Jornal Oficial
da União Europeia

PT
Série L

2025/1944

30.9.2025

REGULAMENTO DE EXECUÇÃO (UE) 2025/1944 DA COMISSÃO

de 29 de setembro 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 os processos de envio e receção de dados nos serviços qualificados de envio registado eletrónico e no respeitante à interoperabilidade desses serviços

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 44.º, n.ºs 2 e 2-B,

Considerando o seguinte:

(1) Os serviços qualificados de envio registado eletrónico proporcionam um canal seguro para a transmissão de documentos, incluindo a prova de envio e receção de dados. Visam fornecer segurança na identificação do destinatário e manter um elevado nível de confiança na identificação do remetente.

(2) A presunção de conformidade estabelecida no artigo 44.º, n.º 1-A, do Regulamento (UE) n.º 910/2014 só deve aplicar-se quando os serviços de confiança qualificados para o fornecimento de serviços qualificados de envio registado eletrónico cumprirem as normas estabelecidas no presente regulamento. 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.

(3) Se um prestador de serviços de confiança cumprir os requisitos estabelecidos no anexo I do 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.

(4) Nos termos do artigo 44.º, n.º 2-A, do Regulamento (UE) n.º 910/2014, sempre que os prestadores qualificados de serviços de confiança acordarem em tornar os seus serviços interoperáveis, é importante que respeitem as normas e especificações adequadas estabelecidas no anexo II do presente regulamento de execução, a fim de transferir facilmente os dados registados por via eletrónica entre dois ou mais prestadores qualificados de serviços de confiança e de promover práticas leais no mercado interno.

(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]) aplicam-se a todas as 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 para serviços qualificados de envio registado eletrónico

As normas de referência e especificações a que se refere o artigo 44.º, n.º 2, do Regulamento (UE) 910/2014 constam do anexo I do presente regulamento.

Artigo 2.º

Normas de referência e especificações para a interoperabilidade entre serviços qualificados de envio registado eletrónico

As normas de referência e especificações a que se refere o artigo 44.º, n.º 2-B, do Regulamento (UE) 910/2014 constam do anexo II do presente regulamento.

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 29 de setembro 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 I

Lista das normas de referência e especificações a que se refere o artigo 1.º

Aplica-se a norma ETSI EN 319 521 V1.1.1 (2019-02) («ETSI EN 319 521»), com as seguintes adaptações:

1) Para a norma ETSI EN 319 521

1) 2.1 Referências normativas

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

— [2] ETSI EN 319 411-1 V1.5.1 (2025-04) «Eletrónica Signatures and Trust Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements» [Assinaturas eletrónicas e infraestruturas de confiança (ESI); requisitos de política e segurança para os prestadores de serviços de confiança que emitem certificados; parte 1: requisitos gerais].

— [3] ETSI EN 319 522-1 V1.2.1 (2024-01) «Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 1: Framework and Architecture» [Assinaturas eletrónicas e infraestruturas (ESI); serviços de envio registado eletrónico; parte 1: regime e arquitetura].

— [4] ETSI EN 319 522-2 V1.2.1 (2024-01) «Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic content» [Assinaturas eletrónicas e infraestruturas (ESI); serviços de envio registado eletrónico; parte 2: conteúdo semântico].

— [5] 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]).

— [6] ISO/IEC 15408-1:2022 — «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).

— [7] Regulamento de Execução (UE) 2024/482 da Comissão ([2]), 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).

— [8] Regulamento de Execução (UE) 2024/3144 ([3]) da Comissão, que altera o Regulamento de Execução (UE) 2024/482 no respeitante às normas internacionais aplicáveis e que retifica esse regulamento de execução.

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

2) 3.1 Termos

— Selo eletrónico avançado: na aceção do Regulamento (UE) n.º 910/2014 [i.1].

— Assinatura eletrónica avançada: na aceção do Regulamento (UE) n.º 910/2014 [i.1].

— Selo eletrónico qualificado: na aceção do Regulamento (UE) n.º 910/2014 [i.1].

— Assinatura eletrónica qualificada: na aceção do Regulamento (UE) n.º 910/2014 [i.1].

— 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.

([1]) https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en.
([2]) JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj..
([3]) JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj.

3) 5.1.1 Disposições comuns

— REQ-ERDS-5.1.1-01 O serviço de envio registado eletrónico (ERDS) deve assegurar que a disponibilidade, a integridade e a confidencialidade do conteúdo do utente estão devidamente garantidas enquanto este é tratado pelo ERDS, selecionando técnicas criptográficas adequadas de integridade e confidencialidade em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [5].

