

Este texto constitui um instrumento de documentação e não tem qualquer efeito jurídico. As Instituições da União não assumem qualquer responsabilidade pelo respetivo conteúdo. As versões dos atos relevantes que fazem fé, incluindo os respetivos preâmbulos, são as publicadas no Jornal Oficial da União Europeia e encontram-se disponíveis no EUR-Lex. É possível aceder diretamente a esses textos oficiais através das ligações incluídas no presente documento.

**►B 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**

(JO L 257 de 28.8.2014, p. 73)

Alterado por:

		Jornal Oficial			
		n.º	página	data	
<b>►M1</b>	Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022	L 333	80	27.12.2022	
<b>►M2</b>	Regulamento (UE) 2024/1183 do Parlamento Europeu e do Conselho de 11 de abril de 2024	L 1183	1	30.4.2024	

Retificado por:

- C1** Retificação, JO L 90317 de 9.4.2025, p. 1 (2024/1183)

**▼B****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**

**CAPÍTULO I****DISPOSIÇÕES GERAIS****▼M2***Artigo 1.º***Objeto**

O presente regulamento visa assegurar o bom funcionamento do mercado interno e a disponibilização de um nível adequado de segurança dos meios de identificação eletrónica e dos serviços de confiança utilizados em toda a União, a fim de permitir e facilitar o exercício, por pessoas singulares e coletivas, do direito de participar na sociedade digital em segurança e de aceder aos serviços públicos e privados em linha em toda a União. Para o efeito, o presente regulamento:

- a) Estabelece as condições em que os Estados-Membros devem reconhecer os meios de identificação eletrónica de pessoas singulares e coletivas abrangidas por um sistema de identificação eletrónica notificado de outro Estado-Membro e fornecer e reconhecer carteiras europeias de identidade digital;
- b) Estabelece normas aplicáveis aos serviços de confiança, nomeadamente às transações eletrónicas;
- c) Estabelece um regime jurídico para as assinaturas eletrónicas, os selos eletrónicos, os selos temporais eletrónicos, os documentos eletrónicos, os serviços de envio registado eletrónico, os serviços de certificados para autenticação de sítios Web, o arquivo eletrónico, o certificado eletrónico de atributos, dispositivos de criação de assinaturas eletrónicas, dispositivos de criação de selos eletrónicos, e os livros-razão eletrónicos.

**▼B***Artigo 2.º***Âmbito de aplicação****▼M2**

1. O presente regulamento aplica-se aos sistemas de identificação eletrónica notificados pelos Estados-Membros, às carteiras europeias de identidade digital fornecidas por um Estado-Membro e aos prestadores de serviços de confiança estabelecidos na União.

**▼B**

2. O presente regulamento não se aplica à oferta de serviços de confiança utilizados exclusivamente dentro de sistemas fechados que decorram da legislação nacional ou de acordos entre um grupo definido de participantes.

**▼M2**

3. O presente regulamento não prejudica o direito da União ou nacional em matéria de celebração e validade de contratos, outras obrigações legais ou de natureza processual relacionadas com a forma ou requisitos setoriais específicos relativos à forma.

**▼M2**

4. O presente regulamento não prejudica o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho <sup>(1)</sup>.

**▼B**

*Artigo 3.º*

**Definições**

Para efeitos do presente regulamento, entende-se por:

**▼M2**

- 1) «Identificação eletrónica»: o processo de utilização dos dados de identificação pessoal em formato eletrónico que representem de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente outra pessoa singular ou uma pessoa coletiva;
- 2) «Meio de identificação eletrónica»: uma unidade material e/ou imaterial, que contenha os dados de identificação pessoal e que é utilizada para autenticação para um serviço em linha ou, se for caso disso, um serviço fora de linha;
- 3) «Dados de identificação pessoal»: um conjunto de dados que é emitido de acordo com o direito da União ou nacional e que permite determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente outra pessoa singular ou uma pessoa coletiva;
- 4) «Sistema de identificação eletrónica»: um sistema de identificação eletrónica ao abrigo do qual sejam emitidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem outras pessoas singulares ou pessoas coletivas;
- 5) «Autenticação»: o processo eletrónico que permite a confirmação da identificação eletrónica de uma pessoa singular ou coletiva ou a confirmação da origem e integridade de dados em formato eletrónico;
- 5-A) «Utente»: uma pessoa singular ou coletiva, ou uma pessoa singular que represente outra pessoa singular ou uma pessoa coletiva, que utiliza serviços de confiança ou meios de identificação eletrónica, prestados em conformidade com o presente regulamento;
- 6) «Utilizador»: uma pessoa singular ou coletiva que recorre à identificação eletrónica, às carteiras europeias de identidade digital ou a outros meios de identificação eletrónica, ou a um serviço de confiança;
- 7) «Organismo público»: uma entidade estatal nacional, regional ou local, um organismo de direito público ou uma associação formada por uma ou mais dessas entidades ou por um ou mais organismos de direito público, ou uma entidade privada mandatada por, pelo menos, uma dessas autoridades, organismos ou associações como sendo de interesse público, ao abrigo de tal mandato;

<sup>(1)</sup> 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).

**▼B**

- 8) «Organismo de direito público»: o organismo definido no artigo 2.º, n.º 1, ponto 4), da Diretiva 2014/24/UE do Parlamento Europeu e do Conselho <sup>(1)</sup>;
- 9) «Signatário»: a pessoa singular que cria uma assinatura eletrónica;
- 10) «Assinatura eletrónica»: os dados em formato eletrónico que se ligam ou estão logicamente associados a outros dados em formato eletrónico e que sejam utilizados pelo signatário para assinar;
- 11) «Assinatura eletrónica avançada»: uma assinatura eletrónica que obedeça aos requisitos estabelecidos no artigo 26.º;
- 12) «Assinatura eletrónica qualificada»: uma assinatura eletrónica avançada criada por um dispositivo qualificado de criação de assinaturas eletrónicas e que se baseie num certificado qualificado de assinatura eletrónica;
- 13) «Dados para a criação de uma assinatura eletrónica»: o conjunto único de dados que é utilizado pelo signatário para criar uma assinatura eletrónica;
- 14) «Certificado de assinatura eletrónica»: um atestado eletrónico que associa os dados de validação da assinatura eletrónica a uma pessoa singular e confirma, pelo menos, o seu nome ou pseudónimo;
- 15) «Certificado qualificado de assinatura eletrónica»: um certificado de assinatura eletrónica, que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I;

**▼M2**

- 16) «Serviço de confiança»: um serviço eletrónico geralmente prestado mediante remuneração, que consista num dos seguintes:
  - a) Na emissão de certificados de assinaturas eletrónicas, certificados de selos eletrónicos, certificados de autenticação de sítios Web ou certificados para a prestação de outros serviços de confiança;
  - b) Na validação de certificados de assinaturas eletrónicas, certificados de selos eletrónicos, certificados de autenticação de sítios Web ou certificados para a prestação de outros serviços de confiança;
  - c) Na criação de assinaturas eletrónicas ou de selos eletrónicos;
  - d) Na validação de assinaturas eletrónicas ou de selos eletrónicos;
  - e) Na conservação de assinaturas eletrónicas, de selos eletrónicos, de certificados de assinaturas eletrónicas ou de certificados de selos eletrónicos;
  - f) Na gestão de dispositivos de criação de assinaturas eletrónicas à distância ou dispositivos de criação de selos eletrónicos à distância;
  - g) Na emissão de certificados eletrónicos de atributos;
  - h) Na validação de certificados eletrónicos de atributos;

<sup>(1)</sup> Diretiva 2014/24/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa aos contratos públicos e que revoga a Diretiva 2004/18/CE (JO L 94 de 28.3.2014, p. 65).

**▼M2**

- i) Na criação de selos temporais eletrónicos;
- j) Na validação de selos temporais eletrónicos;
- k) Na prestação de serviços de envio registado eletrónico;
- l) Na validação dos dados transmitidos através de serviços de envio registado eletrónico e comprovativos conexos;
- m) No arquivo eletrónico de dados eletrónicos e de documentos eletrónicos;
- n) No registo de dados eletrónicos num livro-razão eletrónico;

**▼B**

- 17) «Serviço de confiança qualificado»: um serviço de confiança que satisfaça os requisitos aplicáveis estabelecidos no presente regulamento;

**▼M2**

- 18) «Organismo de avaliação da conformidade»: um organismo de avaliação da conformidade na aceção do artigo 2.º, ponto 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para efetuar a avaliação da conformidade de um prestador qualificado de serviços de confiança e dos serviços de confiança qualificados que aquele presta, ou como sendo competente para proceder à certificação de carteiras europeias de identidade digital ou de meios de identificação eletrónica;

**▼B**

- 19) «Prestador de serviços de confiança»: a pessoa singular ou coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança;
- 20) «Prestador qualificado de serviços de confiança»: o prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela entidade supervisora;

**▼M2**

- 21) «Produto»: equipamento informático ou software, ou componentes pertinentes de equipamento informático ou software, que se destinam a ser utilizados para a prestação de serviços de identificação eletrónica e de serviços de confiança;

**▼B**

- 22) «Dispositivo de criação de assinaturas eletrónicas»: *software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas;
- 23) «Dispositivo qualificado de criação de assinaturas eletrónicas»: o dispositivo para a criação de assinaturas eletrónicas que cumpra os requisitos estabelecidos no anexo II;

**▼M2**

- 23-A) «Dispositivo qualificado de criação de assinaturas eletrónicas à distância»: um dispositivo qualificado de criação de assinaturas eletrónicas gerido por um prestador qualificado de serviços de confiança nos termos do artigo 29.º-A em nome de um signatário;

**▼M2**

- 23-B) «Dispositivo qualificado de criação de selos eletrónicos à distância»: um dispositivo qualificado de criação de selos eletrónicos gerido por um prestador qualificado de serviços de confiança nos termos do artigo 39.<sup>º</sup>-A em nome de um criador de selos;

**▼B**

- 24) «Criador de um selo»: a pessoa coletiva que cria um selo eletrónico;
- 25) «Selo eletrónico»: os dados em formato eletrónico apenso ou logicamente associado a outros dados em formato eletrónico para garantir a origem e a integridade destes últimos;
- 26) «Selo eletrónico avançado»: um selo eletrónico que obedeça aos requisitos estabelecidos no artigo 36.<sup>º</sup>:
- 27) «Selo eletrónico qualificado»: selo eletrónico avançado criado por um dispositivo qualificado de criação de selos eletrónicos e que se baseie num certificado qualificado de selo eletrónico;
- 28) «Dados para a criação de um selo eletrónico»: o conjunto único de dados que seja utilizado pelo criador do selo eletrónico para criar um selo eletrónico;
- 29) «Certificado de selo eletrónico»: um atestado eletrónico que associa os dados de validação do selo eletrónico a uma pessoa coletiva e confirma o seu nome;
- 30) «Certificado qualificado de selo eletrónico»: um certificado de selo eletrónico emitido por um prestador qualificado de serviços de confiança que satisfaça os requisitos estabelecidos no anexo III;
- 31) «Dispositivo de criação de selos eletrónicos»: *software* ou *hardware* configurados, utilizados para criar selos eletrónicos;
- 32) «Dispositivo qualificado de criação de selos eletrónicos»: um dispositivo para a criação de selos eletrónicos que satisfaça *mutatis mutandis* os requisitos estabelecidos no anexo II;
- 33) «Selos temporais»: os dados em formato eletrónico que vinculam outros dados em formato eletrónico a uma hora específica, criando uma prova de que esses outros dados existiam nesse momento;
- 34) «Selo temporal qualificado»: um selo temporal que satisfaça os requisitos estabelecidos no artigo 42.<sup>º</sup>;
- 35) «Documento eletrónico»: qualquer conteúdo armazenado em formato eletrónico, nomeadamente texto ou gravação sonora, visual ou audiovisual;
- 36) «Serviço de envio registado eletrónico»: um serviço que torne possível a transmissão de dados entre terceiros por meios eletrónicos e forneça prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que proteja os dados transferidos contra o risco de perda, roubo, dano ou alteração não autorizada;

**▼B**

- 37) «Serviço qualificado de envio registado eletrónico»: um serviço de envio registado eletrónico que satisfaça os requisitos estabelecidos no artigo 44.º;

**▼M2**

- 38) «Certificado de autenticação de sítios Web»: um atestado eletrónico que torne possível autenticar um sítio Web e associe o sítio Web à pessoa singular ou coletiva à qual o certificado tenha sido emitido;

**▼B**

- 39) «Certificado qualificado de autenticação de sítios web»: um certificado de autenticação de sítios *web* que seja emitido por um prestador de serviços de confiança e satisfaça os requisitos estabelecidos no anexo I;
- 40) «Dados de validação»: dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico;

**▼M2**

- 41) «Validação»: o processo pelo qual é verificada e confirmada a validade dos dados em formato eletrónico em conformidade com o presente regulamento;
- 42) «Carteira europeia de identidade digital»: um meio de identificação eletrónica que permite ao utente armazenar, gerir e validar de forma segura dados de identificação pessoal e certificados eletrónicos de atributos, com o objetivo de os fornecer aos utilizadores e a outros utentes de carteiras europeias de identidade digital, e assinar com assinatura eletrónica qualificada e apor selos com selos eletrónicos qualificados;
- 43) «Atributo»: uma característica, qualidade, direito ou autorização de uma pessoa singular ou coletiva ou de um objeto;
- 44) «Certificado eletrónico de atributos»: um certificado em formato eletrónico que permite a autenticação de atributos;
- 45) «Certificado eletrónico qualificado de atributos»: um certificado eletrónico de atributos que é emitido por um prestador qualificado de serviços de confiança e satisfaz os requisitos estabelecidos no anexo V;
- 46) «Certificado eletrónico de atributos emitido por um organismo do setor público responsável por uma fonte autêntica, ou em seu nome»: um certificado eletrónico de atributos emitido por um organismo do setor público responsável por uma fonte autêntica ou por um organismo do setor público designado pelo Estado-Membro para emitir tais certificados de atributos em nome dos organismos do setor público responsáveis pelas fontes autênticas, em conformidade com o artigo 45.º-F e o anexo VII;
- 47) «Fonte autêntica»: um repositório ou sistema, sob a responsabilidade de um organismo do setor público ou de uma entidade privada, que contém e fornece atributos relativos a uma pessoa singular ou coletiva ou a um objeto e é considerado uma fonte principal dessa informação ou reconhecido como autêntico de acordo com o direito da União ou nacional, incluindo a prática administrativa;

**▼M2**

- 48) «Arquivo eletrónico»: um serviço que assegura 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 para preservar a sua integridade, confidencialidade e prova de origem durante todo o período de preservação;
- 49) «Serviço qualificado de arquivo eletrónico»: um serviço de arquivo eletrónico prestado por um prestador qualificado de serviços de confiança e que satisfaz os requisitos estabelecidos no artigo 45.º-J;
- 50) «Marca de confiança ‘UE’ para a carteira de identidade digital»: uma indicação verificável, simples e reconhecível, comunicada de forma clara, de que uma carteira europeia de identidade digital foi fornecida em conformidade com o presente regulamento;
- 51) «Autenticação forte do utente»: uma autenticação baseada em pelo menos dois fatores de autenticação pertencentes a categorias diferentes, quer de conhecimento, algo que só o utente conhece, posse, algo que só o utente possui, ou inherência, uma característica própria do utente, os quais são independentes, na medida em que a violação de um deles não compromete a fiabilidade dos outros, e que é concebida para proteger a confidencialidade dos dados de autenticação;
- 52) «Livro-razão eletrónico»: uma sequência de regtos eletrónicos de dados que assegura a integridade desses regtos e a exatidão do ordenamento cronológico desses regtos;
- 53) «Livro-razão eletrónico qualificado»: um livro-razão eletrónico fornecido por um prestador qualificado de serviços de confiança e que satisfaz os requisitos estabelecidos no artigo 45.º-L;
- 54) «Dados pessoais»: qualquer informação na aceção do artigo 4.º, ponto 1), do Regulamento (UE) 2016/679;
- 55) «Correspondência de identidade»: um processo em que os dados de identificação pessoal ou os meios de identificação eletrónicos correspondem ou são ligados a uma conta existente pertencente à mesma pessoa;
- 56) «Registo de dados»: os dados eletrónicos registados com metadados conexos que apoiam o tratamento dos dados;
- 57) «Modo fora de linha»: no que respeita às carteiras europeias de identidade digital, a interação entre um utente e um terceiro num local físico utilizando tecnologias de proximidade, sem que seja necessário que a carteira europeia de identidade digital acceda a sistemas à distância através de redes de comunicações eletrónicas para efeitos da interação.

**▼B***Artigo 4.º***Princípios relativos ao mercado interno**

1. Não podem ser impostas restrições à prestação de serviços de confiança no território dos Estados-Membros por prestadores de serviços de confiança estabelecidos noutros Estados-Membros por razões que se enquadrem nos domínios abrangidos pelo presente regulamento.

**▼B**

2. Os produtos e serviços de confiança que cumpram o disposto no presente regulamento podem circular livremente no mercado interno.

**▼M2**

*Artigo 5.<sup>º</sup>*

**Pseudónimos nas transações eletrónicas**

Sem prejuízo das regras específicas do direito da União ou nacional que exijam que os utentes se identifiquem ou dos efeitos legais conferidos aos pseudónimos nos termos das legislações nacionais, não é proibido utilizar pseudónimos escolhidos pelo utente.

**▼B**

CAPÍTULO II

**IDENTIFICAÇÃO ELETRÓNICA**

**▼M2**

*SECÇÃO 1*

*Carteira europeia de identidade digital*

*Artigo 5.<sup>º</sup>-A*

**Carteiras europeias de identidade digital**

1. A fim de assegurar que todas as pessoas singulares e coletivas na União dispõem de acesso além-fronteiras seguro, contínuo e de confiança a serviços públicos e privados, mantendo simultaneamente pleno controlo sobre os seus dados, cada Estado-Membro fornece pelo menos uma carteira europeia de identidade digital no prazo de 24 meses a contar da data de entrada em vigor dos atos de execução a que se referem o n.<sup>º</sup> 23 do presente artigo e o artigo 5.<sup>º</sup>-C, n.<sup>º</sup> 6.

2. As carteiras europeias de identidade digital são fornecidas de uma ou várias das seguintes formas:

- a) Diretamente por um Estado-Membro;
- b) Por mandato de um Estado-Membro;
- c) De forma independente de um Estado-Membro, mas reconhecida por esse Estado-Membro.

3. O código-fonte dos componentes de *software* de aplicação das carteiras europeias de identidade digital é objeto de licença de fonte aberta. Os Estados-Membros podem prever que, por razões devidamente justificadas, o código-fonte de componentes específicos que não sejam os instalados nos dispositivos dos utentes não seja divulgado.

4. As carteiras europeias de identidade digital permitem ao utente, de uma forma que seja de fácil utilização, transparente e rastreável pelo utilizador:

- a) Solicitar, obter, selecionar, combinar, armazenar, apagar, partilhar e apresentar de forma segura, sob o controlo exclusivo do utente, dados de identificação pessoal e, se for caso disso, em combinação com certificados eletrónicos de atributos, autenticar-se em linha aos utilizadores e, se for caso disso, em modo fora de linha, a fim de aceder a serviços públicos e privados, assegurando simultaneamente a possibilidade de divulgação seletiva de dados;

**▼M2**

- b) Gerar pseudónimos e armazená-los de forma cifrada e localmente na carteira europeia de identidade digital;
- c) Autenticar de forma segura a carteira europeia de identidade digital de outra pessoa e receber e partilhar dados de identificação pessoal e certificados eletrónicos de atributos de forma segura entre as duas carteiras europeias de identidade digital;
- d) Aceder a um registo de todas as transações realizadas através da carteira europeia de identidade digital, recorrendo a um painel de controlo comum que permita ao utente:
  - i) visualizar uma lista atualizada dos utilizadores com as quais o utente estabeleceu uma ligação e, se for caso disso, todos os dados trocados,
  - ii) solicitar facilmente o apagamento de dados pessoais por parte de um utilizador, nos termos do artigo 17.º do Regulamento (UE) 2016/679,
  - iii) Denunciar facilmente um utilizador à autoridade nacional responsável pela proteção em caso de receção de um pedido de dados alegadamente ilegal ou suspeito;
- e) Assinar com assinaturas eletrónicas qualificadas ou apor selos com selos eletrónicos qualificados;
- f) Descarregar, na medida em que tal seja tecnicamente viável, os dados do utente, o certificado eletrónico de atributos e as configurações;
- g) Exercer os direitos do utente à portabilidade dos dados.

