabelecidos para os casos de utilização híbrida, se existentes. O prestador de serviços de prova de identidade deve manter sistematicamente estes valores-alvo para taxa de falsa aceitação e a taxa de falsa rejeição, com base numa análise de risco e no seu procedimento de informação sobre ameaças.

5) 8.3.3 Validação de documento de identidade físico

— VAL-8.3.3-21: a eficácia das medidas para cumprir os requisitos VAL-8.3.3-05X, VAL-8.3.3-05A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07A e VAL-8.3.3-07X deve ser testada por um laboratório acreditado ou por uma autoridade nacional competente, se designada, o mais tardar até 19 de agosto de 2027 e, posteriormente, de dois em dois anos.

6) 7.12 Cessação e planos de cessação

— OVR-7.12-02: o plano de cessação 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].