4) 5.2.1.1 Observações gerais

— REQ-QERDS-5.2.1.1-01 O prestador de serviços qualificados de envio registado eletrónico (QERDSP) deve verificar, com um nível de confiança muito elevado, a identidade do destinatário, quer diretamente quer recorrendo a um terceiro, utilizando um dos seguintes meios ou uma combinação dos mesmos, conforme necessário:

a) Pela presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, através de elementos de prova e procedimentos adequados, em conformidade com o direito nacional;

b) À distância, utilizando um meio de identificação eletrónica que cumpra os requisitos estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 [i.1] no que diz respeito ao nível de garantia «elevado», ou através da carteira europeia de identidade digital;

c) Por meio de um certificado de assinatura eletrónica qualificada ou de selo eletrónico qualificado;

d) Utilizando outros métodos de identificação que garantam que a pessoa singular ou o representante autorizado da pessoa coletiva possa ser identificado com um nível de confiança muito elevado. A garantia de que esta identificação é efetuada com um nível de confiança muito elevado deve ser confirmada por um organismo de avaliação da conformidade.

— REQ-QERDS-5.2.1.1-01A O QERDSP deve verificar a identidade do remetente pelos meios adequados, quer diretamente quer recorrendo a um terceiro, utilizando um dos seguintes meios ou uma combinação dos mesmos:

a) Pela presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, através de elementos de prova e procedimentos adequados, em conformidade com o direito nacional;

b) À distância, utilizando a carteira europeia de identidade digital ou um meio de identificação eletrónica notificado que cumpra os requisitos estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 [i.1] no que diz respeito ao nível de garantia «substancial», desde que tenha sido emitido mediante a presença física da pessoa singular ou de um representante autorizado da pessoa coletiva;

c) Através de um certificado de assinatura eletrónica avançada ou de selo eletrónico avançado, desde que o certificado tenha sido emitido à pessoa singular ou a um representante autorizado da pessoa coletiva ao abrigo da política de certificação normalizada (NCP), tal como definido na norma ETSI EN 319 411-1 [2]; ou

d) Utilizando outros métodos de identificação que garantam que a pessoa singular ou o representante autorizado da pessoa coletiva possa ser identificado com um nível de confiança muito elevado. A garantia de que esta identificação é efetuada com um nível de confiança elevado deve ser confirmada por um organismo de avaliação da conformidade.

— NOTA O terceiro que verifica a identidade do remetente e do destinatário pode ser outro QERDSP se o remetente e o destinatário forem assinantes de diferentes QERDSP.

5) 5.2.1.2 Identificação do destinatário e transmissão do conteúdo do utente

— REQ-QERDS-5.2.1.2-03 Se a identificação do destinatário se basear num processo interno do QERDS, o QERDSP deve conduzir todo o processo num ambiente seguro e controlado.

6) 5.2.2 Disposições relativas à autenticação EU QERDS

— REQ-QERDS-5.2.2-03 [CONDICIONAL] Quando o QERDSP vincula meios de autenticação a uma identidade do remetente verificada em conformidade com a cláusula 5.2.1, estes devem ser um dos seguintes:

a) Mecanismos de autenticação de dois fatores;

b) Uma carteira europeia de identidade digital ou um meio de identificação eletrónica notificado que cumpra os requisitos estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 [i.1] no que diz respeito ao nível de garantia «elevado» ou «substancial»;

c) Uma autenticação de segurança da camada de transporte (TLS) mútua, que inclua o certificado emitido ao remetente ao abrigo da NCP, tal como definido na norma ETSI EN 319 411-1 [2];

d) Uma assinatura digital apoiada por um certificado emitido ao abrigo da NCP, tal como definido na norma ETSI EN 319 411-1 [2];

e) Outros meios que assegurem a autenticação do remetente identificado. A conformidade de tais vinculações deve ser confirmada por um organismo de avaliação da conformidade. Exemplo: tal pode incluir a utilização de um dos meios acima referidos nas alíneas a), b) e d) para registar um certificado de cliente de TLS para envio automatizado através da TLS mútua ou para registar um certificado de selo digital utilizado para selar afirmações de autenticação no ERDS. Podem igualmente aplicar-se outros mecanismos em que os remetentes identificados recorrem a serviços delegados de terceiros.

— REQ-QERDS-5.2.2-03A [CONDICIONAL] Quando o QERDSP vincula meios de autenticação a uma identidade do destinatário verificada em conformidade com a cláusula 5.2.1, estes devem ser um dos seguintes, desde que esses meios, ou qualquer combinação de meios, garantam um nível de confiança muito elevado no que respeita à identidade do destinatário autenticado:

a) Um mecanismo de autenticação multifatores;

b) Uma carteira europeia de identidade digital ou um meio de identificação eletrónica notificado que cumpra os requisitos estabelecidos no artigo 8.º do Regulamento (UE) n.º 910/2014 [i.1] no que diz respeito ao nível de garantia «elevado» ou «substancial»;

c) Um certificado de assinatura eletrónica qualificada ou de selo eletrónico qualificado;

d) Outros meios que assegurem a autenticação do destinatário identificado. A conformidade de tais vinculações deve ser confirmada por um organismo de avaliação da conformidade. Exemplo: tal pode incluir a utilização de um dos meios acima referidos nas alíneas a) a c), para registar um certificado de cliente de TLS para envio automatizado através da TLS mútua ou para registar um certificado de selo digital utilizado para selar afirmações de autenticação no ERDS. Podem igualmente aplicar-se outros mecanismos em que os remetentes identificados recorrem a serviços delegados de terceiros.