## 5. Em especial, as carteiras europeias de identidade digital:

- a) Apoiam protocolos e interfaces comuns:
  - i) para a emissão de dados de identificação pessoal, certificados eletrónicos qualificados e não qualificados de atributos ou certificados qualificados e não qualificados para a carteira europeia de identidade digital;
  - ii) para os utilizadores pedirem e validarem dados de identificação pessoal e certificados eletrónicos de atributos;
  - iii) para a partilhar e apresentar aos utilizadores dados de identificação pessoal ou de certificados eletrónicos de atributos ou dados conexos divulgados seletivamente em linha e, se for caso disso, em modo fora de linha;
  - iv) para o utente poder interagir com a carteira europeia de identidade digital e exibir uma «marca de confiança “UE” para a carteira de identidade digital»;
  - v) para a adesão segura do utente, utilizando um meio de identificação eletrónica, em conformidade com o artigo 5.º-A, n.º 24,
  - vi) para a interação entre as carteiras europeias de identidade digital de duas pessoas para efeitos de receção, validação e partilha de dados de identificação pessoal e certificados eletrónicos de atributos de forma segura;

**▼M2**

- vii) para autenticar e identificar os utilizadores através da aplicação de mecanismos de autenticação em conformidade com o artigo 5.º-B;
- viii) para os utilizadores verificarem a autenticidade e a validade das carteiras europeias de identidade digital;
- ix) para solicitar a um utilizador o apagamento de dados pessoais, nos termos do artigo 17.º do Regulamento (UE) 2016/679;
- x) para denunciar um utilizador à autoridade nacional responsável pela proteção de dados, em caso de receção de um pedido de dados alegadamente ilegal ou suspeito;
- xi) para a criação de assinaturas eletrónicas qualificadas ou de selos eletrónicos qualificados com dispositivos qualificados de criação de assinaturas eletrónicas ou de selos eletrónicos;
- b) Não facultam quaisquer informações aos prestadores de serviços de confiança de certificados eletrónicos de atributos sobre a utilização desses certificados eletrónicos;
- c) Asseguram que a identidade dos utilizadores possa ser autenticada e identificada através da aplicação de mecanismos de autenticação em conformidade com o artigo 5.º-B;
- d) Cumprem os requisitos estabelecidos no artigo 8.º no que diz respeito ao nível de garantia elevado, em especial à sua aplicação aos requisitos de prova e verificação da identidade, assim como à gestão e autenticação de meios de identificação eletrónica;
- e) No caso do certificado eletrónico de atributos com políticas de divulgação incorporadas, aplicam o mecanismo adequado para informar o utente de que o utilizador ou o utente da carteira europeia de identidade digital que requer esse certificado eletrónico de atributos está autorizado a aceder ao mesmo;
- f) Asseguram que os dados de identificação pessoal, disponíveis a partir do sistema de identificação eletrónica ao abrigo do qual é fornecida a carteira europeia de identidade digital, representam de modo único a pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa singular ou coletiva, e estão associados a essa carteira europeia de identidade digital;
- g) Oferecem a todas as pessoas singulares a possibilidade de assinar através de assinaturas eletrónicas qualificadas por defeito e gratuitamente.

Não obstante o disposto na alínea g) do primeiro parágrafo, os Estados-Membros podem prever medidas proporcionadas para assegurar que a utilização gratuita de assinaturas eletrónicas qualificadas por pessoas singulares se limite a fins não profissionais.

6. Os Estados-Membros informam os utentes, sem demora, de qualquer violação da segurança que possa ter comprometido total ou parcialmente a respetiva carteira europeia de identidade digital ou o seu conteúdo, em particular, se a respetiva carteira europeia de identidade digital tiver sido suspensa ou revogada, nos termos do artigo 5.º-E.

**▼M2**

7. Sem prejuízo do artigo 5.º-F, os Estados-Membros podem prever, em conformidade com o direito nacional, funcionalidades adicionais das carteiras europeias de identidade digital, incluindo a interoperabilidade com os meios nacionais de identificação eletrónica existentes. Essas funcionalidades adicionais devem cumprir o disposto no presente artigo.

8. Os Estados-Membros preveem mecanismos de validação gratuitos para:

- a) Garantir que a autenticidade e validade das carteiras europeias de identidade digital podem ser verificadas;
- b) Permitir aos utentes verificar a autenticidade e a validade da identidade dos utilizadores registados em conformidade com o artigo 5.º-B.

9. Os Estados-Membros velam por que a validade da carteira europeia de identidade digital possa ser revogada nas seguintes circunstâncias:

- a) Mediante pedido explícito do utente;
- b) Caso a segurança da carteira europeia de identidade digital tenha sido comprometida;
- c) Em caso de morte do utente ou de cessação da atividade da pessoa coletiva.

10. Os fornecedores de carteiras europeias de identidade digital asseguram que os utentes possam facilmente solicitar apoio técnico e comunicar problemas técnicos ou quaisquer outros incidentes que tenham um impacto negativo na utilização da carteira europeia de identidade digital.

11. As carteiras europeias de identidade digital são fornecidas ao abrigo de um sistema de identificação eletrónica com nível de garantia elevado.

12. As carteiras europeias de identidade digital garantem a segurança desde a conceção.

13. A emissão, uso e revogação das carteiras europeias de identidade digital são gratuitos para todas as pessoas singulares.

14. Os utentes controlam plenamente a utilização da sua carteira europeia de identidade digital e dos dados contidos na mesma. O fornecedor da carteira europeia de identidade digital não recolhe informações sobre a utilização da carteira europeia de identidade digital que não sejam necessárias para a prestação dos serviços da carteira europeia de identidade digital, nem combina os dados de identificação pessoal ou quaisquer outros dados pessoais armazenados ou relacionados com a utilização da carteira europeia de identidade digital com dados pessoais de outros serviços por si oferecidos ou de serviços de terceiros que não sejam necessários para a prestação dos serviços da carteira europeia de identidade digital, salvo pedido expresso do utilizador. Os dados pessoais relacionados com o fornecimento da carteira europeia de identidade digital são conservados logicamente separados de quaisquer outros dados detidos pelo fornecedor da carteira europeia de identidade digital. Se a carteira europeia de identidade digital for fornecida por partes privadas nos termos do n.º 2, alíneas b) e c), do presente artigo, o disposto no artigo 45.º-H, n.º 3, aplica-se *mutatis mutandis*.

**▼M2**

15. A utilização das carteiras europeias de identidade digital é voluntária. O acesso a serviços públicos e privados, o acesso ao mercado de trabalho e a liberdade de empresa não podem, de forma alguma, ser restringidos nem desfavorecer as pessoas singulares e coletivas que não utilizam a carteira europeia de identidade digital. Continua a ser possível aceder a serviços públicos e privados através de outros meios de identificação e autenticação existentes.

16. O enquadramento técnico da carteira europeia de identidade digital:

- a) Não permite que os fornecedores de certificados eletrónicos de atributos ou qualquer outra parte, após a emissão do certificado de atributos, obtenham dados que permitam que as transações ou o comportamento dos utentes sejam seguidos, ligados ou correlacionados, ou que o conhecimento das transações ou o comportamento dos utentes seja obtido de outra forma, salvo autorização explícita do próprio utente;
- b) Permite técnicas de preservação da privacidade que garantam a ausência de associação, sempre que o certificado de atributos não exija a identificação do utente.

17. Qualquer tratamento de dados pessoais efetuado pelos Estados-Membros ou, em seu nome, por organismos ou partes responsáveis pelo fornecimento das carteiras europeias de identidade digital como meio de identificação eletrónica é efetuado em conformidade com medidas adequadas e eficazes de proteção de dados. A conformidade de tais atividades de tratamento com o Regulamento (UE) 2016/679 deve ser demonstrada. Os Estados-Membros podem introduzir disposições nacionais para especificar melhor a aplicação dessas medidas.

18. Os Estados-Membros notificam à Comissão, sem demora injustificada, informações sobre:

- a) O organismo responsável pela elaboração e manutenção da lista dos utilizadores registados que recorrem às carteiras europeias de identidade digital, em conformidade com o artigo 5.º-B, n.º 5, e a localização dessa lista;
- b) Os organismos responsáveis pelo fornecimento das carteiras europeias de identidade digital, em conformidade com o artigo 5.º-A, n.º 1;
- c) Os organismos responsáveis por assegurar que os dados de identificação pessoal estão associados à carteira europeia de identidade digital, em conformidade com o artigo 5.º-A, n.º 5, alínea f);
- d) O mecanismo que permite a validação dos dados de identificação pessoal a que se refere o artigo 5.º-A, n.º 5, alínea f), e sobre a identidade dos utilizadores;
- e) O mecanismo para validar a autenticidade e a validade das carteiras europeias de identidade digital.

A Comissão disponibiliza ao público as informações notificadas nos termos do primeiro parágrafo, através de um canal seguro, num formato assinado ou selado por via eletrónica, adequado ao tratamento automático.

**▼M2**

19. Sem prejuízo do disposto no n.º 22 do presente artigo, o artigo 11.º aplica-se *mutatis mutandis* à carteira europeia de identidade digital.

20. O artigo 24.º, n.º 2, alíneas b), e, d) a h), aplica-se *mutatis mutandis* aos fornecedores de carteiras europeias de identidade digital.

21. As carteiras europeias de identidade digital são disponibilizadas para utilização por pessoas com deficiência, em condições iguais às dos restantes utentes, em conformidade com a Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho <sup>(1)</sup>.

22. Para efeitos do fornecimento de carteiras europeias de identidade digital, as carteiras europeias de identidade digital e os sistemas de identificação eletrónica ao abrigo dos quais são fornecidas não estão sujeitos aos requisitos estabelecidos nos artigos 7.º, 9.º, 10.º, 12.º e 12.º-A.

23. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para os requisitos a que se referem os n.ºs 4, 5, 8 e 18 do presente artigo sobre a implementação da carteira europeia de identidade digital. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

24. A Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos a fim de facilitar a adesão à carteira europeia de identidade digital através de meios de identificação eletrónica conformes com o nível de garantia elevado ou através de meios de identificação eletrónica conformes com o nível de garantia substancial, em conjugação com procedimentos de integração à distância adicionais que, em conjunto, cumpram os requisitos de nível de garantia elevado. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 5.º-B*

**Utilizadores de carteiras europeias de identidade digital**

1. Sempre que pretenda recorrer a carteiras europeias de identidade digital para a prestação de serviços públicos ou privados por meio da interação digital, o utilizador regista-se no Estado-Membro em que está estabelecido.

2. O processo de registo é eficaz em termos de custos e proporcional ao risco. O utilizador presta, pelo menos:

a) As informações necessárias para autenticar as carteiras europeias de identidade digital, que incluem, no mínimo:

i) o Estado-Membro em que o utilizador está estabelecido, e

<sup>(1)</sup> Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos requisitos de acessibilidade dos produtos e serviços (JO L 151 de 7.6.2019, p. 70).

**▼M2**

- ii) o nome do utilizador e, se for caso disso, o seu número de registo, tal como consta num registo oficial, juntamente com os dados de identificação desse registo oficial;
  - b) Os dados de contacto do utilizador;
  - c) A utilização prevista das carteiras europeias de identidade digital, incluindo uma indicação dos dados a solicitar aos utentes pelo utilizador.
3. Os utilizadores não podem solicitar aos utentes que forneçam quaisquer dados para além dos indicados nos termos do n.<sup>º</sup> 2, alínea c).
4. Os n.<sup>º</sup>s 1 e 2 não prejudicam as disposições do direito da União ou nacional aplicável à prestação de serviços específicos.
5. Os Estados-Membros disponibilizam ao público em linha as informações a que se refere o n.<sup>º</sup> 2, num formato assinado ou selado por via eletrónica, adequado ao tratamento automático.
6. Os utilizadores registados nos termos do presente artigo informam sem demora os Estados-Membros de qualquer alteração das informações indicadas no registo nos termos do n.<sup>º</sup> 2.
7. Os Estados-Membros preveem um mecanismo comum que permita a identificação e a autenticação dos utilizadores, tal como referido no artigo 5.<sup>º</sup>-A, n.<sup>º</sup> 5, alínea c).
8. Sempre que os utilizadores pretendam recorrer a carteiras europeias de identidade digital, identificam-se junto do utente.
9. Os utilizadores são responsáveis por executar o procedimento de autenticação e validação de dados de identificação pessoal e de certificados eletrónicos de atributos solicitados a partir de carteiras europeias de identidade digital. Os utilizadores não podem recusar a utilização de pseudónimos, se a identificação do utente não for exigida pelo direito da União ou nacional.
10. Os intermediários que atuam em nome dos utilizadores são considerados utilizadores e não podem armazenar dados sobre o conteúdo da transação.
11. Até 21 de novembro de 2024, a Comissão estabelece especificações técnicas e procedimentos para os requisitos a que se referem os n.<sup>º</sup>s 2, 5, e 6 a 9 do presente artigo, por meio de atos de execução relativos à implementação das carteiras europeias de identidade digital, como referido no artigo 5.<sup>º</sup>-A, n.<sup>º</sup> 23. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

*Artigo 5.<sup>º</sup>-C***Certificação de carteiras europeias de identidade digital**

1. A conformidade das carteiras europeias de identidade digital e do sistema de identificação eletrónica ao abrigo do qual são fornecidas com os requisitos estabelecidos no artigo 5.<sup>º</sup>-A, n.<sup>º</sup>s 4, 5 e 8, com o requisito de separação lógica estabelecido no artigo 5.<sup>º</sup>-A, n.<sup>º</sup> 14, e, se for caso disso, com as normas e especificações técnicas a que se refere o artigo 5.<sup>º</sup>-A, n.<sup>º</sup> 24, é certificada por organismos de avaliação da conformidade designados pelos Estados-Membros.

**▼M2**

2. A certificação da conformidade das carteiras europeias de identidade digital com os requisitos a que se refere o n.º 1 do presente artigo, ou partes destes, que sejam pertinentes em matéria de cibersegurança é efetuada em conformidade com os sistemas europeus de certificação de cibersegurança adotados nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho<sup>(1)</sup> e referidos nos atos de execução a que se refere o n.º 6 do presente artigo.

3. Para os requisitos a que se refere o n.º 1 do presente artigo não relacionados com a cibersegurança e, no que respeita aos requisitos a que se refere o n.º 1 do presente artigo relacionados com a cibersegurança, na medida em que os sistemas de certificação da cibersegurança a que se refere o n.º 2 do presente artigo não abrangerem, ou abrangerem apenas parcialmente, esses requisitos de cibersegurança, também para esses requisitos, os Estados-Membros estabelecem sistemas nacionais de certificação em conformidade com os requisitos estabelecidos nos atos de execução a que se refere o n.º 6 do presente artigo. Os Estados-Membros transmitem os seus projetos de sistemas nacionais de certificação ao Grupo de Cooperação Europeia para a Identidade Digital criado nos termos do artigo 46.º-E, n.º 1 («grupo de cooperação»). O grupo de cooperação pode emitir pareceres e recomendações.

4. A certificação nos termos do n.º 1 é válida por um período máximo de cinco anos, desde que seja realizada uma avaliação da vulnerabilidade de dois em dois anos. Quando uma vulnerabilidade for identificada e não corrigida em tempo útil após tal identificação, a certificação será cancelada.

5. O cumprimento dos requisitos estabelecidos no artigo 5.º-A do presente regulamento relativos às operações de tratamento de dados pessoais pode ser certificado nos termos do Regulamento (UE) 2016/679.

6. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para a certificação das carteiras europeias de identidade digital a que se referem os n.os 1, 2 e 3 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

7. Os Estados-Membros comunicam à Comissão o nome e o endereço dos organismos de avaliação da conformidade a que se refere o n.º 1. A Comissão disponibiliza a informação a todos os Estados-Membros.

8. A Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 47.º que estabelecem os critérios específicos a cumprir pelos organismos de avaliação da conformidade referidos no n.º 1 do presente artigo.

<sup>(1)</sup> Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

**▼M2***Artigo 5.º-D***Publicação de uma lista de carteiras europeias de identidade digital certificadas**

1. Os Estados-Membros informam a Comissão e o grupo de cooperação criado nos termos do artigo 46.º-E, n.º 1, sem demora indevida sobre as carteiras europeias de identidade digital que foram fornecidas nos termos do artigo 5.º-A e certificadas pelos organismos de avaliação da conformidade a que se refere o artigo 5.º-C, n.º 1. Informam a Comissão e o grupo de cooperação, criado nos termos do artigo 46.º-E, n.º 1, sem demora indevida se a certificação for cancelada e indicam os motivos do cancelamento.

2. Sem prejuízo do artigo 5.º-A, n.º 18, as informações prestadas pelos Estados-Membros a que se refere o n.º 1 do presente artigo incluem, pelo menos:

- a) O certificado e o relatório de avaliação da certificação da carteira europeia de identidade digital certificada;
- b) A descrição do sistema de identificação eletrónica ao abrigo do qual é fornecida a carteira europeia de identidade digital;
- c) O regime de supervisão aplicável e as informações sobre o regime de responsabilidade no que diz respeito à parte que fornece a carteira europeia de identidade digital;
- d) Os dados da autoridade ou autoridades responsáveis pelo sistema de identificação eletrónica;
- e) As disposições previstas para a suspensão ou a revogação do sistema de identificação eletrónica, da autenticação ou das partes afectadas em causa.

3. Com base nas informações recebidas nos termos do n.º 1, a Comissão elabora, publica no *Jornal Oficial da União Europeia* e mantém, num formato legível por máquina, uma lista de carteiras europeias de identidade digital certificadas.

4. Os Estados-Membros podem solicitar à Comissão que retire da lista referida no n.º 3 uma carteira europeia de identidade digital, bem como o sistema de identificação eletrónica ao abrigo do qual é fornecida.

5. Em caso de alteração das informações prestadas nos termos do n.º 1, o Estado-Membro fornece à Comissão informações atualizadas.

6. A Comissão mantém atualizada a lista a que se refere o n.º 3, publicando no *Jornal Oficial da União Europeia* as correspondentes alterações correspondentes da lista no prazo de um mês a contar da receção de um pedido nos termos do n.º 4 ou de informações atualizadas nos termos do n.º 5.

7. Até 21 de novembro de 2024, a Comissão estabelece os formatos e procedimentos aplicáveis para efeitos dos n.ºs 1, 4 e 5 do presente artigo mediante atos de execução relativos à implementação das carteiras europeias de identidade digital conforme referido no artigo 5.º-A, n.º 23. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼M2***Artigo 5.º-E***Violação da segurança das carteiras europeias de identidade digital**

1. Se as carteiras europeias de identidade digital fornecidas nos termos do artigo 5.º-A, os mecanismos de validação a que se refere o artigo 5.º-A, n.º 8, ou o sistema de identificação eletrónica ao abrigo do qual são fornecidas as carteiras europeias de identidade digital, forem violados ou ficarem parcialmente comprometidos de uma forma que afete a sua fiabilidade ou a fiabilidade das demais carteiras europeias de identidade digital, o Estado-Membro que forneceu as carteiras europeias de identidade digital suspende, sem demora indevida, o fornecimento e a utilização das carteiras europeias de identidade digital.

Sempre que a gravidade da violação ou comprometimento de segurança a que se refere o primeiro parágrafo o justifique, o Estado-Membro retira as carteiras europeias de identidade digital sem demora indevida.

O Estado-Membro informa do facto os utentes afetados, os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, os utilizadores e a Comissão.

2. Se a violação ou o comprometimento da segurança a que se refere o n.º 1, primeiro parágrafo, do presente artigo não forem corrigidos no prazo de três meses a contar da suspensão, o Estado-Membro que forneceu as carteiras europeias de identidade digital retira-as e revoga a sua validade. O Estado-Membro informa do facto os utentes afetados, os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, os utilizadores e a Comissão.

3. Caso a violação ou o comprometimento da segurança a que se refere o n.º 1, primeiro parágrafo, do presente artigo seja corrigido, o Estado-Membro fornecedor restabelece o fornecimento e a utilização das carteiras europeias de identidade digital e informa desse facto, sem demora indevida, os utentes e os utilizadores afetados, os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, e a Comissão.

4. A Comissão publica no *Jornal Oficial da União Europeia*, sem demora indevida, as correspondentes alterações da lista a que se refere o artigo 5.º-D.

5. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para as medidas a que se referem os n.ºs 1, 2 e 3 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 5.º-F***Recurso transfronteiriço às carteiras europeias de identidade digital**

1. Sempre que os Estados-Membros exigirem a identificação eletrónica e uma autenticação para aceder a um serviço em linha prestado por um organismo público, aceitam igualmente as carteiras europeias de identidade digital fornecidas em conformidade com o presente regulamento.

**▼M2**

2. Sempre que os utilizadores privados que prestam serviços, com exceção das microempresas e das pequenas empresas, na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE da Comissão <sup>(1)</sup>, forem obrigados pelo direito nacional ou da União a utilizar a autenticação forte do utente para efeitos de identificação em linha, ou sempre que a autenticação forte do utente para efeitos de identificação em linha for exigida por obrigação contratual — nomeadamente nos domínios dos transportes, da energia, dos serviços bancários, dos serviços financeiros, da segurança social, da saúde, da água potável, dos serviços postais, das infraestruturas digitais, da educação ou das telecomunicações — esses utilizadores privados aceitam também, o mais tardar 36 meses a contar da data de entrada em vigor dos atos de execução a que se referem o artigo 5.º-A, n.º 23, e o artigo 5.º-C, n.º 6, e exclusivamente a pedido voluntário do utente, as carteiras europeias de identidade digital fornecidas em conformidade com o presente regulamento.

3. Sempre que os prestadores das plataformas em linha de muito grande dimensão a que se refere o artigo 33.º do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho <sup>(2)</sup>, exigirem que a autenticação do utilizador para aceder a serviços em linha, aceitam e facilitam também a utilização de carteiras europeias de identidade digital fornecidas de acordo com o presente regulamento para a autenticação do utente, exclusivamente a pedido voluntário do utente e respeitando os dados mínimos necessários para o serviço em linha específico para o qual é exigida a autenticação.

4. Em cooperação com os Estados-Membros, a Comissão facilita a elaboração de códigos de conduta em estreita colaboração com todas as partes interessadas pertinentes, incluindo a sociedade civil, a fim de contribuir para a ampla disponibilidade e usabilidade de carteiras europeias de identidade digital abrangidas pelo âmbito de aplicação do presente regulamento, e incentiva os prestadores de serviços a concluírem a elaboração de códigos de conduta.

5. No prazo de 24 meses após a implantação das carteiras europeias de identidade digital, a Comissão avalia a procura, a disponibilidade e a usabilidade das carteiras europeias de identidade digital, tendo em conta critérios como a aceitação pelos utentes, a presença transfronteiriça de prestadores de serviços, o desenvolvimento tecnológico, a evolução dos padrões de utilização e a procura dos utentes.

**▼M2***SECÇÃO 2**Sistemas de identificação eletrónica***▼B***Artigo 6.º***Reconhecimento mútuo**

1. Quando, para aceder a um serviço em linha prestado por um organismo público de um Estado-Membro, seja exigida, ao abrigo da legislação ou nos termos da prática administrativa nacional, uma

<sup>(1)</sup> Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

<sup>(2)</sup> Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO L 277 de 27.10.2022, p. 1).

**▼B**

identificação eletrónica baseada num meio de identificação eletrónica e numa autenticação, o meio de identificação eletrónica produzido noutro Estado-Membro é reconhecido no primeiro Estado-Membro para efeitos de autenticação transfronteiriço para o referido serviço em linha, se estiverem reunidas as seguintes condições:

- a) O meio de identificação eletrónica ser produzido por um sistema de identificação eletrónica constante da lista publicada pela Comissão nos termos do artigo 9.º;
- b) O nível de garantia do meio de identificação eletrónica corresponder a um nível de garantia igual ou superior ao exigido pelo organismo público para o acesso ao serviço em linha no primeiro Estado-Membro, desde que o nível de garantia do referido meio de identificação eletrónica corresponda ao nível substancial ou elevado;
- c) O organismo público em causa utilizar o nível de garantia substancial ou elevado para conceder acesso ao referido serviço em linha.

O reconhecimento é efetuado num prazo de 12 meses após a Comissão ter publicado, a lista a que se refere a alínea a) do primeiro parágrafo.

2. O meio de identificação eletrónica produzido por um sistema de identificação eletrónica constante da lista publicada pela Comissão nos termos do artigo 9.º, e correspondente ao nível de garantia baixo, pode ser reconhecido pelos organismos públicos para efeitos de autenticação transfronteiriça para conceder acesso ao serviço prestado em linha por esses mesmos organismos.

*Artigo 7.º*

**Elegibilidade para notificação dos sistemas de identificação eletrónica**

Os sistemas de identificação eletrónica podem ser notificados nos termos do artigo 9.º, n.º 1, se estiverem reunidas todas as seguintes condições:

- a) Os meios de identificação eletrónica que integram o sistema de identificação eletrónica serem produzidos:
  - i) pelo Estado-Membro notificante,
  - ii) por mandato do Estado-Membro notificante, ou
  - iii) independentemente do Estado-Membro notificante e serem por ele reconhecidos;
- b) Os meios de identificação eletrónica que integram o sistema de identificação eletrónica poderem ser utilizados para aceder pelo menos a um serviço prestado por um organismo público que exija identificação eletrónica no Estado-Membro notificante;
- c) O sistema de identificação eletrónica e os meios de identificação eletrónica por ele produzidos preencherem os requisitos de pelo menos um dos níveis de garantia estabelecidos no ato de execução a que se refere o artigo 8.º, n.º 3;

**▼B**

- d) O Estado-Membro notificante garantir que os dados de identificação que representam de modo único a pessoa em causa são atribuídos, em conformidade com as especificações técnicas, as normas e os procedimentos para o nível de garantia pertinente definido no ato de execução a que se refere o artigo 8.º, n.º 3, à pessoa singular ou coletiva referida no artigo 3.º, ponto 1, no momento em que os meios de identificação eletrónica que integram o sistema forem produzidos;
- e) A parte que produz os meios de identificação eletrónica que integram o sistema garantir que os mesmos meios de identificação são atribuídos à pessoa singular ou coletiva a que se refere a alínea d), do presente artigo, em conformidade com as especificações técnicas, as normas e os procedimentos para o nível de garantia pertinente definido no ato de execução a que se refere o artigo 8.º, n.º 3;
- f) O Estado-Membro notificante garantir a possibilidade de autenticação em linha, para que qualquer utilizador estabelecido no território de outro Estado-Membro possa confirmar os dados de identificação recebidos em formato eletrónico.

Para os utilizadores que não sejam organismos públicos, o Estado-Membro notificante pode definir termos de acesso à referida autenticação. Este tipo de autenticação transfronteiriça é gratuito se for realizado para acesso a um serviço em linha prestado por um organismo público.

Os Estados-Membros não podem impor requisitos técnicos específicos desproporcionados aos utilizadores que pretendam executar essa autenticação, se esses requisitos impedirem ou dificultarem significativamente a interoperabilidade dos sistemas de identificação eletrónica notificados;

**▼M2**

- g) No mínimo seis meses antes da notificação prevista no artigo 9.º, n.º 1, o Estado-Membro notificante fornecer aos outros Estados-Membros para efeitos do artigo 12.º, n.º 5, uma descrição do sistema, de acordo com as modalidades processuais definidas pelos atos de execução adotados nos termos do artigo 12.º, n.º 6;

**▼B**

- h) O sistema de identificação eletrónica cumprir os requisitos definidos no ato de execução mencionado no artigo 12.º, n.º 8.

*Artigo 8.º***Níveis de garantia dos sistemas de identificação eletrónica**

1. Os sistemas de identificação eletrónica notificados nos termos do artigo 9.º, n.º 1, especificam os níveis de garantia reduzidos, substanciais e/ou elevados para os meios de identificação eletrónica neles produzidos.
2. Os níveis de garantia reduzidos, substanciais e elevados cumprem, respetivamente, os seguintes critérios:

**▼B**

- a) O nível de garantia reduzido corresponde a um meio de identificação eletrónica, no contexto de um sistema de identificação eletrónica, que confere um nível de confiança limitado relativamente à identidade declarada ou reivindicada por determinada pessoa, e que se caracteriza por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é reduzir o risco de utilização ou alteração indevida da identidade;
- b) O nível de garantia substancial corresponde a um meio de identificação eletrónica, no contexto de um sistema de identificação eletrónica, que confere um nível de confiança substancial relativamente à identidade declarada ou reivindicada por determinada pessoa, e que se caracteriza por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é reduzir substancialmente o risco de utilização ou alteração indevida da identidade;
- c) O nível de garantia elevado corresponde a um meio de identificação eletrónica, no contexto de um sistema de identificação eletrónica, que confere um nível de confiança relativamente à identidade declarada ou reivindicada por determinada pessoa mais elevado do que os meios de identificação eletrónica com o nível de garantia substancial, e que se caracteriza por referência a especificações técnicas, normas e procedimentos conexos, nomeadamente controlos técnicos, cuja finalidade é evitar a utilização ou a alteração indevida da identidade.

**▼M2**

3. Até 18 de setembro de 2015, tendo em conta as normas internacionais aplicáveis e sob reserva do n.º 2, a Comissão define, por meio de atos de execução, as especificações técnicas mínimas, as normas e os procedimentos que devem servir de referência para a especificação dos níveis de garantia reduzido, substancial e elevado para meios de identificação eletrónica.;

**▼B**

As especificações técnicas mínimas, as normas e os procedimentos são estabelecidos por referência à confiança e qualidade:

- a) Do procedimento para provar e verificar a identidade das pessoas singulares ou coletivas que requeiram a produção do meio de identificação eletrónica;
- b) Do procedimento para a produção do meio de identificação eletrónica solicitado;
- c) Do mecanismo de autenticação através do qual a pessoa singular ou coletiva utiliza o meio de identificação eletrónica para confirmar a sua identidade a um utilizador;
- d) Da entidade que produz os meios de identificação eletrónica;
- e) De qualquer outro organismo implicado no processo de requisição da produção do meio de identificação eletrónica; e
- f) Das especificações técnicas e de segurança do meio de identificação eletrónica produzido.

Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

*Artigo 9.º*

**Notificação**

1. O Estado-Membro notificante notifica à Comissão as seguintes informações e, sem atrasos indevidos, todas as eventuais alterações posteriores às mesmas:

- a) Uma descrição do sistema de identificação eletrónica, nomeadamente dos seus níveis de garantia e do produtor ou produtores dos meios de identificação eletrónica que integram o sistema;
- b) O regime de supervisão e de responsabilidade aplicáveis no que diz respeito:
  - i) à parte que produz o meio de identificação eletrónica, e
  - ii) à parte que executa o procedimento de autenticação.
- c) Os dados da autoridade ou autoridades responsáveis pelo sistema de identificação eletrónica notificado;
- d) Os dados da entidade ou entidades que gerem o registo dos dados únicos de identificação da pessoa singular ou coletiva;
- e) Uma descrição da forma como são cumpridos os requisitos definidos nos atos de execução a que se refere o artigo 12.º, n.º 8;
- f) Uma descrição da autenticação referida no artigo 7.º, alínea f);
- g) As disposições previstas para a suspensão ou a revogação do sistema de identificação eletrónica notificado, da autenticação ou das partes afetadas em causa.

**▼M2**

2. A Comissão publica, sem demora injustificada, no *Jornal Oficial da União Europeia* uma lista dos sistemas de identificação eletrónica que tenham sido notificados nos termos do n.º 1, juntamente com as informações básicas a eles respeitantes.

3. A Comissão publica no *Jornal Oficial da União Europeia* as alterações da lista referida no n.º 2 no prazo de um mês a contar da data de receção dessa notificação.

**▼B**

4. Os Estados-Membros podem solicitar à Comissão que retire da lista referida no n.º 2 os sistemas de identificação eletrónica que tenham notificado. A Comissão publica no *Jornal Oficial da União Europeia* as correspondentes alterações à lista no prazo de um mês após a receção do pedido do Estado-Membro.

**▼B**

5. A Comissão pode, por meio de atos de execução, definir as circunstâncias, os formatos e os procedimentos para a notificação ao abrigo do n.º 1. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 10.º***▼M2****Violação da segurança dos sistemas de identificação eletrónica****▼B**

1. Se o sistema de identificação eletrónica notificado nos termos do artigo 9.º, n.º 1, ou a autenticação referida no artigo 7.º, alínea f), forem violados ou parcialmente comprometidos de forma que prejudique a fiabilidade da autenticação transfronteiriça do sistema, o Estado-Membro notificante suspende ou revoga sem demora a referida autenticação ou os elementos comprometidos, informando desse facto os outros Estados-Membros e a Comissão.

2. Se a violação ou o comprometimento referidos no n.º 1 forem sanados, o Estado-Membro notificante restabelece a autenticação transfronteiriça e informa desse facto sem demora indevida os outros Estados-Membros e a Comissão.

3. Se a violação ou o comprometimento referidos no n.º 1 não forem sanados no prazo de três meses a contar da suspensão ou revogação, o Estado-Membro notificante notifica os outros Estados-Membros e a Comissão da supressão do sistema de identificação eletrónica.

A Comissão publica no *Jornal Oficial da União Europeia*, sem demora indevida, as alterações correspondentes à lista a que se refere o artigo 9.º, n.º 2.

*Artigo 11.º***Responsabilidade**

1. O Estado-Membro notificante responde pelos danos causados deliberadamente ou por negligência a qualquer pessoa singular ou coletiva por incumprimento das obrigações que lhe são impostas nos termos do artigo 7.º, alíneas d) e f), numa transação transfronteiriça.

2. A parte que produz o meio de identificação eletrónica responde pelos danos causados deliberadamente ou por negligência a qualquer pessoa singular ou coletiva pelo incumprimento da obrigação que lhe é imposta nos termos do artigo 7.º, alínea e), numa transação transfronteiriça.

3. A parte que executa o procedimento de autenticação responde pelos danos causados deliberadamente ou por negligência a qualquer pessoa singular ou coletiva por não assegurar, numa transação transfronteiriça, a correta autenticação a que se refere o artigo 7.º, alínea f).

4. Os n.ºs 1, 2 e 3 aplicam-se nos termos das disposições nacionais em matéria de responsabilidade.

**▼B**

5. Os n.os 1, 2 e 3 aplicam-se sem prejuízo da responsabilidade das partes nos termos do direito nacional, relativamente a uma transação em que sejam utilizados meios de identificação eletrónica abrangidos pelo sistema de identificação eletrónica notificado nos termos do artigo 9.º, n.º 1.

**▼M2***Artigo 11.º-A***Determinação de correspondência de identidade a nível transfronteiriço**

1. Quando atuarem como utilizadores para serviços transfronteiriços, os Estados-Membros asseguram a determinação inequívoca da correspondência de identidade das pessoas singulares que utilizam meios de identificação eletrónica notificados ou carteiras europeias de identidade digital.

2. Os Estados-Membros preveem medidas técnicas e organizativas para assegurar um elevado nível de proteção dos dados pessoais utilizados para a determinação da correspondência de identidade e para impedir a perfilagem dos utilizadores.

3. Até 21 de novembro de 2024, a Comissão estabelece uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para os requisitos a que se refere o n.º 1 do presente artigo, por meio de atos de execução. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 12.º***▼M2****Interoperabilidade****▼B**

1. Os sistemas nacionais de identificação eletrónica notificados nos termos do artigo 9.º, n.º 1 são interoperáveis.

2. Para efeitos do requisito previsto no n.º 1, é estabelecido o quadro de interoperabilidade.

3. O quadro de interoperabilidade obedece aos seguintes critérios:

- a) Procurar ser tecnologicamente neutro e não fazer discriminações em relação às soluções técnicas nacionais específicas utilizadas para a identificação eletrónica no Estado-Membro em causa;
- b) Seguir, se possível, as normas europeias e internacionais;

**▼M2**

- c) Facilitar o respeito da privacidade e da segurança, desde a conceção;

**▼B**

4. O quadro de interoperabilidade comprehende:

- a) A referência aos requisitos técnicos mínimos relacionados com os níveis de garantia previstos no artigo 8.º;

**▼B**

- b) A tabela das correspondências entre os níveis de garantia nacionais dos sistemas de identificação eletrónica notificados e os níveis de garantia previstos no artigo 8.º;
- c) A referência aos requisitos técnicos mínimos para a interoperabilidade;

**▼M2**

- d) A referência a um conjunto mínimo de dados de identificação necessários para representar de modo único uma pessoa singular ou coletiva, ou uma pessoa singular que represente outra pessoa singular ou uma pessoa coletiva, disponível a partir de sistemas de identificação eletrónica;

**▼B**

- e) As regras processuais;
- f) As disposições em matéria de resolução de litígios; e
- g) As normas comuns de segurança operacional.

**▼M2**

5. Os Estados-Membros realizam avaliações pelos pares dos sistemas de identificação eletrónica abrangidos pelo âmbito de aplicação do presente regulamento e que devem ser notificados nos termos do artigo 9.º, n.º 1, alínea a).

6. Até 18 de março de 2025, a Comissão estabelece, por meio de atos de execução, as necessárias disposições processuais para as avaliações pelos pares a que se refere o n.º 5 do presente artigo, tendo em vista promover um nível elevado de confiança e segurança, adequado ao grau de risco. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

---

8. Até 18 de setembro de 2025, para efeitos da definição das condições uniformes para o cumprimento do requisito referido no n.º 1 do presente artigo, a Comissão, sob reserva dos critérios estabelecidos no n.º 3 do presente artigo e tendo em conta os resultados da cooperação entre os Estados-Membros, adota atos de execução referentes ao quadro de interoperabilidade tal como é definido no n.º 4 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

9. Os atos de execução referidos nos n.os 7 e 8 são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼M2***Artigo 12.º-A***Certificação de sistemas de identificação eletrónica**

1. A conformidade dos sistemas de identificação eletrónica que devem ser notificados, com os requisitos de cibersegurança estabelecidos no presente regulamento, incluindo a conformidade com os requisitos pertinentes em matéria de cibersegurança estabelecidos no artigo 8.º, n.º 2, no que diz respeito aos níveis de garantia dos sistemas de identificação eletrónica, é certificada pelos organismos de avaliação da conformidade designados pelos Estados-Membros.

**▼M2**

2. A certificação nos termos do n.º 1 do presente artigo é efetuada ao abrigo de um sistema de certificação da cibersegurança pertinente nos termos do Regulamento (UE) 2019/881 ou de partes do mesmo, na medida em que o certificado de cibersegurança ou partes do mesmo abranjam esses requisitos de cibersegurança.

3. A certificação nos termos do n.º 1 é válida por um período máximo de cinco anos, desde que seja realizada, de dois em dois anos, uma avaliação da vulnerabilidade. Sempre que seja detetada uma vulnerabilidade e a mesma não seja corrigida no prazo de três meses, a certificação é cancelada.

4. Não obstante o disposto no n.º 2, os Estados-Membros podem, em conformidade com o mesmo parágrafo, solicitar ao Estado-Membro notificante informações adicionais sobre os sistemas de identificação eletrónica, ou parte dos mesmos, certificados.

5. A avaliação pelos pares dos sistemas de identificação eletrónica a que se refere o artigo 12.º, n.º 5, não se aplica aos sistemas de identificação eletrónica ou partes desses sistemas que tenham sido certificados em conformidade com o n.º 1 do presente artigo. Os Estados-Membros podem utilizar um certificado ou uma declaração de conformidade emitidos de acordo com um sistema de certificação pertinente ou parte desses sistemas, com os requisitos não relacionados com a cibersegurança estabelecidos no artigo 8.º, n.º 2, relativamente ao nível de garantia dos sistemas de identificação eletrónica.