— REQ-QERDS-5.2.2-04 [CONDICIONAL] Caso o remetente se ligue ao QERDS através de uma ligação segura que exija autenticação mútua máquina-máquina entre a máquina do remetente e o servidor do QERDS com base em certificados emitidos de acordo com a NCP, tal como definido na norma ETSI EN 319 411-1 [2], após o estabelecimento da ligação segura, podem ser adotados mecanismos de autenticação de fator único para uma segunda fase de autenticação do remetente, se os procedimentos organizacionais e as medidas de segurança aplicadas garantirem confiança na autenticação do remetente.

7) 5.4.1 Disposições comuns

— REQ-ERDS-5.4.1-06 O ERDS gera e disponibiliza às partes interessadas legítimas elementos de prova do ERDS sobre eventos de envio registado eletrónico (ERD), tal como definido na cláusula 6 da norma ETSI EN 319 522-1 [3].

— REQ-ERDS-5.4.1-07 O ERDSP arquiva os elementos de prova e/ou as sínteses dos elementos de prova para cada elemento que tenha emitido.

— REQ-ERDS-5.4.1-08 Os elementos de prova do ERDS gerados pelo ERDS devem estar em conformidade com a semântica dos elementos de prova definida na cláusula 8 da norma ETSI EN 319 522-2 [4].

8) 7.2.1 Disposições comuns

— REQ-ERDS-7.2.1-02 O pessoal do ERDSP 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.

— REQ-ERDS-7.2.1-03 A conformidade com o REQ-ERDS-7.2.1-02 deve incluir atualizações regulares (pelo menos a cada 12 meses) sobre as novas ameaças e as atuais práticas de segurança.

9) 7.3.2 Manipulação dos suportes

— REQ-ERDS-7.3.1-02 Aplicam-se todos os requisitos especificados na norma ETSI EN 319 401 [1], cláusula 7.3.3.

10) 7.5 Controlos criptográficos

— REQ-ERDS-7.5-01A O ERDS 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 [5].

— REQ-ERDSP-7.5-03 A chave privada de assinatura do ERDS deve ser conservada e utilizada 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 [6] ou nos Critérios Comuns para a Avaliação da Segurança das Tecnologias da Informação, versão CC:2002, 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 (EUCC) [7] [8] e certificado com o nível EAL 4 ou superior; ou

c) Até 31.12.2030, FIPS PUB 140-3 [9] 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 [7] [8], esse dispositivo deve ser configurado e utilizado em conformidade com essa certificação.

11) 7.8 Segurança da rede

— REQ-ERDSP-7.8-04 O ERDSP deve utilizar protocolos e algoritmos sofisticados para encriptação ao nível da camada do transporte em conformidade com os mecanismos criptográficos acordados, aprovados pelo Grupo Europeu para a Certificação da Cibersegurança e publicados pela ENISA [5].

— REQ-ERDSP-7.8-06 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.

— REQ-ERDSP-7.8-07 O teste de penetração solicitado pelo REQ-7.8-17X da norma ETSI EN 319 401 [1] deve ser efetuado pelo menos uma vez por ano.

— REQ-ERDSP-7.8-08 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 (TSP).

12) 7.12 Cessação do ERDSP e planos de cessação do ERDS

— REQ-ERDS-7.12-03 O plano de cessação do ERDSP 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].

13) 7.14 Cadeia de abastecimento

— REQ-ERDS-7.14-01 Aplicam-se os requisitos especificados na norma ETSI EN 319 401 [1], cláusula 7.14.

ANEXO II

Lista das normas de referência e especificações a que se refere o artigo 2.º

Aplicam-se as normas ETSI EN 319 522-1 V1.2.1 (2024-01) («ETSI EN 319 522-1»), ETSI EN 319 522-2 V1.2.1 (2024-01) («ETSI EN 319 522-2»), ETSI EN 319 522-3 V1.2.1 (2024-01) («ETSI EN 319 522-3»), ETSI EN 319 522-4-1 V1.2.1 (2019-01) («ETSI EN 319 522-4-1»), ETSI EN 319 522-4-2 V1.1.1 (2018-09) («ETSI EN 319 522-4-2») e ETSI EN 319 522--4-3 V1.1.1 (2018-09) («ETSI EN 319 522-4-3»).