6. Os Estados-Membros comunicam à Comissão o nome e o endereço dos organismos de avaliação da conformidade a que se refere o n.º 1. A Comissão disponibiliza essa informação a todos os Estados-Membros.

*Artigo 12.º-B*

**Acesso a funcionalidades de hardware e de software**

Caso os fornecedores de carteiras europeias de identidade digital e os emitentes de meios de identificação eletrónica notificados que atuem a título comercial ou profissional e utilizem serviços essenciais de plataforma na aceção do artigo 2.º, ponto 2, do Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho<sup>(1)</sup> para efeitos, ou no decurso da prestação de serviços de carteira europeia de identidade digital e de meios de identificação eletrónica aos utentes finais, sejam utilizadores profissionais na aceção do artigo 2.º, ponto 21, do mesmo regulamento, os controladores de acesso permitem-lhes, nomeadamente, a interoperabilidade efetiva e, para efeitos de interoperabilidade, o acesso ao mesmo sistema operativo ou funcionalidades de *hardware* ou de *software*. Essa interoperabilidade efetiva e o acesso são permitidos a título gratuito e independentemente de as funcionalidades de *hardware* ou de *software* fazerem parte do sistema operativo, estarem disponíveis ou serem utilizados por esse controlador de acesso aquando da prestação desses serviços, na aceção do artigo 6.º, n.º 7, do Regulamento (UE) 2022/1925. O presente artigo não prejudica o disposto no artigo 5.º-A, n.º 14, do presente regulamento.

<sup>(1)</sup> Regulamento (UE) 2022/1925 do Parlamento Europeu e do Conselho, de 14 de setembro de 2022, relativo à disputabilidade e equidade dos mercados no setor digital e que altera as Diretivas (UE) 2019/1937 e (UE) 2020/1828 (Regulamento dos Mercados Digitais) (JO L 265 de 12.10.2022, p. 1).

**▼B**

CAPÍTULO III  
SERVIÇOS DE CONFIANÇA

*SECÇÃO 1*

*Disposições gerais*

*Artigo 13.º*

**Responsabilidade e ónus da prova**

**▼M2**

1. Não obstante o disposto no n.º 2 do presente artigo e sem prejuízo do disposto no Regulamento (UE) 2016/679, os prestadores de serviços de confiança respondem pelos danos causados com dolo ou negligência a qualquer pessoa singular ou coletiva por incumprimento das obrigações previstas no presente regulamento. Qualquer pessoa singular ou coletiva que tenha sofrido danos patrimoniais ou não patrimoniais em resultado de uma infração do presente regulamento por um prestador de serviços de confiança tem o direito de pedir uma indemnização nos termos do direito nacional ou da União.

O ónus da prova do dolo ou negligência de um prestador não qualificado de serviços de confiança recai sobre a pessoa singular ou coletiva que intente a ação de indemnização pelos danos referidos no n.º 1.

Presume-se a existência de dolo ou negligência por parte de um prestador qualificado de serviços de confiança exceto se este provar que os danos referidos no primeiro parágrafo não foram causados com dolo ou negligência por parte desse prestador qualificado de serviços de confiança.

**▼B**

2. Se os prestadores de serviços de confiança informarem prévia e devidamente os seus clientes sobre os limites da utilização dos serviços prestados e, se esses limites forem identificáveis por terceiros, os mesmos prestadores de serviços de confiança não respondem pelos danos decorrentes de uma utilização dos serviços que excede os limites indicados.
3. Os n.ºs 1 e 2 aplicam-se nos termos das disposições nacionais em matéria de responsabilidade.

**▼M2**

*Artigo 14.º*

**Aspectos internacionais**

1. Os serviços de confiança prestados por prestadores de serviços de confiança estabelecidos num país terceiro ou por uma organização internacional são reconhecidos como juridicamente equivalentes aos serviços de confiança qualificados prestados por prestadores qualificados de serviços de confiança estabelecidos na União, se os serviços de confiança originários do país terceiro ou da organização internacional forem reconhecidos por meio de atos de execução ou de um acordo celebrado entre a União e o país terceiro em causa ou uma organização internacional nos termos do artigo 218.º do TFUE.

Os atos de execução referidos no primeiro parágrafo são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼M2**

2. Os atos de execução e o acordo a que se refere o n.º 1 asseguram que os requisitos aplicáveis aos prestadores qualificados de serviços de confiança estabelecidos na União e os serviços de confiança qualificados por eles prestados são cumpridos pelos prestadores de serviços de confiança no país terceiro em causa ou pelas organizações internacionais e pelos serviços de confiança que prestarem. Os países terceiros e as organizações internacionais, em especial, estabelecem, mantêm e publicam uma lista de confiança de prestadores de serviços de confiança reconhecidos.

3. Os acordos referidos no n.º 1 asseguram que os serviços de confiança qualificados prestados pelos prestadores qualificados de serviços de confiança estabelecidos na União são reconhecidos como juridicamente equivalentes aos serviços de confiança prestados por prestadores de serviços de confiança nos países terceiros ou pelas organizações internacionais com os quais tenham sido celebrados.

*Artigo 15.º***Acessibilidade para as pessoas com deficiência e necessidades especiais**

Os meios de identificação eletrónica, os serviços de confiança e os produtos destinados ao utente final que são utilizados na prestação desses serviços são disponibilizados em linguagem clara e inteligível, em conformidade com a Convenção das Nações Unidas sobre os Direitos das Pessoas com Deficiência e com os requisitos de acessibilidade da Diretiva (UE) 2019/882, beneficiando assim também as pessoas com limitações funcionais, como os idosos, e as pessoas com acesso limitado às tecnologias digitais.

*Artigo 16.º***Sanções**

1. Sem prejuízo do disposto no artigo 31.º da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho <sup>(1)</sup>, os Estados-Membros estabelecem o regime de sanções aplicável às infrações ao presente regulamento. Essas sanções devem ser efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros asseguram que as infrações ao presente regulamento por prestadores qualificados e não qualificados de serviços de confiança sejam passíveis de coimas de um montante máximo de, pelo menos:

- a) 5 000 000 EUR se o prestador de serviços de confiança for uma pessoa singular; ou
- b) Se o prestador de serviços de confiança for uma pessoa coletiva, 5 000 000 EUR ou 1 % do volume de negócios anual total a nível mundial da empresa a que o prestador de serviços de confiança pertencia no exercício anterior ao ano em que ocorreu a infração, consoante o que for mais elevado.

<sup>(1)</sup> Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972, e que revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

**▼M2**

3. Dependendo do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de uma forma segundo a qual a coima é iniciada pela entidade supervisora competente e imposta pelos tribunais nacionais competentes. A aplicação dessas regras nesses Estados-Membros assegura que essas vias de recurso são eficazes e têm um efeito equivalente às coimas aplicadas diretamente pelas autoridades supervisoras.

**▼B***SECÇÃO 2***▼M2***Serviços de confiança não qualificados***▼M1****▼M2***Artigo 19.º-A***Requisitos aplicáveis aos prestadores não qualificados de serviços de confiança**

1. Os prestadores não qualificados de serviços de confiança que prestam serviços de confiança não qualificados:

- a) Dispõem de políticas adequadas e tomam as medidas correspondentes para gerir riscos jurídicos, comerciais, operacionais e outros riscos diretos ou indiretos relacionados com a prestação de serviços de confiança não qualificados, as quais devem, não obstante o disposto no artigo 21.º da Diretiva (UE) 2022/2555, incluir, pelo menos, as relacionadas com:
  - i) os procedimentos de registo e adesão a um serviço de confiança,
  - ii) os controlos processuais ou administrativos necessários para prestar serviços de confiança,
  - iii) a gestão e implementação de serviços de confiança;
- b) Notificam a entidade supervisora, as pessoas afetadas identificáveis, o público, se for de interesse público, e, se for caso disso, outras autoridades competentes, de quaisquer violações da segurança ou perturbações na prestação do serviço ou na aplicação das medidas referidas na alínea a), subalínea i), ii) ou iii), que tenham um impacto significativo no serviço de confiança prestado ou nos dados pessoais nele conservados, sem demora indevida e, em qualquer caso, o mais tardar 24 horas após terem tomado conhecimento de quaisquer violações da segurança ou perturbações.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para o n.º 1, alínea a), do presente artigo. Sempre que essas normas, especificações e procedimentos forem cumpridos, beneficiam da presunção de conformidade com os requisitos estabelecidos neste artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***SECÇÃO 3**Serviços qualificados de confiança**Artigo 20.<sup>º</sup>***Fiscalização dos prestadores qualificados de serviços de confiança****▼M2**

1. Os prestadores qualificados de serviços de confiança são auditados, pelo menos de 24 em 24 meses, a expensas suas, por um organismo de avaliação da conformidade. A auditoria confirma que tanto os prestadores qualificados de serviços de confiança como os serviços de confiança qualificados que prestam cumprem os requisitos estabelecidos pelo presente regulamento e pelo artigo 21.<sup>º</sup> da Diretiva (UE) 2022/2555. Os prestadores qualificados de serviços de confiança apresentam o relatório de avaliação da conformidade à entidade supervisora no prazo de três dias úteis após a sua receção.

1-A. Os prestadores qualificados de serviços de confiança informam a entidade supervisora um mês antes das auditorias previstas e permitem à entidade supervisora participar na qualidade de observador, mediante pedido.

1-B. Os Estados-Membros transmitem à Comissão, sem demora indevida, os nomes, endereços e dados relativos à acreditação dos organismos de avaliação da conformidade a que se refere o n.<sup>º</sup> 1, bem como quaisquer alterações subsequentes dos mesmos. A Comissão põe essa informação à disposição dos Estados-Membros.

2. Sem prejuízo do disposto no n.<sup>º</sup> 1, a entidade supervisora pode, em qualquer altura, auditar ou pedir a um organismo de avaliação da conformidade que efetue uma avaliação da conformidade dos prestadores qualificados de serviços de confiança, a expensas desses prestadores qualificados de serviços de confiança, para confirmar que tanto os próprios prestadores, como os serviços de confiança qualificados por eles prestados cumprem as condições estabelecidas no presente regulamento. Em caso de suspeita de violação das regras de proteção de dados pessoais, a entidade supervisora informa, sem demora indevida, as autoridades de controlo competentes criadas nos termos do artigo 51.<sup>º</sup> do Regulamento (UE) 2016/679.

3. Se o prestador qualificado de serviços de confiança não cumprir algum dos requisitos estabelecidos pelo presente regulamento, a entidade supervisora exige-lhe que corrija a situação num prazo determinado, se aplicável.

Se o prestador não corrigir a situação, se aplicável, no prazo fixado pela entidade supervisora, esta última, se tal se justificar, nomeadamente, pela extensão, pela duração e pelas consequências do incumprimento, retira o estatuto de qualificado ao prestador ou ao serviço afetado por ele prestado.

3-A. Se as autoridades competentes designadas ou criadas nos termos do artigo 8.<sup>º</sup>, n.<sup>º</sup> 1, da Diretiva (UE) 2022/2555, informarem a entidade supervisora de que o prestador qualificado de serviços de confiança não cumpre nenhum dos requisitos estabelecidos no artigo 21.<sup>º</sup> dessa diretiva, a entidade supervisora, se tal se justificar, nomeadamente, pela extensão, pela duração e pelas consequências do incumprimento, retira o estatuto de qualificado ao prestador ou ao serviço em causa por ele prestado.

**▼M2**

3-B. Se as autoridades de controlo criadas nos termos do artigo 51.º do Regulamento (UE) 2016/679, informarem a entidade supervisora de que o prestador qualificado de serviços de confiança não cumpre nenhum dos requisitos estabelecidos nesse regulamento, a entidade supervisora, se tal se justificar, nomeadamente, pela extensão, pela duração e pelas consequências do incumprimento, retira o estatuto de qualificado ao prestador ou ao serviço em causa por ele prestado.

3-C. A entidade supervisora informa o prestador qualificado de serviços de confiança da retirada do seu estatuto de qualificado ou do estatuto de qualificado do serviço em causa. A entidade supervisora informa a entidade notificada nos termos do artigo 22.º, n.º 3, do presente regulamento, para efeitos de atualização das listas de confiança referidas no n.º 1 do mesmo artigo, bem como a autoridade competente designada ou criada nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555.

4. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos no que diz respeito:

- a) À acreditação dos organismos de avaliação da conformidade e ao relatório de avaliação da conformidade a que se refere o n.º 1;
- b) Aos requisitos de auditoria para os organismos de avaliação da conformidade efetuarem a avaliação da conformidade, inclusive a avaliação compósita, dos prestadores qualificados de serviços de confiança a que se refere o n.º 1;
- c) Aos sistemas de avaliação da conformidade utilizados pelos organismos de avaliação da conformidade para realizar a avaliação da conformidade dos prestadores qualificados de serviços de confiança e para a apresentação do relatório a que se refere o n.º 1.

Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 21.º***Início de um serviço de confiança qualificado****▼M2**

1. Quando os prestadores de serviços de confiança pretendam começar a prestar serviços de confiança qualificado, apresentam à entidade supervisora uma notificação da sua intenção, acompanhada de um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade que ateste o cumprimento dos requisitos estabelecidos no presente regulamento e no artigo 21.º da Diretiva (UE) 2022/2555.

2. A entidade supervisora verifica se o prestador de serviços de confiança e os serviços de confiança por ele prestados cumprem os requisitos estabelecidos no presente regulamento e, designadamente, os requisitos previstos para os prestadores qualificados de serviços de confiança e para os serviços de confiança qualificados por eles prestados.

**▼M2**

A fim de verificar se o prestador de serviços de confiança cumpre os requisitos estabelecidos no artigo 21.º da Diretiva (UE) 2022/2555, a entidade supervisora solicita às autoridades competentes designadas ou criadas nos termos do artigo 8.º, n.º 1, dessa diretiva que realizem ações de supervisão nesse sentido e prestem informações sobre o resultado, sem demora indevida e, em qualquer caso, no prazo de dois meses a contar da receção desse pedido. Se a verificação não ficar concluída no prazo de dois meses a contar da notificação, a autoridade competente informa a entidade supervisora, indicando as razões do atraso e o prazo dentro do qual a verificação estará concluída.

Se concluir que o prestador de serviços de confiança e os serviços de confiança por ele prestados cumprem os requisitos previstos no presente regulamento, a entidade supervisora atribui o estatuto de qualificado ao prestador de serviços de confiança e aos serviços de confiança por ele prestados e informa a entidade referida no artigo 22.º, n.º 3, para efeitos de atualização das listas de confiança referidas no artigo 22.º, n.º 1, o mais tardar três meses após a notificação feita nos termos do n.º 1 do presente artigo.

Se a verificação não ficar concluída no prazo de três meses a contar da notificação, a entidade supervisora informa o prestador de serviços de confiança, indicando as razões do atraso e o prazo dentro do qual a verificação estará concluída.

**▼B**

3. Os prestadores qualificados de serviços de confiança podem iniciar a prestação do serviço de confiança qualificado depois de o estatuto de qualificado ter sido publicado nas listas de confiança referidas no artigo 22.º, n.º 1.

**▼M2**

4. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, os formatos e procedimentos de notificação e verificação para efeitos do disposto nos n.os 1 e 2 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 22.º***Listas de confiança**

1. Os Estados-Membros elaboram, conservam e publicam listas de confiança com informações relativas aos prestadores qualificados de serviços de confiança para os quais forem competentes, assim como informações relacionadas com os serviços de confiança qualificados por eles prestados.

2. Os Estados-Membros elaboram e publicam, em condições seguras, as listas de confiança referidas no n.º 1, eletronicamente assinadas ou seladas, num formato adequado ao tratamento automático.

3. Os Estados-Membros transmitem à Comissão, sem atrasos indevidos, informações sobre a entidade responsável pela elaboração, conservação e publicação das listas de confiança nacionais, os dados referentes ao local em que tais listas se encontram publicadas, bem como sobre os certificados utilizados para as assinar ou selar e as eventuais alterações a tais informações.

**▼B**

4. A Comissão disponibiliza ao público, através de um canal seguro, as informações referidas no n.º 3 num formato eletronicamente assinado ou selado, adequado ao tratamento automático.

5. Até 18 de setembro de 2015, a Comissão especifica, por meio de atos de execução, as informações referidas no n.º 1 e define as especificações técnicas e os formatos das listas de confiança aplicáveis para efeitos do disposto nos n.os 1 a 4. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 23.º***Marca de confiança «UE» para serviços de confiança qualificados**

1. Depois de o estatuto de qualificado referido no artigo 21.º, n.º 2, segundo parágrafo, ser publicado na lista de confiança a que se refere o artigo 22.º, n.º 1, os prestadores qualificados de serviços de confiança podem utilizar a marca de confiança «UE» para identificar, de forma simples, reconhecível e clara, os serviços de confiança qualificados que prestam.

2. Ao utilizar a marca de confiança «UE» para os serviços de confiança qualificados referida no n.º 1, os prestadores qualificados de serviços de confiança asseguram-se da existência de uma ligação à correspondente lista de confiança no seu sítio web.

3. Até 1 de julho de 2015, a Comissão estabelece, por meio de atos de execução, as especificações relativas à forma e, em particular, à apresentação, composição, dimensão e conceção da marca de confiança «UE» para serviços de confiança qualificados. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 24.º***Requisitos aplicáveis aos prestadores qualificados de serviços de confiança****▼M2**

1. Ao emitirem certificados qualificados ou certificados eletrónicos qualificados de atributos, os prestadores qualificados de serviços de confiança verificam a identidade e, se aplicável, os eventuais atributos específicos da pessoa singular ou coletiva à qual é emitido o certificado qualificado ou o certificado eletrónico qualificado de atributos.

1-A. A verificação da identidade referida no n.º 1 é efetuada, pelos meios adequados, pelos prestadores qualificados de serviços de confiança, diretamente ou através de um terceiro, com base num dos seguintes métodos ou numa combinação dos mesmos, quando necessário, em conformidade com os atos de execução a que se refere o n.º 1-C:

- a) Através da carteira europeia de identidade digital ou de um meio de identificação eletrónica notificado que satisfaça os requisitos estabelecidos no artigo 8.º no que diz respeito ao nível de garantia elevado;
- b) Através de um certificado qualificado de assinatura eletrónica ou de um selo eletrónico qualificado emitido em cumprimento da alínea a), c) ou d);

**▼M2**

- c) Utilizando outros métodos de identificação que garantam a identificação da pessoa com um elevado nível de certeza, cuja conformidade é atestada por um organismo de avaliação da conformidade;
- d) Pela presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, através de elementos de prova adequados e procedimentos, em conformidade com o direito nacional.

1-B. A verificação dos atributos referida no n.º 1 é efetuada, pelos meios adequados, pelos prestadores qualificados de serviços de confiança, diretamente ou através de um terceiro, com base num dos seguintes métodos ou, caso seja necessário, numa combinação dos mesmos, em conformidade com os atos de execução a que se refere o n.º 1-C:

- a) Através da carteira europeia de identidade digital ou de um meio de identificação eletrónica notificado que satisfaça os requisitos estabelecidos no artigo 8.º no que diz respeito ao nível de garantia elevado;
- b) Através de um certificado qualificado de assinatura eletrónica ou de um selo eletrónico qualificado emitido em conformidade com o n.º 1-A, alínea a), c) ou d);
- c) Através de uma validação qualificada de certificados eletrónicos de atributos;
- d) Utilizando outros métodos que garantam a verificação dos atributos com um elevado nível de confiança, cuja conformidade é atestada por um organismo de avaliação da conformidade;
- e) Através da presença física da pessoa singular ou de um representante autorizado da pessoa coletiva, através de elementos de prova adequados e procedimentos, em conformidade com o direito nacional.

1-C. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para a verificação da identidade e dos atributos em conformidade com os n.os 1, 1-A e 1-B do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

2. Os prestadores qualificados de serviços de confiança que prestam serviços de confiança qualificados:

**▼M2**

- a) Informam a entidade supervisora pelo menos um mês antes de implementar qualquer alteração da prestação dos seus serviços de confiança qualificados ou, pelo menos, três meses antes em caso de intenção de cessar essas atividades;
- b) Empregam pessoal e, eventualmente, subcontratantes que possuam a especialização, a confiança, experiência e as qualificações necessárias e que tenham recebido formação adequada em matéria de regras de segurança e de proteção de dados pessoais e aplicam procedimentos administrativos e de gestão que correspondam às normas europeias ou internacionais;
- c) Face ao risco da responsabilidade por danos prevista no artigo 13.º, conservam recursos financeiros suficientes e/ou adquirem um seguro de responsabilidade adequado, de acordo com a legislação nacional;

**▼M2**

- d) Antes de estabelecerem uma relação contratual, informam, de forma clara, completa e facilmente acessível, num espaço acessível ao público e individualmente, as pessoas que pretendam utilizar serviços de confiança qualificados dos termos e condições exatos da utilização de tais serviços, incluindo de qualquer limitação à sua utilização;
- e) Utilizam sistemas e produtos fiáveis que estejam protegidos contra modificações e garantam a segurança e a fiabilidade técnicas dos processos de que são suporte, incluindo a utilização de técnicas criptográficas adequadas;

**▼B**

- f) Utilizam sistemas fiáveis de armazenamento dos dados que lhes são fornecidos, num formato verificável, de modo a que:
  - i) os dados apenas estejam publicamente disponíveis para extração se tiver sido obtido o consentimento da pessoa a quem os dados digam respeito,
  - ii) apenas as pessoas autorizadas possam introduzir dados e alterações aos dados armazenados,
  - iii) a autenticidade dos dados possa ser verificada;

**▼M2**

- f-A) Não obstante o disposto no artigo 21.º da Diretiva (UE) 2022/2555, dispõem de políticas adequadas e tomam as medidas correspondentes para gerir riscos jurídicos, comerciais, operacionais e outros riscos diretos ou indiretos relacionados com a prestação de serviços de confiança qualificados, incluindo, pelo menos, medidas relacionadas com:
  - i) os procedimentos de registo e adesão a um serviço,
  - ii) os controlos processuais ou administrativos,
  - iii) a gestão e implementação de serviços;
- f-B) Notificam a entidade supervisora, as pessoas afetadas identificáveis, outros organismos competentes relevantes, se for caso disso, e, a pedido da entidade supervisora, o público, se tal for de interesse público, de quaisquer violações da segurança ou perturbações na prestação do serviço ou na aplicação das medidas referidas na alínea f-A), subalíneas i), ii) ou iii), que tenham um impacto significativo no serviço de confiança prestado ou nos dados pessoais nele conservados, sem demora indevida e, em qualquer caso, no prazo de 24 horas após o incidente;
- g) Tomam as medidas adequadas contra a falsificação, o roubo ou a apropriação indevida dos dados, ou a eliminação, a alteração ou o impedimento do acesso aos dados, na ausência de direito para tal;
- h) Registam e mantêm acessíveis durante o tempo que for necessário depois de o prestador qualificado de serviços de confiança ter cessado as suas atividades, todas as informações pertinentes relativas aos dados emitidos e recebidos pelo prestador qualificado de serviços de confiança, para efeitos de apresentação de provas em processos judiciais e para garantir a continuidade do serviço. Esse registo poderá ser feito por via eletrónica;

**▼M2**

- i) Conservam um plano de cessação de atividades atualizado que garanta a continuidade do serviço de acordo com as disposições verificadas pela entidade supervisora nos termos do artigo 46.º-B, n.º 4, alínea i);

**▼B**

- k) Criam e mantêm atualizada uma base de dados de certificados, quando emitam certificados qualificados.

**▼M2**

A entidade supervisora pode solicitar informações para além das informações notificadas nos termos da alínea a) do primeiro parágrafo ou do resultado de uma avaliação da conformidade e pode condicionar a concessão da autorização para implementar as alterações pretendidas dos serviços de confiança qualificados. Se a verificação não ficar concluída no prazo de três meses a contar da notificação, a entidade supervisora informa o prestador de serviços de confiança, indicando as razões do atraso e o prazo dentro do qual a verificação deve estar concluída.

**▼B**

3. Se os prestadores qualificados de serviços de confiança que emitem certificados qualificados decidirem revogar um certificado, registram a revogação na sua base de dados e publicam-na em tempo útil, mas sempre no prazo de 24 horas após a receção do pedido. A revogação produz efeitos imediatamente após a sua publicação.

4. No que respeita ao disposto no n.º 3, os prestadores qualificados de serviços de confiança que emitam certificados qualificados fornecem a qualquer utilizador informações sobre a validade ou a revogação dos certificados qualificados por eles emitidos. Estas informações são fornecidas pelo menos para cada certificado, em qualquer altura e mesmo após o termo do prazo de validade do certificado, de uma maneira automática que seja fiável, gratuita e eficaz.

**▼M2**

4-A. Os n.os 3 e 4 aplicam-se em conformidade à revogação de certificados eletrónicos qualificados de atributos.

4-B. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 47.º, estabelecendo as medidas adicionais referidas no n.º 2, alínea f-A), do presente artigo.

5. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos para os requisitos referidos no n.º 2 do presente artigo. Sempre que essas especificações técnicas, procedimentos e normas forem cumpridos, beneficiam da presunção de conformidade com os requisitos estabelecidos no presente número. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 24.º-A***Reconhecimento de serviços de confiança qualificados**

1. As assinaturas eletrónicas qualificadas baseadas num certificado qualificado emitido num Estado-Membro e os selos eletrónicos qualificados baseados num certificado qualificado emitido num

**▼M2**

Estado-Membro são reconhecidos, respetivamente, como assinaturas eletrónicas qualificadas e selos eletrónicos qualificados em todos os outros Estados-Membros.

2. Os dispositivos qualificados de criação de assinaturas eletrónicas e os dispositivos qualificados de criação de selos eletrónicos certificados num Estado-Membro são reconhecidos, respetivamente, como dispositivos qualificados de criação de assinaturas eletrónicas e dispositivos qualificados de criação de selos eletrónicos em todos os outros Estados-Membros.

3. Um certificado qualificado para assinaturas eletrónicas, um certificado qualificado para selos eletrónicos, um serviço de confiança qualificado para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e um serviço de confiança qualificado para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância fornecidos num Estado-Membro são reconhecidos, respetivamente, como um certificado qualificado para assinaturas eletrónicas, um certificado qualificado para selos eletrónicos, um serviço de confiança qualificado para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância e um serviço de confiança qualificado para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância em todos os outros Estados-Membros.

4. Um serviço qualificado de validação de assinaturas eletrónicas qualificadas e um serviço qualificado de validação de selos eletrónicos qualificados prestados num Estado-Membro são reconhecidos, respetivamente, como um serviço qualificado de validação de assinaturas eletrónicas qualificadas e um serviço qualificado de validação de selos eletrónicos qualificados em todos os outros Estados-Membros.

5. Um serviço qualificado de preservação de assinaturas eletrónicas qualificadas e um serviço qualificado de preservação de selos eletrónicos qualificados prestados num Estado-Membro são reconhecidos, respetivamente, como um serviço qualificado de preservação de assinaturas eletrónicas qualificadas e um serviço qualificado de preservação de selos eletrónicos qualificados em todos os outros Estados-Membros.

6. Um selo temporal qualificado fornecido num Estado-Membro é reconhecido como um selo temporal qualificado em todos os outros Estados-Membros.

7. Um certificado qualificado de autenticação de sítios Web emitido num Estado-Membro é reconhecido como um certificado qualificado para autenticação de sítios Web em todos os outros Estados-Membros.

8. Um serviço qualificado de envio registado eletrónico prestado num Estado-Membro é reconhecido como um serviço qualificado de envio registado eletrónico em todos os outros Estados-Membros.

9. Um certificado eletrónico qualificado de atributos emitido num Estado-Membro é reconhecido como um certificado eletrónico qualificado de atributos em todos os outros Estados-Membros.

10. Um serviço qualificado de arquivo eletrónico prestado num Estado-Membro é reconhecido como um serviço qualificado de arquivo eletrónico em todos os outros Estados-Membros.

**▼M2**

11. Um livro-razão eletrónico qualificado fornecido num Estado-Membro é reconhecido como livro-razão eletrónico qualificado em todos os outros Estados-Membros.

**▼B***SEÇÃO 4**Assinaturas eletrónicas**Artigo 25.º***Efeitos legais das assinaturas eletrónicas**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a uma assinatura eletrónica pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos exigidos para as assinaturas eletrónicas qualificadas.

2. A assinatura eletrónica qualificada tem um efeito legal equivalente ao de uma assinatura manuscrita.

**▼M2****▼B***Artigo 26.º***Requisitos para as assinaturas eletrónicas avançadas**

**►M2** 1. ◀ A assinatura eletrónica avançada obedece aos seguintes requisitos:

- a) Estar associada de modo único ao signatário;
- b) Permitir identificar o signatário;
- c) Ser criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo; e
- d) Estar ligada aos dados por ela assinados de tal modo que seja detetável qualquer alteração posterior dos dados.

**▼M2**

2. Até 21 de maio de 2026, a Comissão avalia se é necessário adotar atos de execução para estabelecer uma lista de normas de referência e, se necessário, estabelecer especificações e procedimentos para as assinaturas eletrónicas avançadas. Com base nessa avaliação, a Comissão pode adotar esses atos de execução. As assinaturas avançadas que satisfazem esses procedimentos, normas e especificações beneficiam da presunção de conformidade com os requisitos para as assinaturas eletrónicas avançadas. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 27.º***Assinaturas eletrónicas em serviços públicos**

1. O Estado-Membro que exigir assinatura eletrónica avançada para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes, reconheça as assinaturas eletrónicas avançadas, as

**▼B**

assinaturas eletrónicas avançadas baseadas em certificados qualificados para assinaturas eletrónicas e as assinaturas eletrónicas qualificadas que pelo menos se apresentem nos formatos ou utilizem os métodos definidos nos atos de execução a que se refere o n.º 5.

2. O Estado-Membro que exigir assinatura eletrónica avançada baseada num certificado qualificado para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes, reconheça as assinaturas eletrónicas avançadas baseadas em certificados qualificados para assinaturas eletrónicas e as assinaturas eletrónicas qualificadas que pelo menos se apresentem nos formatos ou utilizem os métodos definidos nos atos de execução a que se refere o n.º 5.

3. Os Estados-Membros não exigem para a utilização transfronteiriça em serviços em linha prestados por organismos públicos, uma assinatura eletrónica com um nível de garantia de segurança superior ao da assinatura eletrónica qualificada.

**▼M2****▼B**

5. Até 18 de setembro de 2015, e tendo em conta as práticas, normas e atos jurídicos da União, a Comissão, mediante atos de execução, define os formatos de referência das assinaturas eletrónicas avançadas ou os métodos de referência se forem utilizados formatos alternativos. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 28.º***Certificados qualificados de assinaturas eletrónicas**

1. Os certificados qualificados de assinaturas eletrónicas cumprem os requisitos estabelecidos no anexo I.

2. Os certificados qualificados de assinaturas eletrónicas não podem estar sujeitos a requisitos obrigatórios que excedam os requisitos estabelecidos no anexo I.

3. Os certificados qualificados de assinaturas eletrónicas podem incluir características específicas adicionais não obrigatórias. Tais características não prejudicam a interoperabilidade e o reconhecimento das assinaturas eletrónicas qualificadas.

4. Os certificados qualificados de assinaturas eletrónicas que tenham sido revogados após a ativação inicial perdem a validade a partir do momento da revogação, não podendo o seu estatuto ser revertido, em nenhuma circunstância.

5. Os Estados-Membros podem estabelecer regras nacionais sobre a suspensão temporária dos certificados qualificados de uma assinatura eletrónica na condição de:

- a) O certificado qualificado de assinatura eletrónica que tiver sido suspenso temporariamente perder a sua validade durante o período da suspensão.
- b) O período de suspensão ser claramente indicado na base de dados de certificados e, durante o período pertinente, o estatuto de suspensão ser visível para o serviço que presta informações sobre o estatuto dos certificados.

**▼M2**

6. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para certificados qualificados de assinatura eletrónica. Os certificados qualificados para assinatura eletrónica que cumprem esses procedimentos, normas e especificações beneficiam da presunção de conformidade com os requisitos estabelecidos no anexo I. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

**▼B**

*Artigo 29.<sup>º</sup>*

**Requisitos aplicáveis aos dispositivos qualificados de criação de assinaturas eletrónicas**

1. Os dispositivos qualificados de criação de assinaturas eletrónicas cumprem os requisitos estabelecidos no anexo II.

**▼M2**

1-A. A geração ou a gestão de dados para a criação de uma assinatura eletrónica ou a duplicação desses dados para a criação de assinaturas para fins de cópia de segurança podem ser efetuadas apenas em nome do signatário, a pedido deste, e por um prestador qualificado de serviços de confiança que ofereça um serviço de confiança qualificado para a gestão de um dispositivo qualificado de criação de assinaturas eletrónicas à distância.

**▼B**

2. A Comissão pode, por meio de atos de execução, estabelecer os números de referência das normas relativas aos dispositivos qualificados de criação de assinaturas eletrónicas. Os dispositivos qualificados de criação de assinaturas eletrónicas conformes com as referidas normas beneficiam da presunção de conformidade com os requisitos estabelecidos no anexo II. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

**▼M2**

*Artigo 29.<sup>º</sup>-A*

**Requisitos aplicáveis a um serviço qualificado para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância**

1. A gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância enquanto serviço qualificado só pode ser realizada por um prestador qualificado de serviços de confiança que:

- a) Proceda à geração ou à gestão de dados para a criação de uma assinatura eletrónica em nome do signatário;
- b) Não obstante o disposto no ponto 1, alínea d), do anexo II, duplica os dados para a criação de uma assinatura eletrónica apenas para fins de cópia de segurança, desde que sejam cumpridos os seguintes requisitos:
  - i) a segurança dos conjuntos de dados duplicados está ao mesmo nível da dos conjuntos de dados originais,
  - ii) o número de conjuntos de dados duplicados não excede o mínimo necessário para garantir a continuidade do serviço;

**▼M2**

- c) Cumpra todos os requisitos identificados no relatório de certificação do específico dispositivo qualificado de criação de assinaturas eletrónicas à distância emitido nos termos do artigo 30.º.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, especificações e procedimentos para efeitos do n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 30.º***Certificação dos dispositivos qualificados de criação de assinaturas eletrónicas**

1. A conformidade dos dispositivos qualificados de criação de assinaturas eletrónicas com os requisitos estabelecidos no anexo II é certificada pelas entidades públicas ou privadas competentes designadas pelos Estados-Membros.

2. Os Estados-Membros comunicam à Comissão a denominação e o endereço da entidade pública ou privada por eles designada, referida no n.º 1. A Comissão põe a informação à disposição dos Estados-Membros.

3. A certificação referida no n.º 1 é baseada:

- a) Num processo de avaliação de segurança executado de acordo com as normas da avaliação de segurança dos produtos informáticos constantes da lista elaborada nos termos do segundo parágrafo; ou
- b) Num processo diferente do referido na alínea a), desde que esse processo utilize níveis de segurança comparáveis e a entidade pública ou privada referida no n.º 1 notifique esse processo à Comissão. Esse processo só pode ser utilizado na falta das normas constantes da alínea a) ou se estiver em curso um processo de avaliação de segurança referido na alínea a).

A Comissão deve, por meio de atos de execução, elaborar a lista de normas da avaliação de segurança dos produtos informáticos a que se refere a alínea a). Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 8.º.

**▼M2**

3-A. A validade da certificação a que se refere o n.º 1 não excede cinco anos, desde que as avaliações das vulnerabilidades sejam realizadas de dois em dois anos. Sempre que sejam identificadas vulnerabilidades e as mesmas não sejam corrigidas, a certificação é cancelada.

**▼B**

4. A Comissão tem poderes para adotar atos delegados nos termos do artigo 47.º para estabelecer os critérios específicos a cumprir pelas entidades designadas referidas no n.º 1 do presente artigo.

**▼B***Artigo 31.º***Publicação de uma lista de dispositivos qualificados e certificados de criação de assinaturas eletrónicas**

1. Os Estados-Membros comunicam à Comissão, sem atrasos indevidos, no prazo de um mês após a conclusão da certificação, informações sobre os dispositivos qualificados de criação de assinaturas eletrónicas que tenham sido certificados pelas entidades referidas no artigo 30.º, n.º 1. Comunicam também à Comissão, sem atrasos indevidos, no prazo de um mês após a conclusão da certificação, informações sobre os dispositivos de criação de assinaturas eletrónicas que deixem de estar certificados.

2. Com base nas informações recebidas, a Comissão elabora, publica e mantém atualizada uma lista dos dispositivos qualificados e certificados de criação de assinaturas eletrónicas.

**▼M2**

3. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, formatos e procedimentos aplicáveis para efeitos do disposto no n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 32.º***Requisitos aplicáveis à validade das assinaturas eletrónicas qualificadas**

1. O processo de validação de uma assinatura eletrónica qualificada confirma a validade desta na condição de:

- a) No momento da assinatura, o certificado que lhe serve de suporte ser um certificado qualificado de assinatura eletrónica conforme com o disposto no anexo I;
- b) O certificado qualificado ter sido emitido por um prestador qualificado de serviços de confiança e ser válido no momento da assinatura;
- c) Os dados para a validação da assinatura corresponderem aos dados fornecidos ao utilizador;
- d) O conjunto único de dados que representam o signatário no certificado serem corretamente fornecidos ao utilizador;
- e) A utilização de um pseudónimo no momento da assinatura ser claramente indicada ao utilizador;
- f) A assinatura eletrónica ter sido criada por um dispositivo qualificado de criação de assinatura eletrónica;
- g) A integridade dos dados assinados não ter sido afetada;
- h) Os requisitos previstos no artigo 26.º se encontrarem preenchidos no momento da assinatura;

**▼M2**

A validação de assinaturas eletrónicas qualificadas que cumpre as normas, especificações e procedimentos referidos no n.º 3 beneficia da presunção de conformidade com os requisitos estabelecidos no primeiro parágrafo do presente número.

**▼B**

2. O sistema utilizado para validar a assinatura eletrónica qualificada fornece ao utilizador o resultado correto do processo de validação e permite-lhe detetar eventuais problemas de segurança.

**▼M2**

3. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para a validação de assinaturas eletrónicas qualificadas. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 32.º-A*

**Requisitos para a validação de assinaturas eletrónicas avançadas com base em certificados qualificados**

1. O processo de validação de uma assinatura eletrónica avançada baseado num certificado qualificado atesta a validade de uma assinatura eletrónica avançada baseada num certificado qualificado, desde que:

- a) No momento da assinatura, o certificado que lhe serve de suporte seja um certificado qualificado para assinatura eletrónica conforme com o disposto no anexo I;
- b) O certificado qualificado tenha sido emitido por um prestador qualificado de serviços de confiança e tenha sido válido no momento da assinatura;
- c) Os dados para a validação da assinatura correspondam aos dados fornecidos ao utilizador;
- d) O conjunto único de dados que representam o signatário no certificado sejam corretamente fornecidos ao utilizador;
- e) A utilização de um pseudónimo no momento da assinatura seja claramente indicada ao utilizador;
- f) A integridade dos dados assinados não tenha sido afetada;
- g) Os requisitos previstos no artigo 26.º se encontrassem preenchidos no momento da assinatura.

2. O sistema utilizado para validar a assinatura eletrónica avançada com base em certificados qualificados fornece ao utilizador o resultado correto do processo de validação e permite-lhe detetar eventuais problemas de segurança.

3. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para a validação de assinaturas eletrónicas avançadas com base em certificados qualificados. A validação de assinaturas eletrónicas avançadas com base em certificados qualificados que cumpre essas normas, especificações e procedimentos beneficia da presunção de conformidade com os requisitos estabelecidos no n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***Artigo 33.<sup>º</sup>***Serviço qualificado de validação de assinaturas eletrónicas qualificadas**

1. Os serviços qualificados de validação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que:

- a) Efetuam a validação em conformidade com o artigo 32.<sup>º</sup>, n.<sup>º</sup> 1, e
- b) Permitam aos utilizadores receber o resultado do processo de validação de um modo automático que seja fiável e eficaz e que inclua a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador do serviço qualificado de validação.

**▼M2**

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos relativos ao serviço qualificado de validação a que se refere o n.<sup>º</sup> 1 do presente artigo. Os serviços qualificados de validação de assinaturas eletrónicas qualificadas que cumprem essas normas, especificações e procedimentos beneficiam da presunção de conformidade com os requisitos estabelecidos no n.<sup>º</sup> 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

**▼B***Artigo 34.<sup>º</sup>***Serviço qualificado de preservação de assinaturas eletrónicas qualificadas**

1. Os serviços de preservação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que utilizem procedimentos e tecnologias capazes de prolongar a fiabilidade das assinaturas eletrónicas qualificadas para além do prazo de validade tecnológica.

**▼M2**

1-A. As disposições aplicáveis ao serviço qualificado de conservação de assinaturas eletrónicas qualificadas que cumprem as normas, especificações e procedimentos referidos no n.<sup>º</sup> 2 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.<sup>º</sup> 1.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para serviços qualificados de preservação de assinaturas eletrónicas qualificadas. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

**▼B**

*SECÇÃO 5*

*Selos eletrónicos*

*Artigo 35.º*

**Efeitos legais dos selos eletrónicos**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um selo eletrónico pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos dos selos eletrónicos qualificados.
2. O selo eletrónico qualificado beneficia da presunção da integridade dos dados e da correção da origem dos dados aos quais está associado.

**▼M2**

**▼B**

*Artigo 36.º*

**Requisitos para os selos eletrónicos avançados**

- M2 1. ◀ O selo eletrónico avançado obedece aos seguintes requisitos:
- a) Estar associado de modo único ao seu criador;
  - b) Permitir identificar o seu criador;
  - c) Ser criado através dos dados de criação de selos eletrónicos cujo criador pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico; e
  - d) Estar ligado aos dados a que diz respeito de tal modo que seja detetável qualquer alteração posterior dos dados.

**▼M2**

2. Até 21 de maio de 2026, a Comissão avalia se é necessário adotar atos de execução a fim de estabelecer uma lista de normas de referência e, se necessário, estabelecer especificações e procedimentos aplicáveis aos selos eletrónicos avançados. Com base no resultado dessa avaliação, a Comissão pode adotar tais atos de execução. Os selos eletrónicos avançados que cumprem essas normas, especificações e procedimentos beneficiam da presunção de conformidade com os requisitos para os selos eletrónicos avançados. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

*Artigo 37.º*

**Selos eletrónicos em serviços públicos**

1. O Estado-Membro que exigir selo eletrónico avançado para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes, reconhece os selos eletrónicos avançados, os selos eletrónicos avançados baseados em certificados qualificados para selos eletrónicos e selos eletrónicos qualificados pelo menos que se apresentem nos formatos ou utilizem os métodos definidos nos atos de execução a que se refere o n.º 5.

**▼B**

2. O Estado-Membro que exigir selo eletrónico avançado baseado num certificado qualificado para a utilização de serviços em linha oferecidos por organismos públicos ou em nome destes, reconhece os selos eletrónicos avançados baseados em certificados qualificados para selos eletrónicos e selos eletrónicos qualificados pelo menos que se apresentem nos formatos ou utilizem os métodos definidos nos atos de execução a que se refere o n.º 5.

3. Os Estados-Membros não exigem, para a utilização transfronteiriça em serviços em linha prestados por organismos públicos, um selo eletrónico com um nível de garantia de segurança superior ao do selo eletrónico qualificado.

**▼M2****▼B**

5. Até 18 de setembro de 2015, e tendo em conta as práticas, normas e atos jurídicos da União, a Comissão, através de atos de execução, define os formatos de referência dos selos eletrónicos avançados ou os métodos de referência se forem utilizados formatos alternativos. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 38.º***Certificados qualificados de selos eletrónicos**

1. Os certificados qualificados de selos eletrónicos devem cumprir os requisitos estabelecidos no anexo III.

2. Os certificados qualificados de selos eletrónicos não estão sujeitos a requisitos obrigatórios que excedam os requisitos estabelecidos no anexo III.

3. Os certificados qualificados de selos eletrónicos podem incluir características específicas adicionais não obrigatórias. Tais características não prejudicam a interoperabilidade e o reconhecimento dos selos eletrónicos qualificados.

4. Os certificados qualificados de selo eletrónico que tenham sido revogados após a ativação inicial perdem a validade a partir do momento da revogação, não podendo o seu estatuto ser revertido, em nenhuma circunstância.

5. Os Estados-Membros podem estabelecer regras nacionais sobre a suspensão temporária dos certificados qualificados de selos eletrónicos na condição de:

- a) O certificado qualificado de selo eletrónico que tiver sido suspenso temporariamente perder a sua validade durante o período da suspensão;
- b) O período de suspensão ser claramente indicado na base de dados de certificados e, durante o período pertinente, o estatuto de suspensão ser visível para o serviço que presta informações sobre o estatuto dos certificados.

**▼M2**

6. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para certificados qualificados de selos eletrónicos. Os certificados qualificados de selos eletrónicos que cumprem essas normas, especificações e procedimentos beneficiam da presunção de conformidade com os requisitos estabelecidos no anexo III. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

*Artigo 39.<sup>o</sup>*

**Dispositivos qualificados de criação de selos eletrónicos**

1. O artigo 29.<sup>o</sup> aplica-se com as necessárias adaptações aos requisitos exigidos para os dispositivos qualificados de criação de selo eletrónico.
2. O artigo 30.<sup>o</sup> aplica-se com as necessárias adaptações à certificação dos dispositivos qualificados de criação de selo eletrónico.
3. O artigo 31.<sup>o</sup> aplica-se com as necessárias adaptações à publicação da lista de dispositivos qualificados e certificados de criação de selo eletrónico.

**▼M2**

*Artigo 39.<sup>o</sup>-A*

**Requisitos aplicáveis a um serviço qualificado para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância**

O artigo 29.<sup>o</sup>-A aplica-se *mutatis mutandis* a um serviço qualificado para a gestão de dispositivos qualificados de criação de selos eletrónicos à distância.

**▼B**

*Artigo 40.<sup>o</sup>*

**Validação e preservação dos selos eletrónicos qualificados**

Os artigos 32.<sup>o</sup>, 33.<sup>o</sup> e 34.<sup>o</sup> aplicam-se com as necessárias adaptações à validação e à preservação dos selos eletrónicos qualificados.

**▼M2**

*Artigo 40.<sup>o</sup>-A*

**Requisitos para a validação de selos eletrónicos avançados com base em certificados qualificados**

O artigo 32.<sup>o</sup>-A aplica-se *mutatis mutandis* à validação dos selos eletrónicos avançados com base em certificados qualificados.

**▼B**

*SECÇÃO 6*

**Selos temporais**

*Artigo 41.<sup>o</sup>*

**Efeito legal dos selos temporais**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um selo temporal pelo simples facto de se apresentar em formato eletrónico ou de não cumprir os requisitos do selo temporal qualificado.
2. O selo temporal qualificado beneficia da presunção da exatidão da data e da hora que indica e da integridade dos dados aos quais a data e a hora estão associadas.

**▼M2**

**▼B**

*Artigo 42.º*

**Requisitos aplicáveis aos selos temporais qualificados**

1. Os selos temporais qualificados cumprem os seguintes requisitos:

- a) Vincular a data e a hora aos dados de forma a tornar razoavelmente impossível a alteração dos dados de forma não detetável;
- b) Basear-se numa fonte horária precisa ligada à Hora Universal Coordenada; e
- c) Ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, ou por outro método equivalente.

**▼M2**

1-A. A vinculação da data e da hora aos dados e a precisão da fonte horária que cumprem as normas, especificações e procedimentos referidos no n.º 2 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.º 2.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos relativos à vinculação da data e da hora aos dados e à determinação da precisão das fontes horárias. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

*SECÇÃO 7*

**Serviço de envio registado eletrónico**

*Artigo 43.º*

**Efeito legal dos serviços de envio registado eletrónico**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial aos dados enviados e recebidos com recurso a um serviço de envio registado eletrónico pelo simples facto de se apresentarem em formato eletrónico ou de não cumprirem todos os requisitos do serviço qualificado de envio registado eletrónico.

2. Os dados enviados e recebidos com recurso a um serviço qualificado de envio registado eletrónico beneficiam da presunção legal de integridade dos dados, do envio pelo remetente identificado e da receção pelo destinatário identificado dos dados e da exatidão da data e hora de envio e receção dos dados indicados pelo serviço qualificado de envio registado eletrónico.

*Artigo 44.º*

**Requisitos aplicáveis aos serviços qualificados de envio registado eletrónico**

1. Os serviços qualificados de envio registado eletrónico satisfazem os seguintes requisitos:

**▼B**

- a) Serem efetuados por um ou mais prestadores qualificados de serviços de confiança;
- b) Garantirem, com um elevado nível de confiança, a identificação do remetente;
- c) Garantir a identificação do destinatário antes da entrega dos dados;
- d) O envio e a receção dos dados serem securizados por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador qualificado de serviços de confiança, de modo a tornar impossível a alteração dos dados de forma não detetável;
- e) Qualquer alteração a que devam ser sujeitos para o seu envio ou receção ser claramente indicada ao remetente e ao destinatário dos dados;
- f) A data e a hora do envio e da receção, assim como as eventuais alterações dos dados, serem indicadas por meio de um selo temporal qualificado;

Se os dados forem transferidos entre dois ou mais prestadores qualificados de serviços de confiança, os requisitos das alíneas a) a f) serem aplicados a todos eles.

**▼M2**

1-A. O processo de envio e receção de dados que cumpre as normas, especificações e procedimentos referidos no n.º 2 beneficia da presunção de conformidade com os requisitos estabelecidos no n.º 1.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para os processos de envio e receção de dados. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

2-A. Os prestadores de serviços qualificados de envio registado eletrónico podem acordar na interoperabilidade dos serviços qualificados de envio registado eletrónico que prestam. Este quadro de interoperabilidade cumpre os requisitos estabelecidos no n.º 1 e esse cumprimento é atestado por um organismo de avaliação da conformidade.

2-B. O Comissão pode, por meio de atos de execução, estabelecer uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos relativos ao quadro de interoperabilidade a que se refere o n.º 2-A do presente artigo. As especificações técnicas e o conteúdo das normas são eficazes em termos de custos e proporcionados. Os atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B***SECÇÃO 8**Autenticação de sítios web***▼M2***Artigo 45.<sup>o</sup>***Requisitos aplicáveis aos certificados qualificados de autenticação de sítios Web**

1. Os certificados qualificados de autenticação de sítios Web cumprem os requisitos estabelecidos no anexo IV. A avaliação do cumprimento desses requisitos é efetuada em conformidade com as normas, as especificações e os procedimentos referidos no n.<sup>o</sup> 2 do presente artigo.

1-A. Os certificados qualificados de autenticação de sítios Web emitidos em conformidade com o n.<sup>o</sup> 1 do presente artigo são reconhecidos pelos fornecedores de navegadores Web. Os fornecedores de navegadores Web garantem que os dados de identidade atestados no certificado e os atributos adicionais certificados são apresentados de uma forma que facilite a utilização. Os fornecedores de navegadores Web asseguram a compatibilidade e a interoperabilidade com os certificados qualificados de autenticação de sítios Web a que se refere o n.<sup>o</sup> 1 do presente artigo, com exceção das microempresas ou pequenas empresas, na aceção do artigo 2.<sup>o</sup> do anexo da Recomendação 2003/361/CE, durante os primeiros cinco anos de atividade como prestadores de serviços de navegação Web.

1-B. Os certificados qualificados de autenticação de sítios Web não estão sujeitos a requisitos obrigatórios que excedam os requisitos estabelecidos no n.<sup>o</sup> 1.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos relativos aos certificados qualificados de autenticação de sítios Web a que se refere o n.<sup>o</sup> 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>o</sup>, n.<sup>o</sup> 2.

*Artigo 45.<sup>o</sup>-A***Medidas de precaução em matéria de cibersegurança**

1. Os fornecedores de navegadores Web não tomam nenhuma medida contrária às suas obrigações estabelecidas no artigo 45.<sup>o</sup>, nomeadamente os requisitos de reconhecer certificados qualificados de autenticação de sítios Web e de apresentar os dados de identificação fornecidos de uma forma que facilite a utilização.

2. Em derrogação do n.<sup>o</sup> 1 e apenas em caso de preocupações fundamentadas relacionadas com a violação da segurança ou perda de integridade de um certificado ou conjunto de certificados identificados, os fornecedores de navegadores Web podem tomar medidas de precaução em relação a esse certificado ou conjunto de certificados.

3. Caso um fornecedor de um navegador Web tome medidas de precaução nos termos do n.<sup>o</sup> 2, o fornecedor do navegador Web notifica, por escrito, sem demora indevida, as suas preocupações à Comissão, à entidade de controlo competente, à entidade à qual o certificado

**▼M2**

foi emitido e ao prestador qualificado de serviços de confiança que emitiu esse certificado ou conjunto de certificados, juntamente com uma descrição das medidas tomadas para atenuar essas preocupações. Após receção dessa notificação, a entidade de controlo competente envia um aviso de receção ao fornecedor do navegador Web em causa.

4. A entidade de controlo competente averigua as questões suscitadas na notificação nos termos do artigo 46.º-B, n.º 4, alínea k). Se o resultado dessa averiguação não resultar na retirada do estatuto de qualificado do certificado, a entidade de controlo informa o fornecedor do navegador Web em conformidade e solicita a esse fornecedor que ponha termo às medidas de precaução a que se refere o n.º 2 do presente artigo.

*SECÇÃO 9****Certificado eletrónico de atributos****Artigo 45.º-B***Efeitos legais do certificado eletrónico de atributos**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um certificado eletrónico de atributos pelo simples facto de revestir a forma eletrónica ou de não cumprir os requisitos dos certificados eletrónicos qualificados de atributos.

2. Os certificados eletrónicos qualificados de atributos e os certificados de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome têm o mesmo efeito jurídico que os certificados legalmente emitidos em papel.

3. Os certificados de atributos emitidos por ou em nome de um organismo do setor público responsável por uma fonte autêntica num Estado-Membro são reconhecidos em todos os Estados-Membros como certificados de atributos emitidos por ou em nome de um organismo do setor público responsável por uma fonte autêntica.

*Artigo 45.º-C****Certificado eletrónico de atributos em serviços públicos***

Quando o direito nacional exigir uma identificação eletrónica baseada num meio de identificação eletrónica e numa autenticação para aceder a um serviço em linha prestado por um organismo público, os dados de identificação pessoal constantes do certificado eletrónico de atributos não substituem a identificação eletrónica baseada num meio de identificação eletrónica e numa autenticação para fins de identificação eletrónica, salvo se especificamente autorizado pelo Estado-Membro. Nesse caso, também são aceites os certificados eletrónicos qualificados de atributos de outros Estados-Membros.

*Artigo 45.º-D****Requisitos aplicáveis aos certificados eletrónicos qualificados de atributos***

1. O certificado eletrónico qualificado de atributos satisfaz os requisitos estabelecidos no anexo V.

**▼M2**

2. A avaliação do cumprimento dos requisitos estabelecidos no anexo V é efetuada em conformidade com as normas, especificações e procedimentos referidos no n.º 5 do presente artigo.
3. Os certificados eletrónicos qualificados de atributos não podem estar sujeitos a requisitos obrigatórios para além dos requisitos estabelecidos no anexo V.
4. Sempre que os certificados eletrónicos qualificados de atributos tenham sido revogados após a emissão inicial perdem a validade a partir do momento da revogação, não podendo o seu estatuto ser revertido em caso algum.
5. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos relativos aos certificados eletrónicos qualificados de atributos. Os referidos atos de execução são conformes com os atos de execução a que se refere o artigo 5.º-A, n.º 23, relativos à implementação da carteira europeia de identidade digital. São adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 45.º-E***Verificação de atributos por confronto com fontes autênticas**

1. Os Estados-Membros asseguram, no prazo de 24 meses da data da entrada em vigor dos atos de execução referidos no artigo 5.º-A, n.º 23, e no artigo 5.º-C, n.º 6, que, pelo menos em relação aos atributos enumerados no anexo VI, sempre que esses atributos se baseiem em fontes autênticas do setor público, são adotadas medidas que permitem aos prestadores qualificados de serviços de confiança de certificados eletrónicos de atributos verificar esses atributos com recurso a meios eletrónicos, mediante pedido do utente, em conformidade com o direito da União ou nacional.
2. Até 21 de novembro de 2024, a Comissão estabelece, tendo em conta as normas internacionais aplicáveis, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos relativos ao catálogo de atributos, bem como sistemas de certificação de atributos e procedimentos de verificação referentes aos certificados eletrónicos qualificados de atributos para efeitos do n.º 1 do presente artigo. Os referidos atos de execução são conformes com os atos de execução a que se refere o artigo 5.º-A, n.º 23, relativos à implementação da carteira europeia de identidade digital. São adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 45.º-F***Requisitos para o certificado eletrónico de atributos emitido por ou em nome de um organismo do setor público responsável por uma fonte autêntica**

1. Um certificado eletrónico de atributos emitido por ou em nome de um organismo do setor público responsável por uma fonte autêntica satisfaz os seguintes requisitos:

- a) Aqueles estabelecidos no anexo VII;

**▼M2**

b) O certificado qualificado que sustenta a assinatura eletrónica qualificada ou do selo eletrónico qualificado do organismo do setor público a que se refere o artigo 3.º, ponto 46), identificado como o emitente a que se refere o anexo VII, alínea b), contém um conjunto específico de atributos certificados numa forma adequada para o tratamento automático e que:

- i) indica que o organismo emissor está estabelecido, em conformidade com o direito da União ou nacional, como responsável pela fonte autêntica com base na qual é emitido o certificado eletrónico de atributos, ou como organismo designado para agir em seu nome,
- ii) fornece um conjunto de dados que representem inequivocamente a fonte autêntica referida na subalínea i), e
- iii) identifica o direito da União ou nacional referido na subalínea i).

2. O Estado-Membro em que estão estabelecidos os organismos do setor público a que se refere o artigo 3.º, ponto 46), assegura que os organismos do setor público que emitem certificados eletrónicos de atributos têm um nível de fiabilidade e confiança equivalente ao dos prestadores qualificados de serviços de confiança nos termos do artigo 24.º.

3. Os Estados-Membros notificam à Comissão os organismos do setor público referidos no artigo 3.º, ponto 46). Essa notificação inclui um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade que atesta o cumprimento dos requisitos estabelecidos nos n.ºs 1, 2 e 6 do presente artigo. A Comissão disponibiliza ao público, através de um canal seguro, a lista dos organismos do setor público referidos no artigo 3.º, ponto 46), num formato assinado ou selado por via eletrónica, adequado ao tratamento automático.

4. Se um certificado eletrónico de atributos emitido por um organismo do setor público responsável por uma fonte autêntica, ou em seu nome, tiver sido revogado após a emissão inicial, perde a sua validade a partir do momento da sua revogação e o seu estatuto não é revertido.

5. Um certificado eletrónico de atributos emitido por um organismo do setor público responsável por uma fonte autêntica ou em seu nome é considerado conforme com os requisitos estabelecidos no n.º 1 se cumprir as normas, as especificações e os procedimentos referidos no n.º 6.

6. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos relativos a certificados eletrónicos de atributos emitidos por um organismo do setor público responsável por uma fonte autêntica ou em seu nome. Os referidos atos de execução são conformes com os atos de execução a que se refere o artigo 5.º-A, n.º 23, relativos à implementação da carteira europeia de identidade digital. São adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼M2**

7. Até 21 de novembro de 2024, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos para efeitos do n.º 3 do presente artigo. Os referidos atos de execução são conformes com os atos de execução a que se refere o artigo 5.º-A, n.º 23, relativos à implementação da carteira europeia de identidade digital. São adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

8. Os organismos do setor público referidos no artigo 3.º, ponto 46) que emitem o certificado eletrónico qualificado de atributos facultam uma interface com as carteiras europeias de identidade digital fornecidas nos termos do artigo 5.º-A.

*Artigo 45.º-G***Emissão de certificados eletrónicos de atributos para as carteiras europeias de identidade digital**

1. Os fornecedores de certificados eletrónicos de atributos proporcionam aos utentes de carteiras europeias de identidade digital a possibilidade de solicitar, obter, armazenar e gerir o certificado eletrónico de atributos, independentemente do Estado-Membro em que a carteira europeia de identidade digital é fornecida.

2. Os fornecedores de certificados eletrónicos qualificados de atributos facultam uma interface com as carteiras europeias de identidade digital fornecidas nos termos do artigo 5.º-A.

*Artigo 45.º-H***Regras adicionais para a prestação de serviços de certificados eletrónicos de atributos**

1. Os prestadores de serviços qualificados e não qualificados de certificados eletrónicos de atributos não combinam dados pessoais relacionados com a prestação desses serviços com dados pessoais de quaisquer outros serviços que prestem ou que sejam prestados pelos seus parceiros comerciais.

2. Os dados pessoais relacionados com a prestação de serviços de certificados eletrónicos de atributos são logicamente mantidos separados de outros dados detidos pelo fornecedor de certificados eletrónicos de atributos.

3. Os prestadores de serviços de certificados eletrónicos qualificados de atributos implementam a prestação desses serviços de confiança qualificados de uma forma funcionalmente separada de outros serviços que prestam.

*SECÇÃO 10****Serviços de arquivo eletrónico****Artigo 45.º-I***Efeito legal de serviços de arquivo eletrónico**

1. Não podem ser negados efeitos jurídicos nem admissibilidade como prova em processo judicial aos dados eletrónicos nem aos

**▼M2**

documentos eletrónicos conservados através de um serviço de arquivo eletrónico pelo simples facto de revestirem a forma eletrónica ou de não serem conservados através de um serviço qualificado de arquivo eletrónico.

2. Os dados eletrónicos e os documentos eletrónicos conservados através de um serviço qualificado de arquivo eletrónico gozam da presunção da sua integridade e origem durante o período de conservação pelo prestador qualificado de serviços de confiança.

*Artigo 45.<sup>º</sup>-J*

#### **Requisitos aplicáveis aos serviços qualificados de arquivo eletrónico**

1. Os serviços qualificados de arquivo eletrónico satisfazem os seguintes requisitos:

- a) São fornecidos por prestadores qualificados de serviços de confiança;
- b) Utilizam procedimentos e tecnologias capazes de assegurar a durabilidade e a legibilidade de dados eletrónicos e de documentos eletrónicos para além do período de validade tecnológica e, pelo menos, ao longo do período de conservação legal ou contratual, preservando simultaneamente a sua integridade e a precisão da sua origem;
- c) Asseguram que esses dados eletrónicos e esses documentos eletrónicos são conservados de modo a estarem protegidos contra a perda e a alteração, exceto no que diz respeito às alterações do seu suporte ou formato eletrónico;
- d) Permitem que aos utilizadores autorizadas recebam um relatório de forma automatizada que confirme que dados eletrónicos e documentos eletrónicos extraídos de um arquivo eletrónico qualificado beneficiam da presunção de integridade dos dados desde o início do período de conservação até ao momento da sua extração.

O relatório referido na alínea d) do primeiro parágrafo é apresentado de forma fiável e eficiente e ostenta a assinatura eletrónica qualificada ou o selo eletrónico qualificado do prestador do serviço qualificado de arquivo eletrónico.

2. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista das normas de referência e, se necessário, estabelece especificações e procedimentos relativos aos serviços qualificados de arquivo eletrónico. Os serviços de arquivo eletrónico qualificados que cumprem essas normas, especificações e procedimentos beneficiam da presunção de conformidade com os requisitos para serviços de arquivo eletrónico qualificados. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.<sup>º</sup>, n.<sup>º</sup> 2.

*SECÇÃO 11*

#### **Livros-razão eletrónicos**

*Artigo 45.<sup>º</sup>-K*

#### **Efeitos legais dos livros-razão eletrónicos**

1. Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um livro-razão eletrónico pelo simples facto de revestir a forma eletrónica ou de não satisfazer os requisitos dos livros-razão eletrónicos qualificados.

**▼M2**

2. Os registos de dados contidos num livro-razão eletrónico qualificado beneficiam da presunção da sua ordem cronológica única e exata e da sua integridade.

*Artigo 45.º-L*

**Requisitos aplicáveis aos livros-razão eletrónicos qualificados**

1. Os livros-razão eletrónicos qualificados satisfazem os seguintes requisitos:

- a) São criados e geridos por um ou mais prestadores qualificados de serviços de confiança;
- b) Estabelecem a origem dos registos de dados no livro-razão;
- c) Asseguram a ordem cronológica única e sequencial dos registos de dados no livro-razão;
- d) Registam os dados de forma a que qualquer alteração subsequente dos mesmos seja imediatamente detetável, garantindo a sua integridade ao longo do tempo.

2. Os livros-razão eletrónicos que cumprem as normas, especificações e procedimentos referidos no n.º 3 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.º 1.

3. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, uma lista de normas de referência e, se necessário, estabelece especificações e procedimentos relativos aos requisitos estabelecidos no n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

**CAPÍTULO IV  
DOCUMENTOS ELETRÓNICOS**

*Artigo 46.º*

**Efeitos legais dos documentos eletrónicos**

Não podem ser negados efeitos legais nem admissibilidade enquanto prova em processo judicial a um documento eletrónico pelo simples facto de se apresentar em formato eletrónico.

**▼M2**

**CAPÍTULO IV-A  
REGIME DE GOVERNAÇÃO**

*Artigo 46.º-A*

**Supervisão do Regime para a carteira europeia de identidade digital**

1. Os Estados-Membros designam uma ou mais entidades supervisoras estabelecidas no seu território.

As entidades supervisoras designadas nos termos do primeiro parágrafo são dotadas dos poderes necessários e dos recursos adequados para o exercício das suas funções de forma eficaz, eficiente e independente.

**▼M2**

2. Os Estados-Membros notificam à Comissão os nomes e endereços das suas entidades supervisoras designadas nos termos do n.º 1, bem como eventuais alterações subsequentes dos mesmos. A Comissão publica uma lista das entidades supervisoras notificadas.

3. As entidades supervisoras designadas nos termos do n.º 1 têm as seguintes funções:

- a) Supervisionar os fornecedores de carteiras europeias de identidade digital estabelecidos no Estado-Membro que procedeu à designação por forma a garantir, por meio de atividades de supervisão *a priori* e *a posteriori*, que os fornecedores e as carteiras europeias de identidade digital por eles fornecidas cumprem os requisitos estabelecidos no presente regulamento;
- b) Tomar medidas, se necessário, em relação aos fornecedores de carteiras europeias de identidade digital estabelecidos no território do Estado-Membro que procedeu à designação, por meio de atividades de supervisão **a posteriori**, sempre que sejam informados de que os fornecedores ou as carteiras europeias de identidade digital por eles fornecidas violam o presente regulamento.

4. As funções das entidades supervisoras designadas nos termos do n.º 1 incluem nomeadamente:

- a) Colaborar com outras entidades supervisoras e prestar-lhes assistência, nos termos dos artigos 46.º-C e 46.º-E;
- b) Solicitar as informações necessárias para controlar o cumprimento do presente regulamento;
- c) Informar as autoridades competentes dos Estados-Membros em causa, designadas ou criadas nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555, de quaisquer violações significativas da segurança ou perda de integridade de que tomem conhecimento no exercício das suas funções e, em caso de violação significativa da segurança ou perda de integridade que diga respeito a outros Estados-Membros, informar o ponto de contacto único designado ou criado nos termos do artigo 8.º, n.º 3, da Diretiva (UE) 2022/2555 do Estado-Membro em causa e o ponto de contacto único designado nos termos do artigo 46.º-C, n.º 1, do presente regulamento nos restantes Estados-Membros em causa, e informar o público ou exigir que os fornecedores da carteira europeia de identidade digital o façam, caso a entidade supervisora determine que a divulgação da violação da segurança ou da perda de integridade seja do interesse público;
- d) Realizar inspeções no local e efetuar a supervisão fora do local;
- e) Exigir que os fornecedores de carteiras europeias de identidade digital corrijam eventuais incumprimentos dos requisitos previstos no presente regulamento;
- f) Suspender ou cancelar o registo e a inclusão dos utilizadores no mecanismo a que se refere o artigo 5.º-B, n.º 7, em caso de utilização ilegal ou fraudulenta da carteira europeia de identidade digital;
- g) Cooperar com as autoridades de controlo competentes criadas nos termos do artigo 51.º do Regulamento (UE) 2016/679, nomeadamente informando-as sem demora indevida se houver suspeita de as regras de proteção de dados pessoais terem sido violadas e sobre violações da segurança que pareçam constituir violações dos dados pessoais.

**▼M2**

5. Caso a entidade supervisora designada nos termos do n.º 1 exija que o fornecedor de uma carteira europeia de identidade digital corrija qualquer incumprimento dos requisitos previstos no presente regulamento nos termos do n.º 4, alínea e), e esse fornecedor não atue em conformidade e, se aplicável, dentro de um prazo fixado por essa entidade supervisora, a entidade supervisora designada nos termos do n.º 1 pode, tendo em conta, nomeadamente, a extensão, a duração e as consequências desse incumprimento, ordenar ao fornecedor que suspenda ou cesse a disponibilização da carteira europeia de identidade digital. A entidade supervisora informa sem demora indevida as entidades supervisoras dos outros Estados-Membros, a Comissão, os utilizadores e os utentes da carteira europeia de identidade digital da decisão que exige a suspensão ou a cessação do fornecimento da carteira europeia de identidade digital.

6. Até 31 de março de cada ano, as entidades supervisoras designadas nos termos do n.º 1 apresentam à Comissão um relatório sobre as principais atividades do ano civil anterior. A Comissão disponibiliza esse relatório anual ao Parlamento Europeu e ao Conselho.

7. Até 21 de maio de 2025, a Comissão determina, por meio de atos de execução, os formatos e procedimentos aplicáveis ao relatório a que se refere o n.º 6 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 46.º-B***Supervisão dos serviços de confiança**

1. Os Estados-Membros designam uma entidade supervisora estabelecida no seu território ou designam, de comum acordo com outro Estado-Membro, uma entidade supervisora estabelecida nesse outro Estado-Membro. Essa entidade supervisora é responsável pelas funções de supervisão no Estado-Membro que procedeu à designação no que diz respeito aos serviços de confiança.

As entidades supervisoras designadas nos termos do primeiro parágrafo são dotadas dos poderes necessários e dos recursos adequados para o exercício das suas funções.

2. Os Estados-Membros notificam à Comissão os nomes e endereços das entidades supervisoras designadas nos termos do n.º 1, bem como quaisquer alterações subsequentes dos mesmos. A Comissão publica uma lista das entidades supervisoras notificadas.

3. As entidades supervisoras designadas nos termos do n.º 1 têm as seguintes funções:

- a) Supervisionar os prestadores qualificados de serviços de confiança estabelecidos no território do Estado-Membro que procedeu à designação e assegurar, por meio de atividades de supervisão *a priori* e *a posteriori*, que os prestadores qualificados de serviços de confiança e os serviços de confiança qualificados por eles prestados cumprim os requisitos estabelecidos no presente regulamento;
- b) Se necessário, tomar medidas face aos prestadores não qualificados de serviços de confiança estabelecidos no território do Estado-Membro que procedeu à designação, por meio de atividades de supervisão *a posteriori*, se for informado que os ditos prestadores ou os serviços de confiança por eles prestados não cumprim os requisitos estabelecidos no presente regulamento.

**▼M2**

4. As funções da entidade supervisora designada nos termos do n.º 1 incluem nomeadamente:

- a) Informar as autoridades competentes dos Estados-Membros em causa, designadas ou criadas nos termos do artigo 8.º, n.º 1, da Diretiva (UE) 2022/2555, de qualquer violação significativa da segurança ou perda de integridade de que tome conhecimento no exercício das suas funções e, em caso de violação significativa da segurança ou perda de integridade que diga respeito a outros Estados-Membros, informar o ponto de contacto único designado ou criado nos termos do artigo 8.º, n.º 3, da Diretiva (UE) 2022/2555 do Estado-Membro em causa e os pontos de contacto único designados nos termos do artigo 46.º-C, n.º 1, do presente regulamento nos restantes Estados-Membros em causa, e informar o público ou exigir que o prestador de serviços de confiança o faça, caso a entidade supervisora determine que a divulgação da violação da segurança ou da perda de integridade seja do interesse público;
- b) Colaborar com outras entidades supervisoras e prestar-lhes assistência, nos termos dos artigos 46.º-C e 46.º-E;
- c) Analisar os relatórios de avaliação da conformidade referidos no artigo 20.º, n.º 1, e no artigo 21.º, n.º 1;
- d) Apresentar à Comissão relatório sobre as suas atividades principais, nos termos do n.º 6;
- e) Realizar auditorias ou solicitar a organismos de avaliação da conformidade que efetuam avaliações da conformidade de prestadores qualificados de serviços de confiança, nos termos do artigo 20.º, n.º 2;
- f) Cooperar com as autoridades de controlo competentes criadas nos termos do artigo 51.º do Regulamento (UE) 2016/679, nomeadamente informando-as, sem demora indevida, se houver suspeita de as regras de proteção de dados pessoais terem sido violadas e sobre violações da segurança que pareçam constituir violações dos dados pessoais;
- g) Atribuir e retirar o estatuto de qualificado aos prestadores de serviços de confiança e aos serviços por eles prestados, nos termos dos artigos 20.º e 21.º;
- h) Informar a entidade responsável pela lista de confiança nacional referida no artigo 22.º, n.º 3, das suas decisões de atribuir ou retirar o estatuto de qualificado, exceto se a referida entidade for a própria entidade supervisora designada nos termos do n.º 1 do presente artigo;
- i) Verificar a existência e correta aplicação das disposições sobre os planos de cessação quando o prestador qualificado de serviços de confiança cesse a sua atividade, nomeadamente a forma como é garantido o acesso à informação, nos termos do artigo 24.º, n.º 2, alínea h);
- j) Exigir que os prestadores de serviços de confiança corrijam os eventuais incumprimentos dos requisitos previstos no presente regulamento;

**▼M2**

k) Investigar as alegações apresentadas pelos fornecedores de navegadores Web nos termos do artigo 45.º-A e tomar medidas, se necessário.

5. Os Estados-Membros podem exigir que a entidade supervisora designada nos termos do n.º 1 crie, conserve e atualize uma infraestrutura de confiança de acordo com o direito nacional.

6. Até 31 de março de cada ano, as entidades supervisoras designadas nos termos do n.º 1 apresentam à Comissão um relatório sobre as principais atividades do ano civil anterior. A Comissão disponibiliza o referido relatório anual ao Parlamento Europeu e ao Conselho.

7. Até 21 de maio de 2025, a Comissão adota orientações sobre o exercício, pelas entidades supervisoras designadas nos termos do n.º 1 do presente artigo, das funções a que se refere o n.º 4 do presente artigo e, por meio de atos de execução, estabelece os formatos e procedimentos aplicáveis ao relatório a que se refere o n.º 6 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

*Artigo 46.º-C*

**Pontos de contacto único**

1. Cada Estado-Membro designa um ponto de contacto único para os serviços de confiança, as carteiras europeias de identidade digital e os sistemas de identificação eletrónica notificados.

2. Cada ponto de contacto único exerce uma função de ligação para facilitar a cooperação transfronteiriça entre as entidades supervisoras dos prestadores de serviços de confiança e entre as entidades supervisoras dos fornecedores de carteiras europeias de identidade digital e, se for caso disso, com a Comissão e a Agência da União Europeia para a Cibersegurança (ENISA) e com outras autoridades competentes no seu Estado-Membro.

3. Cada Estado-Membro torna público e, sem demora indevida, notifica à Comissão os nomes e endereços do ponto de contacto único designado nos termos do n.º 1, bem como quaisquer alterações subsequentes dos mesmos.

4. A Comissão publica uma lista dos pontos de contacto único notificados nos termos do n.º 3.

*Artigo 46.º-D*

**Assistência mútua**

1. A fim de facilitar a supervisão e o cumprimento das obrigações decorrentes do presente regulamento, as entidades supervisoras designadas nos termos dos artigos 46.º-A, n.º 1, e 46.º-B, n.º 1, podem solicitar, nomeadamente através do grupo de cooperação criado nos termos do artigo 46.º-E, n.º 1, a assistência mútua das entidades supervisoras de outro Estado-Membro onde o fornecedor da carteira europeia de identidade digital ou o prestador de serviços de confiança está estabelecido, ou onde as suas redes e sistemas de informação estão localizados ou onde são prestados os seus serviços.

2. A assistência mútua implica, pelo menos, que:

**▼M2**

- a) A entidade supervisora que aplica medidas de supervisão e de execução num Estado-Membro informa e consulta a entidade supervisora do outro Estado-Membro em causa;
- b) Uma entidade supervisora pode solicitar à entidade supervisora de outro Estado-Membro em causa que tome medidas de supervisão ou de execução, incluindo, por exemplo, pedidos de realização de inspeções relacionadas com os relatórios de avaliação da conformidade a que se referem os artigos 20.º e 21.º relativos à prestação de serviços de confiança;
- c) Se for caso disso, as entidades supervisoras podem realizar investigações conjuntas com as entidades supervisoras de outros Estados-Membros.

As disposições e os procedimentos aplicáveis às ações conjuntas ao abrigo do primeiro parágrafo são accordadas e estabelecidas pelos Estados-Membros em causa nos termos do seu direito nacional.

3. A entidades supervisora à qual tenham sido dirigidos pedidos de assistências pode indeferi-los por qualquer dos seguintes motivos:

- a) A assistência solicitada não é proporcional às atividades de supervisão da entidade supervisora realizadas nos termos do disposto nos artigos 46.º-A e 46.º-B;
- b) A entidade supervisora não é competentes para prestar a assistência solicitada;
- c) Prestar a assistência solicitada seria incompatível com o presente regulamento.

4. Até 21 de maio de 2025 e, posteriormente, de dois em dois anos, o grupo de cooperação criado nos termos do artigo 46.º-E, n.º 1, emite orientações sobre os aspetos organizacionais e os procedimentos de assistência mútua a que se referem os n.os 1 e 2 do presente artigo.

*Artigo 46.º-E*

**Grupo de Cooperação Europeia para a Identidade Digital**

1. A fim de apoiar e facilitar a cooperação transfronteiriça e o intercâmbio de informações entre os Estados-Membros sobre serviços de confiança, carteiras europeias de identidade digital e sistemas de identificação eletrónica notificados, a Comissão cria um Grupo de Cooperação Europeia para a Identidade Digital («grupo de cooperação»).

2. O grupo de cooperação é composto por representantes designados pelos Estados-Membros e da Comissão. O grupo de cooperação é presidido pela Comissão. A Comissão assegura o secretariado do grupo de cooperação.

3. Os representantes das partes interessadas pertinentes podem, numa base ad hoc, ser convidados a assistir às reuniões do grupo de cooperação e a participar nos seus trabalhos na qualidade de observadores.

4. A ENISA é convidada a participar, na qualidade de observador, nos trabalhos do grupo de cooperação sempre que este proceder à troca de pontos de vista, boas práticas e informações sobre aspetos relevantes de cibersegurança, como a notificação de violações da segurança, e quando for abordada a utilização de certificados ou normas de cibersegurança.

5. As funções do grupo de cooperação são as seguintes:

**▼M2**

- a) Proceder ao intercâmbio de aconselhamentos e cooperar com a Comissão sobre iniciativas estratégicas emergentes no domínio das carteiras de identidade digital, dos meios de identificação eletrónica e dos serviços de confiança;
  - b) Aconselhar a Comissão, se for caso disso, na fase incipiente da elaboração de projetos de atos de execução e de atos delegados a adotar nos termos do presente regulamento;
  - c) A fim de apoiar as entidades supervisoras na aplicação das disposições do presente regulamento:
    - i) proceder ao intercâmbio de boas práticas e informações sobre a aplicação das disposições do presente regulamento,
    - ii) analisar os aspetos importantes da evolução nos setores da carteira de identidade digital, da identificação eletrónica e dos serviços de confiança,
    - iii) organizar reuniões conjuntas com partes interessadas de toda a União para discutir as atividades desenvolvidas pelo grupo de cooperação e partilhar pontos de vista sobre novos desafios políticos,
    - iv) com o apoio da ENISA, proceder à troca de pontos de vista, boas práticas e informações sobre os aspetos de cibersegurança pertinentes relativos às carteiras europeias de identidade digital, aos sistemas de identificação eletrónica e aos serviços de confiança,
    - v) proceder ao intercâmbio boas práticas relativamente ao desenvolvimento e à aplicação de políticas em matéria de notificação de violações da segurança e medidas comuns a que se referem os artigos 5.º-E e 10.º,
    - vi) organizar reuniões conjuntas com o grupo de cooperação SRI criado nos termos do artigo 14.º, n.º 1, da Diretiva (UE) 2022/2555 para proceder ao intercâmbio de informações pertinentes em relação aos serviços de confiança e à identificação eletrónica relacionadas com ciberameaças, incidentes, vulnerabilidades, iniciativas de sensibilização, ações de formação, exercícios e competências, reforço das capacidades, capacidade em matéria de normas e especificações técnicas, bem como normas e especificações técnicas,
    - vii) debater, a pedido de uma entidade supervisora, os pedidos específicos de assistência mútua a que se refere o artigo 46.º-D,
    - viii) facilitar o intercâmbio de informações entre as entidades supervisoras, fornecendo orientações sobre os aspetos organizacionais e os procedimentos de assistência mútua a que se refere o artigo 46.º-D;
  - d) Organizar as avaliações pelos pares dos sistemas de identificação eletrónica a notificar nos termos presente regulamento.
6. Os Estados-Membros garantem a cooperação eficaz e eficiente dos respetivos representantes designados no grupo de cooperação.

**▼M2**

7. Até 21 de maio de 2025, a Comissão estabelece, por meio de atos de execução, as necessárias disposições processuais de facilitação da cooperação entre os Estados-Membros a que se refere o n.º 5 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

**▼B**

## CAPÍTULO V

## DELEGAÇÕES DE PODER E DISPOSIÇÕES DE EXECUÇÃO

*Artigo 47.º*

**Exercício da delegação**

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

**▼M2****▼C1**

2. O poder de adotar atos delegados referido no artigo 5.º-C, n.º 8, no artigo 24.º, n.º 4.º-B, e no artigo 30.º, n.º 4, é conferido à Comissão por tempo indeterminado a contar de 17 de setembro de 2014.

3. A delegação de poderes referida no artigo 5.º-C, n.º 8, no artigo 24.º, n.º 4.º-B, e no artigo 30.º, n.º 4, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

**▼B**

4. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

**▼M2****▼C1**

5. Os atos delegados adotados nos termos do artigo 5.º-C, n.º 8, do artigo 24.º, n.º 4.º-B, ou do artigo 30.º, n.º 4, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

**▼B**

*Artigo 48.º*

**Procedimento de comité**

1. A Comissão é assistida por um comité. Esse comité deve ser entendido como comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

**▼B**

CAPÍTULO VI  
DISPOSIÇÕES FINAIS

**▼M2***Artigo 48.<sup>º</sup>-A***Obrigações de comunicação de informações**

1. Os Estados-Membros asseguram a recolha de estatísticas relativas ao funcionamento das carteiras europeias de identidade digital e dos serviços de confiança qualificados prestados no seu território.
2. As estatísticas recolhidas em conformidade com o disposto no n.º 1 incluem o seguinte:
  - a) O número de pessoas singulares e coletivas que têm uma carteira europeia de identidade digital válida;
  - b) O tipo e número de serviços que aceitam a utilização da carteira europeia de identidade digital;
  - c) O número de queixas dos utentes e incidentes em matéria de proteção dos consumidores ou de proteção de dados relacionados com os utilizadores e os serviços de confiança qualificados;
  - d) Um relatório de síntese, incluindo dados sobre incidentes que impedem a utilização da carteira europeia de identidade digital;
  - e) Um resumo dos incidentes de segurança significativos, violações de dados e utentes afetados das carteiras europeias de identidade digital ou dos serviços de confiança qualificados.
3. As estatísticas a que se refere o n.º 2 são postas à disposição do público num formato aberto, de uso corrente e legível por máquina.
4. Até 31 de março de cada ano, os Estados-Membros apresentam à Comissão um relatório relativo às estatísticas recolhidas em conformidade com o n.º 2.

*Artigo 49.<sup>º</sup>***Revisão**

1. A Comissão analisa a aplicação do presente regulamento e, até 21 de maio de 2026, apresenta um relatório ao Parlamento Europeu e ao Conselho. Nesse relatório, a Comissão avalia nomeadamente se é adequado modificar o âmbito de aplicação do presente regulamento ou as suas disposições especiais, nomeadamente as disposições incluídas no artigo 5.<sup>º</sup>-C, n.º 5, tendo em conta a experiência adquirida na aplicação do presente regulamento, bem como os desenvolvimentos tecnológicos, do mercado e jurídicos. Se necessário, esse relatório é acompanhado de uma proposta de alteração do presente regulamento.
2. O relatório a que se refere o n.º 1 inclui uma avaliação da disponibilidade, segurança e usabilidade dos meios de identificação eletrónica notificados e das carteiras europeias de identidade digital abrangidas pelo âmbito de aplicação do presente regulamento e afere se

**▼M2**

todos os prestadores privados de serviços em linha que dependem de serviços de identificação eletrónica de terceiros para a autenticação de utentes devem ser obrigados a aceitar a utilização dos meios de identificação eletrónica notificados e da carteira europeia de identidade digital.

3. Até 21 de maio de 2030 e, posteriormente, de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre os progressos realizados na consecução dos objetivos do presente regulamento.

**▼B***Artigo 50.º***Revogação**

1. A Diretiva 1999/93/CE é revogada com efeitos a partir de 1 de julho de 2016.

2. As referências à diretiva revogada são consideradas referências ao presente regulamento.

**▼M2***Artigo 51.º***Medidas transitórias**

1. Os dispositivos seguros de criação de assinaturas cuja conformidade tenha sido determinada nos termos do artigo 3.º, n.º 4, da Diretiva 1999/93/CE continuam a ser considerados dispositivos qualificados de criação de assinaturas eletrónicas na aceção do presente regulamento até 21 de maio de 2027.

2. Os certificados qualificados emitidos a pessoas singulares em conformidade com a Diretiva 1999/93/CE continuam a ser considerados certificados qualificados de assinatura eletrónica na aceção do presente regulamento até 21 de maio de 2026.

3. A gestão de dispositivos qualificados de criação de assinaturas e selos eletrónicos à distância por prestadores qualificados de serviços de confiança que não os prestadores qualificados de serviços de confiança que prestam serviços de confiança qualificados para a gestão de dispositivos qualificados de criação de assinaturas eletrónicas e selos eletrónicos à distância em conformidade com os artigos 29.º-A e 39.º-A pode ser realizada sem necessidade de obter o estatuto de qualificado para a prestação desses serviços de gestão até 21 de maio de 2026.

4. Os prestadores qualificados de serviços de confiança aos quais tenha sido concedido o estatuto de qualificado ao abrigo do presente regulamento antes de 20 de maio de 2024, apresentam à entidade supervisora um relatório de avaliação da conformidade que comprove a conformidade com o artigo 24.º, n.os 1, 1-A e 1-B, o mais rapidamente possível e, em qualquer caso, até 21 de maio de 2026.

**▼B***Artigo 52.º***Entrada em vigor**

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

2. O presente regulamento é aplicável a partir de 1 de julho de 2016, com as seguintes exceções:

**▼B**

- a) Os artigos 8.º, n.º 3, 9.º, n.º 5, 12.º, n.os 2 a 9, 17.º, n.º 8, 19.º, n.º 4, 20.º, n.º 4, 21.º, n.º 4, 22.º, n.º 5, 23.º, n.º 3, 24.º, n.º 5, 27.º, n.º 4 e n.º 5, 28.º, n.º 6, 29.º, n.º 2, 30.º, n.º 3 e n.º 4, 31.º, n.º 3, 32.º, n.º 3, 33.º, n.º 2, 34.º, n.º 2, 37.º, n.º 4 e n.º 5, 38.º, n.º 6, 42.º, n.º 2, 44.º, n.º 2, 45.º, n.º 2, 47.º e 48.º são aplicáveis a partir de 17 de setembro de 2014;
- b) Os artigos 7.º, 8.º, n.os 1 e 2, 9.º, 10.º, 11.º e 12.º, n.º 1, são aplicáveis a partir da data de aplicação dos atos de execução referidos nos artigos 8.º, n.º 3, e 12.º, n.º 8;
- c) O artigo 6.º é aplicável três anos após a data de aplicação dos atos de execução referidos nos artigos 8.º, n.º 3, e 12.º, n.º 8.

3. Se o sistema de identificação eletrónica notificado for incluído na lista publicada pela Comissão nos termos do artigo 9.º antes da data referida no n.º 2, alínea c), o reconhecimento dos meios de identificação eletrónica que integram esse sistema nos termos do artigo 6.º é efetuado num prazo de 12 meses após a publicação do sistema, mas não antes da data referida no n.º 2, alínea c).

4. Não obstante o n.º 2, alínea c), os Estados-Membros podem decidir que os meios de identificação eletrónica que integram um sistema de identificação eletrónica notificado por outro Estado-Membro nos termos do artigo 9.º, n.º 1, são reconhecidos no primeiro Estado-Membro a partir da data de aplicação dos atos de execução referidos nos artigos 8.º, n.º 3, e 12.º, n.º 8. Os Estados-Membros que decidam fazê-lo informam a Comissão desse facto. A Comissão torna públicas essas informações.

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

**▼B***ANEXO I***REQUISITOS APLICÁVEIS AOS CERTIFICADOS QUALIFICADOS DE ASSINATURA ELETRÓNICA**

Os certificados qualificados de assinatura eletrónica contêm:

- a) Uma indicação, pelo menos num formato adequado ao tratamento automático, de que o certificado foi emitido como certificado qualificado de assinatura eletrónica;
- b) Um conjunto de dados que representem inequivocamente o prestador qualificado de serviços de confiança que tiver emitido os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontre estabelecido e
  - para as pessoas coletivas: a designação e, eventualmente, o número de registo conforme constam dos registos oficiais,
  - para as pessoas singulares: o nome;
- c) Pelo menos, o nome do signatário, ou um pseudónimo, caso seja utilizado um pseudónimo, este deve ser claramente indicado;
- d) Os dados necessários para a validação da assinatura eletrónica que correspondam aos dados necessários para a criação da assinatura eletrónica;
- e) A indicação do início e do termo da validade do certificado;
- f) O código de identidade do certificado, que deve estar associado de modo único ao prestador qualificado de serviços de confiança;
- g) A assinatura eletrónica avançada ou o selo eletrónico avançado do prestador qualificado de serviços de confiança emitente;
- h) O local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado a que se refere a alínea g);

**▼M2**

- i) A informação ou a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado qualificado;

**▼B**

- j) Se os dados para a criação da assinatura eletrónica relacionados com os dados para a validação da assinatura eletrónica se encontrarem num dispositivo qualificado de criação de assinatura eletrónica, uma indicação adequada desse facto, pelo menos num formato adequado para tratamento automático.

**▼B**

*ANEXO II*

**REQUISITOS APLICÁVEIS AOS DISPOSITIVOS QUALIFICADOS DE CRIAÇÃO DE ASSINATURAS ELETRÓNICAS**

1. Os dispositivos qualificados de criação de assinaturas eletrónicas asseguram, pelos meios técnicos e procedimentais adequados, que pelo menos:
  - a) A confidencialidade dos dados necessários para a criação de assinaturas eletrónicas utilizados para criar as assinaturas eletrónicas esteja razoavelmente assegurada;
  - b) Os dados necessários para a criação de assinaturas eletrónicas utilizados para criar assinaturas eletrónicas só possam, na prática, ocorrer uma vez;
  - c) Os dados necessários para a criação de assinaturas eletrónicas utilizados para criar as assinaturas eletrónicas não possam, com uma segurança razoável, ser deduzidos de outros dados e que as assinaturas estejam protegidas eficazmente contra falsificações produzidas por meio de tecnologias atualmente disponíveis;
  - d) Os dados necessários para a criação de assinaturas eletrónicas utilizados para criar as assinaturas eletrónicas possam ser eficazmente protegidos pelo signatário legítimo contra a utilização por terceiros.
2. Os dispositivos qualificados de criação de assinaturas eletrónicas não podem alterar os dados a assinar nem impedir que esses dados sejam apresentados ao signatário antes da assinatura.

**▼M2**

---

**▼B***ANEXO III***REQUISITOS APLICÁVEIS AOS CERTIFICADOS QUALIFICADOS DE SELOS ELETRÓNICOS**

Os certificados qualificados de selos eletrónicos contêm:

- a) Uma indicação, pelo menos num formato adequado para tratamento automático, de que o certificado foi emitido como certificado qualificado de selo eletrónico;
- b) Um conjunto de dados que representem inequivocamente o prestador qualificado de serviços de confiança que tiver emitido os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontre estabelecido e
  - para as pessoas coletivas: a designação e, eventualmente, o número de registo conforme constam dos registos oficiais,
  - para as pessoas singulares: o nome;
- c) Pelo menos o nome do criador do selo e, eventualmente, o número de registo, conforme constam dos registos oficiais;
- d) Os dados necessários para a validação do selo eletrónico que correspondam aos dados necessários para a criação do selo eletrónico;
- e) A indicação do início e do termo da validade do certificado;
- f) O código de identidade do certificado, que deve estar associado de modo único ao prestador qualificado de serviços de confiança;
- g) A assinatura eletrónica avançada ou o selo eletrónico avançado do prestador qualificado de serviços de confiança emitente;
- h) O local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado a que se refere a alínea g);

**▼M2**

- i) A informação ou a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado qualificado;

**▼B**

- j) Se os dados para a criação do selo eletrónico relacionados com os dados para a validação do selo eletrónico se encontrarem num dispositivo qualificado de criação de selo eletrónico, uma indicação adequada desse facto, pelo menos num formato adequado ao tratamento automático.

**▼B***ANEXO IV***REQUISITOS APLICÁVEIS AOS CERTIFICADOS QUALIFICADOS DE AUTENTICAÇÃO DE SÍTIOS**

Os certificados qualificados de autenticação de sítios *web* contêm:

- a) Uma indicação, pelo menos num formato adequado para tratamento automático, de que o certificado foi emitido como certificado qualificado para autenticação de sítios *web*;
- b) Um conjunto de dados que representem inequivocamente o prestador qualificado de serviços de confiança que tiver emitido os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontre estabelecido e
  - para as pessoas coletivas: a designação e, eventualmente, o número de registo conforme constam dos registos oficiais,
  - para as pessoas singulares: o nome;

**▼M2**

- c) Para as pessoas singulares: pelo menos o nome, ou um pseudónimo, da pessoa à qual o certificado foi emitido; caso seja utilizado um pseudónimo, este deve ser claramente indicado como tal;
- c-A) Para as pessoas coletivas: um conjunto único de dados que representem inequivocamente a pessoa coletiva à qual o certificado é emitido, com, pelo menos o nome da pessoa coletiva à qual o certificado é emitido e, eventualmente, o número de registo, conforme constam dos registos oficiais;

**▼B**

- d) Elementos do endereço, incluindo, pelo menos, a cidade e o Estado, da pessoa singular ou coletiva à qual o certificado é emitido, eventualmente conforme constam dos registos oficiais;
- e) O nome ou os nomes de domínio explorados pela pessoa singular ou coletiva à qual o certificado é emitido;
- f) A indicação do início e do termo da validade do certificado;
- g) O código de identidade do certificado, que deve estar associado de modo único ao prestador qualificado de serviços de confiança;
- h) A assinatura eletrónica avançada ou o selo eletrónico avançado do prestador qualificado de serviços de confiança emitente;
- i) O local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado a que se refere a alínea h);

**▼M2**

- j) A informação ou a localização dos serviços que conferem a validade ao certificado e aos quais se pode recorrer para inquirir da validade do certificado qualificado.

**▼M2***ANEXO V*

**REQUISITOS APLICÁVEIS AOS CERTIFICADOS ELETRÓNICOS  
QUALIFICADOS DE ATRIBUTOS**

Os certificados eletrónicos qualificados de atributos contêm:

- a) Uma indicação, pelo menos num formato adequado ao tratamento automático, de que o certificado foi emitido como certificado eletrónico qualificado de atributos;
- b) Um conjunto de dados que representem inequivocamente o prestador qualificado de serviços de confiança que tiver emitido os certificados eletrónicos qualificados de atributos, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontre estabelecido e:
  - i) para as pessoas coletivas: a designação e, eventualmente, o número de registo conforme constam dos registos oficiais;
  - ii) para as pessoas singulares: o nome da pessoa;
- c) Um conjunto de dados que representem inequivocamente a entidade à qual os atributos certificados se referem; caso seja utilizado um pseudónimo, este deve ser claramente indicado como tal;
- d) O ou os atributos certificados, incluindo, se for caso disso, as informações necessárias para identificar o âmbito desses atributos;
- e) A indicação do início e do termo da validade do certificado;
- f) O código de identificação do certificado, que deve ser único para o prestador qualificado de serviços de confiança e, se aplicável, a indicação do sistema de certificação de que o certificado de atributos faz parte;
- g) A assinatura eletrónica qualificada ou o selo eletrónico qualificado do prestador qualificado de serviços de confiança emitente;
- h) O local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica qualificada ou o selo eletrónico qualificado a que se refere a alínea g);
- i) A informação ou a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado qualificado.

▼M2

*ANEXO VI*

**LISTA MÍNIMA DE ATRIBUTOS**

Em conformidade com o artigo 45.º-E, os Estados-Membros asseguram que sejam tomadas medidas que permitam aos prestadores qualificados de serviços de confiança de certificados eletrónicos de atributos verificar por via eletrónica, a pedido do utente, a autenticidade dos seguintes atributos, por confronto com a fonte autêntica pertinente a nível nacional ou através de intermediários designados reconhecidos a nível nacional, em conformidade com o direito nacional ou da União, e caso esses atributos se baseiem em fontes autênticas do setor público:

1. Endereço;
2. Idade;
3. Género;
4. Estado civil;
5. Composição do agregado familiar;
6. Nacionalidade ou cidadania;
7. Habilidades literárias, títulos e licenças;
8. Qualificações profissionais, títulos e licenças;
9. Poderes e mandatos para representar pessoas singulares ou coletivas;
10. Autorizações e licenças públicas;
11. Para as pessoas coletivas, dados financeiros e das empresas.

**▼M2***ANEXO VII*

**REQUISITOS PARA O CERTIFICADO ELETRÓNICO DE ATRIBUTOS  
EMITIDO POR UM ORGANISMO DO SETOR PÚBLICO  
RESPONSÁVEL POR UMA FONTE AUTÊNTICA OU EM SEU NOME**

Um certificado eletrónico de atributos emitido por um organismo público responsável por uma fonte autêntica ou em seu nome contém:

- a) Uma indicação, pelo menos numa forma adequada ao tratamento automático, de que o certificado foi emitido sob a forma de certificado eletrónico de atributos, emitido por um organismo público responsável por uma fonte autêntica ou em seu nome;
- b) Um conjunto de dados que representem inequivocamente o organismo público que emite o certificado eletrónico de atributos, incluindo, pelo menos, o Estado-Membro em que esse organismo público está estabelecido e o seu nome e, se for caso disso, o seu número de registo, tal como indicado nos registos oficiais;
- c) Um conjunto de dados que representem inequivocamente a entidade a que os atributos certificados se referem; caso seja utilizado um pseudónimo, este deve ser claramente indicado como tal;
- d) O atributo ou os atributos certificados, incluindo, se for caso disso, as informações necessárias para identificar o âmbito desses atributos;
- e) A indicação do início e do termo da validade do certificado;
- f) O código de identificação do certificado, que deve ser único para o organismo público emitente e, se aplicável, uma indicação do sistema de certificação do qual o certificado de atributos faz parte;
- g) A assinatura eletrónica qualificada ou o selo eletrónico qualificado do organismo emitente;
- h) O local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica qualificada ou o selo eletrónico qualificado a que se refere a alínea g);
- i) A informação ou a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado.