



Bruxelas, 25 de novembro de 2022
(OR. en)

14959/22

**Dossiê interinstitucional:
2021/0136(COD)**

LIMITE

**TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774**

NOTA

de:	Comité de Representantes Permanentes (1.ª Parte)
para:	Conselho
n.º doc. ant.:	14344/22
n.º doc. Com.:	9471/21
Assunto:	Proposta de regulamento do Parlamento Europeu e do Conselho que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação de um Quadro Europeu para a Identidade Digital – Orientação geral

I. INTRODUÇÃO

1. Em 3 de junho de 2021, a Comissão adotou a proposta de regulamento relativo à identidade digital europeia¹. Esta iniciativa altera o Regulamento eIDAS de 2014², que criou as bases necessárias para o acesso a serviços e a realização de transações de forma segura, em linha e além-fronteiras na UE.

¹ Doc. 9471/21.

² [Regulamento \(EU\) n.º 910/2014](#).

2. A proposta, baseada no artigo 114.º do TFUE, exige que os Estados-Membros emitam uma carteira europeia de identidade digital no quadro de um sistema de identificação eletrónica notificado, fundado em normas técnicas comuns, e após certificação obrigatória. A fim de criar a arquitetura técnica necessária, acelerar a execução do regulamento revisto, fornecer orientações aos Estados-Membros e evitar a fragmentação, a proposta vinha acompanhada de uma recomendação relativa à elaboração de um conjunto de instrumentos a nível da União.
3. A proposta de regulamento visa assegurar às pessoas e às empresas um acesso universal a soluções de identificação e autenticação eletrónicas seguras e fiáveis, através de uma carteira digital pessoal no telemóvel.

II. TRABALHOS NAS OUTRAS INSTITUIÇÕES

1. No Parlamento Europeu, a proposta foi remetida para a Comissão da Indústria, da Investigação e da Energia (ITRE) com três comissões associadas para emissão de pareceres, a saber, a Comissão do Mercado Interno e da Proteção dos Consumidores (IMCO), a Comissão dos Assuntos Jurídicos (JURI) e a Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos (LIBE). A relatora do dossiê é Romana Jerković (S&D, Croácia). A Comissão ITRE ainda não adotou o seu relatório.
2. Em 15 de julho de 2021, solicitou-se ao Comité Económico e Social Europeu o seu parecer sobre a proposta, que foi emitido a 20 de outubro de 2021. Em 12 de outubro de 2021, o Comité das Regiões Europeu emitiu parecer sobre a proposta, por mote próprio.
3. Em 28 de julho de 2021, a Autoridade Europeia para a Proteção de Dados (AEPD) publicou observações formais sobre a proposta.

III. PONTO DA SITUAÇÃO NO CONSELHO

1. No Conselho, a proposta foi analisada pelo Grupo das Telecomunicações e da Sociedade da Informação (a seguir designado por "Grupo TELECOM"), que deu início aos debates durante a Presidência portuguesa em junho de 2021. A análise da proposta no Grupo TELECOM prosseguiu durante a Presidência eslovena, tendo a primeira leitura ficado concluída com êxito em 15 de novembro de 2021.
2. A Presidência francesa apresentou a sua **primeira proposta de compromisso** em 15 de fevereiro e 5 de abril e a **segunda** foi debatida em 23 de maio e 9 de junho. No contexto de um debate de orientação realizado no Grupo TELECOM em 19 de julho de 2022, a Presidência checa – com base nos trabalhos da Presidência francesa – destacou as principais questões de alto nível pendentes e solicitou às delegações que expusessem as suas opções preferidas, com vista a reformular as partes pertinentes da segunda proposta de compromisso em conformidade. A versão revista resultou numa **terceira proposta de compromisso** que foi apresentada pela Presidência checa ao Grupo TELECOM em 5 e 8 de setembro. Iterações adicionais e ajustes conexos promoveram com êxito um nível mais profundo de convergência na maior parte das questões pendentes.
3. Contudo, a **quarta proposta de compromisso**, apresentada às delegações no Grupo TELECOM em 28 de setembro, revelou divergências persistentes entre os Estados-Membros em torno de uma questão de alto nível específica, nomeadamente o nível de garantia escolhido para a carteira europeia de identidade digital. Alguns Estados-Membros que já dispõem de um sistema nacional de identificação eletrónica adotaram inicialmente, e investiram subsequentemente, num nível de garantia "substancial", ao passo que na atual proposta relativa à identidade digital europeia é exigido um nível de garantia "elevado". Tendo conhecimento que existe um elevado número de meios de identificação eletrónica com um nível de garantia "substancial" emitidos em alguns Estados-Membros, a Presidência checa propôs ainda um mecanismo para facilitar a integração dos utilizadores, contribuindo assim para a adoção de carteiras europeias de identidade digital. A disposição permite que os utilizadores se inscrevam na carteira europeia de identidade digital utilizando os meios nacionais de identificação eletrónica existentes com o nível de garantia "substancial" em conjugação com procedimentos adicionais de integração que, em conjunto, cumprem os requisitos do nível de garantia "elevado". As especificações técnicas e operacionais estão sujeitas à legislação de execução e a conformidade com os requisitos deve ser certificada.

4. A **quinta proposta de compromisso** foi debatida na reunião do Grupo TELECOM de 25 de outubro. Na reunião do Grupo TELECOM de 8 de novembro de 2022, a Presidência checa apresentou as poucas alterações introduzidas e, na sequência das observações e sugestões de redação adicionais recebidas das delegações, preparou a **versão final do texto de compromisso** tendo em vista a sua apresentação ao Coreper.
5. Em 18 de novembro, o Coreper analisou esta proposta de compromisso e **acordou por unanimidade em apresentá-la ao Conselho TTE (Telecomunicações), sem quaisquer alterações, tendo em vista uma orientação geral** na sua reunião de 6 de dezembro de 2022.

IV. PRINCIPAIS ELEMENTOS DA PROPOSTA DE COMPROMISSO

1. Carteira europeia de identidade digital

Um dos principais objetivos políticos da proposta da Comissão relativa a uma carteira europeia de identidade digital ("carteira") consiste em proporcionar aos cidadãos e a outros residentes, tal como definidos na legislação nacional, um meio europeu harmonizado de identidade digital baseado no conceito da carteira europeia de identidade digital. Enquanto meio de identificação eletrónica emitido ao abrigo de sistemas nacionais com nível de garantia "elevado", a carteira seria, por direito próprio, um meio de identificação eletrónica baseado na emissão de dados de identificação pessoal e da carteira pelos Estados-Membros.

2. Nível de garantia da carteira europeia de identidade digital

Os níveis de garantia deverão caracterizar o nível de confiança de um meio de identificação eletrónica na determinação da identidade de uma pessoa, garantindo assim que quem declara ter determinada identidade é de facto a pessoa a quem essa identidade foi atribuída. Com base no amplo apoio registado nas reuniões do Grupo e no debate do Coreper de 14 de outubro, a carteira deve ser emitida no âmbito de um sistema de identificação eletrónica com o nível de garantia "elevado". Além disso, foi aditada ao **artigo 6.º-A** uma disposição específica sobre a integração dos utilizadores. Esta alteração destina-se a dar resposta às preocupações dos Estados-Membros em que já foi emitido um número significativo de meios nacionais de identificação eletrónica com o nível de garantia "substancial". A disposição permite que os utilizadores utilizem os seus meios nacionais de identificação eletrónica em conjugação com

procedimentos adicionais de integração remota para tornar possível a prova de identidade com o nível de garantia "elevado" e, em última análise, obter uma carteira. Uma vez que o projeto de Regulamento Identificação Eletrónica assenta em sistemas de certificação da cibersegurança que devem proporcionar um nível de confiança harmonizado na segurança das carteiras europeias de identidade digital, espera-se também que o armazenamento seguro de material criptográfico passe a estar sujeito a certificação da cibersegurança. Por conseguinte, a Presidência propôs um novo **considerando (10-B)** que incide sobre estas condições técnicas prévias para alcançar o nível de garantia "elevado" e permite um processo de acompanhamento no âmbito da implementação das carteiras europeias de identidade digital.

3. Notificação das partes utilizadoras

3.1 O **artigo 6.º-B** relativo à notificação das partes utilizadoras foi reformulado. Regra geral, o processo de notificação através do qual a parte utilizadora comunica a sua intenção de recorrer a carteiras deve ser eficaz em termos de custos, proporcional ao risco e assegurar que a parte utilizadora fornece, pelo menos, as informações necessárias para autenticar a carteira. Por defeito, apenas são necessárias informações mínimas e a notificação deve permitir a utilização de procedimentos automatizados ou simples de autocomunicação.

3.2 Contudo, pode ser necessário um regime específico devido aos requisitos do setor, como os aplicáveis ao tratamento de categorias especiais de dados pessoais. Por conseguinte, foi introduzida uma disposição correspondente que visa abranger os casos em que é necessário um procedimento de registo ou autorização mais rigoroso. Em contrapartida, se o direito nacional ou da União não estabelecer requisitos específicos para aceder às informações fornecidas através da carteira, os Estados-Membros podem isentar essas partes utilizadoras da obrigação de notificar a sua intenção de recorrer às carteiras.

4. Certificação

4.1 O regulamento deve tirar partido, recorrer e impor a utilização dos sistemas de certificação pertinentes e existentes do Regulamento Cibersegurança, ou de partes dos mesmos, para certificar a conformidade das carteiras, ou de partes das mesmas, com os requisitos de cibersegurança aplicáveis. Por conseguinte, o quadro do Regulamento Cibersegurança é plenamente aplicável, incluindo o mecanismo de análise pelos pares entre as autoridades nacionais de certificação da cibersegurança previsto no Regulamento Cibersegurança. A fim de alinhar tanto quanto possível o Regulamento Identificação Eletrónica e o Regulamento Cibersegurança, os Estados-Membros designarão organismos públicos e privados acreditados para certificar a carteira, tal como previsto no Regulamento Cibersegurança.

4.2 Além disso, a Comissão é incentivada a mandar a ENISA para levar a cabo o desenvolvimento e a adoção de um sistema específico do Regulamento Cibersegurança para a certificação da cibersegurança da carteira. Até que esse sistema seja desenvolvido, o EUCC (sistema europeu de certificação da cibersegurança) baseado em critérios comuns publicado ao abrigo do Regulamento Cibersegurança será utilizado como metodologia de base para a certificação de carteiras. Para os requisitos não relacionados com a cibersegurança, nomeadamente os que abrangem outros aspetos funcionais e operacionais da carteira, há que estabelecer uma lista de especificações, procedimentos e normas de referência. Estes requisitos são objeto de certificação.

5. Período de aplicação para o fornecimento da carteira

Com base nas orientações dos Estados-Membros, foi proposto que se conte o período de aplicação de 24 meses a partir da adoção dos atos de execução referidos no **artigo 6.º-A, n.º 11**, e no **artigo 6.º-C, n.º 4**.

6. Taxas

Foi clarificado no **artigo 6.º-A, n.º 6-A** e no considerando correspondente que a emissão, a utilização para autenticação e a revogação de carteiras devem ser gratuitas para as pessoas singulares. Exceto nos casos em que as carteiras são utilizadas para autenticação, os serviços que recorrem à utilização da carteira podem incorrer em custos, por exemplo, a emissão de certificados eletrónicos de atributos à carteira.

7. Acesso a equipamento informático e *software*, incluindo o elemento seguro

A Presidência sugeriu que se previsse uma articulação explícita com o Regulamento (UE) 2022/1925, que assegura o acesso ao equipamento informático e às funcionalidades do *software* como parte dos serviços essenciais de plataforma prestados pelos controladores de acesso. O novo **artigo 12.º-B** clarifica que os fornecedores de carteiras e os emissores de meios de identificação eletrónica notificados que atuem a título comercial ou profissional são utilizadores profissionais de controladores de acesso na aceção da respetiva definição constante do Regulamento Mercados Digitais. Foi aditado um considerando para descrever as implicações da interligação com o Regulamento Mercados Digitais, a saber, que os controladores de acesso devem ser obrigados a assegurar, a título gratuito, a interoperabilidade efetiva e o acesso para efeitos de interoperabilidade com o mesmo sistema operativo, equipamento informático ou funcionalidades de *software* disponíveis ou utilizados na prestação dos seus próprios serviços complementares e de apoio.

8. Possibilidades alternativas de emissão de certificados eletrónicos de atributos por organismos públicos

Foi mantida a emissão de certificados eletrónicos qualificados de atributos por prestadores qualificados, incluindo a obrigação de os Estados-Membros assegurarem que os atributos podem ser verificados através de uma fonte autêntica no setor público. Além disso, foi introduzida a possibilidade de o certificado eletrónico de atributos com os mesmos efeitos jurídicos que o certificado eletrónico qualificado de atributos poder ser emitido diretamente para a carteira pelo organismo do setor público responsável pela fonte autêntica ou por um organismo do setor público designado em nome de um organismo do setor público responsável por uma fonte autêntica, desde que sejam cumpridos os requisitos necessários. A proposta está refletida nos novos **artigos 45.º-A, 45.º-DA** e no **anexo VII**.

9. Correspondência de registos

O **artigo 11.º-A** original passou a designar-se "Correspondência de registos", uma vez que tal reflete melhor o objetivo da disposição. Com base no debate, o conceito de identificador único e persistente foi mantido para as carteiras. A respetiva definição esclarece que o identificador pode consistir numa combinação de vários identificadores nacionais e setoriais, desde que sirva o seu objetivo. É explicitamente referido que a correspondência de registos pode ser facilitada por um certificado eletrónico qualificado de atributos. Além disso, foi incorporada no **artigo 11.º-A** uma disposição de salvaguarda, segundo a qual os Estados-Membros devem assegurar a proteção dos dados pessoais e impedir a definição de perfis dos utilizadores. Por último, os Estados-Membros, na sua qualidade de partes utilizadoras, devem assegurar a correspondência de registos.

VI. CONCLUSÃO

1. À luz do exposto, convida-se o Conselho a:
 - analisar o texto de compromisso, constante do anexo à presente nota;
 - confirmar uma orientação geral sobre a proposta de regulamento relativo à identidade digital europeia na reunião do Conselho TTE (Telecomunicações) de 6 de dezembro de 2022.

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que altera o Regulamento (UE) n.º 910/2014 no respeitante à criação de um Quadro Europeu para a
Identidade Digital

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o
artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu³,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

- (1) A Comunicação da Comissão de 19 de fevereiro de 2020, intitulada "Construir o futuro digital da Europa"⁴, anuncia uma revisão do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho com o objetivo de melhorar a sua eficácia, alargar as suas vantagens ao setor privado e promover a utilização de identidades digitais fíáveis por todos os europeus.

³ JO C de , p. .

⁴ COM/2020/67 final

- (2) Nas suas conclusões de 1 e 2 de outubro de 2020⁵, o Conselho Europeu apelou à Comissão para que apresentasse uma proposta de desenvolvimento de um quadro relativo à identificação eletrónica pública segura em toda a UE, incluindo assinaturas digitais interoperáveis, a fim de dar às pessoas o controlo sobre a sua identidade e os seus dados em linha, bem como de permitir o acesso a serviços digitais públicos, privados e transfronteiriços.
- (3) A Comunicação da Comissão de 9 de março de 2021, intitulada "Orientações para a Digitalização até 2030: a via europeia para a Década Digital"⁶, define o objetivo de um quadro da União que, até 2030, conduza a uma ampla implantação de uma identidade fiável e controlada pelo utilizador, permitindo a cada cidadão controlar as suas próprias interações e presença em linha.
- (4) Uma abordagem mais harmonizada da identificação digital deverá reduzir os riscos e custos da atual fragmentação, causada pela utilização de soluções nacionais divergentes e reforçará o mercado único, permitindo aos cidadãos, outros residentes, conforme definidos pela legislação nacional, e empresas identificarem-se em linha de uma forma conveniente e uniforme em toda a União. A carteira europeia de identidade digital proporcionará às pessoas singulares e coletivas em toda a União um meio de identificação eletrónica harmonizado que lhes permitam autenticar e partilhar dados relacionados com a sua identidade. Todas as pessoas deverão poder aceder de forma segura a serviços públicos e privados apoiando-se num ecossistema melhorado de serviços de confiança e em provas verificadas de identidade e certificados de atributos, tais como um diploma universitário legalmente reconhecido e aceite em toda a União. O Quadro Europeu para a Identidade Digital visa alcançar uma mudança da dependência exclusiva de soluções de identidade digital nacionais para o fornecimento de certificados eletrónicos de atributos válidos a nível europeu. Os fornecedores de certificados eletrónicos de atributos deverão beneficiar de um conjunto claro e uniforme de regras e as administrações públicas deverão poder confiar em documentos eletrónicos num determinado formato.

⁵ <https://www.consilium.europa.eu/pt/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>

⁶ COM/2021/118 final/2

- (4-A) Vários Estados-Membros implementaram e utilizam em grande medida meios de identificação eletrónica que atualmente são aceites pelos prestadores de serviços na União. Além disso, foram realizados investimentos em soluções nacionais e transfronteiriças com base no atual Regulamento eIDAS, incluindo a infraestrutura técnica de interoperabilidade dos nós eIDAS. A fim de garantir a complementaridade e a rápida adoção das carteiras europeias de identidade digital pelos atuais utilizadores dos meios de identificação eletrónica notificados e de minimizar os impactos nos prestadores de serviços existentes, espera-se que as carteiras europeias de identidade digital tirem partido da experiência adquirida com os meios de identificação eletrónica existentes e da infraestrutura eIDAS implantada a nível europeu e nacional.
- (5) Para apoiar a competitividade das empresas europeias, os prestadores de serviços em linha deverão poder contar com soluções de identidade digital reconhecidas em toda a União, independentemente do Estado-Membro em que tenham sido fornecidas, beneficiando assim de uma abordagem europeia harmonizada em matéria de confiança, segurança e interoperabilidade. Tanto os utilizadores como os prestadores de serviços deverão ser capazes de beneficiar do mesmo valor jurídico que o conferido aos certificados eletrónicos de atributos na União.
- (6) O Regulamento (UE) 2016/679⁷ aplica-se ao tratamento dos dados pessoais realizado em aplicação do presente regulamento. Por conseguinte, o presente regulamento deverá estabelecer garantias específicas para impedir que os fornecedores de meios de identificação eletrónica e de certificados eletrónicos de atributos combinem dados pessoais de outros serviços com dados pessoais relativos aos serviços abrangidos pelo âmbito de aplicação do presente regulamento. Os dados pessoais relacionados com o fornecimento de carteiras europeias de identidade digital deverão ser mantidos separados logicamente de quaisquer outros dados detidos pelo emitente. O presente regulamento não impede os emitentes de carteiras europeias de identidade digital de aplicarem medidas técnicas adicionais que contribuam para a proteção dos dados pessoais, como a separação física dos dados pessoais relacionados com o fornecimento de carteiras em relação a quaisquer outros dados detidos pelo emitente.

⁷ 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.

- (7) É necessário estabelecer condições harmonizadas para a criação de um quadro para as carteiras europeias de identidade digital a fornecer pelos Estados-Membros, que deverão habilitar todos os cidadãos da União e outros residentes, conforme definidos pela legislação nacional, a partilharem de forma segura dados relacionados com a sua identidade de uma maneira simples de utilizar e conveniente, sob o controlo exclusivo do utilizador. As tecnologias utilizadas para alcançar esses objetivos deverão ser desenvolvidas visando o mais elevado nível de segurança, privacidade e conveniência para o utilizador, bem como uma ampla usabilidade. Os Estados-Membros deverão assegurar a igualdade de acesso a identificação digital a todos os seus nacionais e residentes.
- (8) A fim de assegurar que as partes utilizadoras podem confiar na utilização de carteiras europeias de identidade digital e proteger o utilizador contra a utilização ilícita de dados sensíveis, as partes utilizadoras deverão ser registadas como parte de um processo de notificação. Os requisitos de notificação aplicáveis às partes utilizadoras deverão, na maioria dos casos, basear-se no fornecimento de uma quantidade limitada de informações necessárias para a autenticação da parte utilizadora para a carteira europeia de identidade digital. Os requisitos deverão também permitir a utilização de procedimentos automatizados ou simples de autocomunicação, incluindo a confiança nos registos existentes e a utilização dos mesmos pelos Estados-Membros. Ao mesmo tempo, para categorias de dados sensíveis, podem existir regimes específicos a nível nacional ou da União, que podem impor requisitos de registo e autorização mais rigorosos às partes utilizadoras, a fim de evitar a utilização ilícita de dados de identificação nesses casos. Noutros casos de utilização, as partes utilizadoras podem ser dispensadas de notificar a sua intenção de recorrer à carteira digital europeia, por exemplo, quando o direito de verificar atributos específicos não exigir ou permitir a autenticação da parte utilizadora por via eletrónica. Normalmente, nestes cenários presenciais, o utilizador é capaz de identificar a parte utilizadora graças ao contexto, por exemplo, quando interage com um funcionário de uma empresa de aluguer de automóveis ou com um farmacêutico. O processo de notificação destina-se a ser conduzido por legislação setorial da União ou nacional, uma vez que tal permite ter em conta vários casos de utilização que podem diferir em termos de requisitos de registo, de modo de funcionamento (em linha/fora de linha) ou em termos do requisito de autenticação de dispositivos capazes de interagir com a carteira europeia de identidade digital. A verificação da utilização da carteira europeia de identidade digital pelas partes utilizadoras não deverá ser de aplicação obrigatória ao nível da carteira europeia de identidade digital.

- (9) Todas as carteiras europeias de identidade digital deverão permitir aos utilizadores identificarem-se eletronicamente e autenticarem-se em linha e fora de linha além-fronteiras para aceder a um vasto leque de serviços públicos e privados. Sem prejuízo das prerrogativas dos Estados-Membros no que diz respeito à identificação dos seus nacionais e residentes, as carteiras podem também servir as necessidades institucionais das administrações públicas, das organizações internacionais e das instituições, órgãos e organismos da União. A utilização fora de linha será importante em muitos setores, nomeadamente o setor da saúde onde os serviços são amiúde prestados através de uma interação presencial e onde a verificação da autenticidade das receitas eletrónicas deverá poder basear-se em códigos QR ou tecnologias similares. Apoando-se no nível de garantia "elevado", as carteiras europeias de identidade digital deverão beneficiar do potencial oferecido por soluções invioláveis, como elementos seguros, para cumprir os requisitos de segurança previstos no presente regulamento. As carteiras europeias de identidade digital deverão também permitir aos utilizadores criar e utilizar assinaturas e selos eletrónicos qualificados que sejam aceites em toda a UE. Num intuito de simplificação e de redução de custos em prol das pessoas e empresas na UE, nomeadamente ao permitir poderes de representação e mandatos eletrónicos, os Estados-Membros deverão emitir carteiras europeias de identidade digital, baseadas em normas comuns para assegurar uma interoperabilidade contínua e um elevado nível de segurança. Apenas as autoridades competentes dos Estados-Membros podem oferecer um elevado nível de confiança na determinação da identidade de uma pessoa e, portanto, assegurar que a pessoa que reivindica ou declara ter uma determinada identidade é efetivamente a pessoa que alega ser. Por conseguinte, é necessário que as carteiras europeias de identidade digital se baseiem na identidade jurídica dos cidadãos, outros residentes ou entidades jurídicas. A confiança nas carteiras europeias de identidade digital será reforçada pelo facto de as partes emitentes serem obrigadas a implementar medidas técnicas e organizacionais adequadas para garantir um nível de segurança proporcional aos riscos criados para os direitos e liberdades das pessoas singulares, em consonância com o Regulamento (UE) 2016/679. A emissão e utilização para autenticação e revogação das carteiras europeias de identidade digital deverá ser gratuita para as pessoas singulares. Os serviços que recorrem à utilização da carteira podem incorrer em custos, por exemplo, a emissão de certificados eletrónicos de atributos à carteira.

(9-A) É vantajoso facilitar a adoção e a utilização das carteiras europeias de identidade digital, integrando-as sem descontinuidades no ecossistema de serviços digitais públicos e privados já implementados a nível nacional, local ou regional. Para alcançar este objetivo, os Estados-Membros podem prever medidas jurídicas e organizacionais para aumentar a flexibilidade para os emitentes de carteiras europeias de identidade digital e para permitir funcionalidades adicionais das carteiras europeias de identidade digital para além do estabelecido pelo presente regulamento, nomeadamente através de uma maior interoperabilidade com os meios nacionais de identificação eletrónica existentes. Tal não deverá, de modo algum, prejudicar a prestação de funções essenciais das carteiras europeias de identidade digital, tal como definidas no presente regulamento, nem a promoção das soluções nacionais existentes em relação às carteiras europeias de identidade digital. Uma vez que vão além do âmbito do presente regulamento, essas funcionalidades adicionais não beneficiam das disposições relativas à dependência transfronteiras das carteiras europeias de identidade digital estabelecidas no presente regulamento.

(10) A fim de alcançar um elevado nível de proteção de dados, segurança e confiança, o presente regulamento deverá estabelecer um quadro harmonizado das especificações e dos requisitos comuns aplicáveis às carteiras europeias de identidade digital. A conformidade das carteiras europeias de identidade digital com esses requisitos deverá ser certificada por organismos de avaliação de conformidade acreditados designados pelos Estados-Membros. A certificação deverá basear-se, em especial, nos sistemas europeus de certificação da cibersegurança pertinentes, ou em partes dos mesmos, estabelecidos nos termos do Regulamento (UE) 2019/881⁸, na medida em que abranjam os requisitos de cibersegurança aplicáveis às carteiras europeias de identidade digital. A utilização de sistemas europeus de certificação da cibersegurança deverá proporcionar um nível de confiança harmonizado na segurança das carteiras europeias de identidade digital, independentemente do local da União onde sejam emitidas. A certificação da cibersegurança das carteiras europeias de identidade digital deverá basear-se no papel das autoridades nacionais de certificação da cibersegurança na supervisão e no controlo da conformidade dos certificados emitidos pelos organismos de avaliação da conformidade sob a sua jurisdição com os sistemas europeus de cibersegurança pertinentes. Do mesmo modo, a certificação deverá tirar partido, se for caso disso, das normas e especificações técnicas indicadas no Regulamento (UE) 2019/881. Essas especificações podem ser utilizadas como documentos do estado da arte, conforme especificado no âmbito dos sistemas de certificação da cibersegurança pertinentes nos termos do Regulamento (UE) 2019/881. Se nenhum sistema europeu de certificação da cibersegurança criado nos termos do Regulamento (UE) 2019/881 abranger a certificação de serviços ou processos pertinentes que contribuam para a segurança da carteira, deverão ser criados sistemas adequados em conformidade com o título III do Regulamento (UE) 2019/881. Deverá ser criado um sistema comum e harmonizado de certificação das carteiras europeias de identidade digital para avaliar a sua conformidade com as especificações e os requisitos comuns previstos no presente regulamento, com exceção dos relacionados com a cibersegurança e a proteção de dados, nomeadamente os que abrangem os aspetos funcionais e operacionais. No que diz respeito a esta certificação, a fim de assegurar um elevado nível de confiança e transparência, deverão ser estabelecidos mecanismos e procedimentos destinados a promover a aprendizagem entre pares e a cooperação entre os Estados-Membros em matéria de controlo e revisão dos organismos de certificação e dos certificados e relatórios de certificação que emitem. Esse mecanismo de aprendizagem entre pares não deverá prejudicar o disposto nos Regulamentos (UE) 2016/679 e (UE) 2019/881. A certificação da carteira ao abrigo do Regulamento (UE) 2016/679 é um instrumento voluntário, entre outros, que pode ser utilizado para demonstrar a conformidade com os requisitos estabelecidos no Regulamento (UE) 2016/679, na medida em que se aplicam às carteiras europeias de identidade digital e ao seu fornecimento aos cidadãos europeus.

⁸ 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.

- (10-A) A integração de cidadãos e residentes na carteira europeia de identidade digital deverá ser facilitada com base em meios de identificação eletrónica emitidos com um nível de garantia "elevado". Os meios de identificação eletrónica emitidos ao nível de garantia "substancial" só deverão ser utilizados nos casos em que as especificações técnicas e operacionais harmonizadas que utilizam meios de identificação eletrónica emitidos ao nível de garantia "substancial", em combinação com outros meios suplementares de verificação da identidade, permitam o cumprimento dos requisitos estabelecidos no presente regulamento no que diz respeito ao nível de garantia "elevado". Esses meios ou medidas suplementares deverão ser fiáveis e fáceis de utilizar pelos utilizadores e podem basear-se na possibilidade de utilizar procedimentos de integração à distância, certificados qualificados apoiados por assinaturas qualificadas, certificados eletrónicos qualificados de atributos ou uma combinação dos mesmos. A fim de assegurar a adoção suficiente das carteiras europeias de identidade digital, deverão ser estabelecidas, em atos de execução, especificações técnicas e operacionais harmonizadas para a integração dos utilizadores através de meios de identificação eletrónica, incluindo os emitidos com um nível de garantia "substancial".
- (10-B) O objetivo do presente regulamento é proporcionar ao utilizador uma carteira europeia de identidade digital totalmente móvel, segura e convival. Como medida transitória até à disponibilidade de soluções certificadas à prova de falsificação, tais como elementos seguros nos dispositivos dos utilizadores, as carteiras europeias de identidade digital podem basear-se em elementos seguros externos certificados para a proteção do material criptográfico e de outros dados sensíveis ou em soluções nacionais notificadas com um nível de garantia "elevado", a fim de demonstrar a conformidade com os requisitos pertinentes do regulamento no que diz respeito ao nível de garantia da carteira. A utilização da medida transitória acima referida deverá limitar-se a casos que exijam um nível de garantia "elevado", como a integração do utilizador na carteira e a autenticação para serviços que exijam um nível de garantia "elevado". No caso da autenticação para serviços que exijam um nível de garantia "substancial", as carteiras europeias de identidade digital não deverão exigir a utilização da medida transitória acima referida. O presente regulamento não deverá prejudicar as condições nacionais para a emissão e utilização de elementos de segurança externa certificados, caso esta medida transitória dependa desses elementos.

- (11) As carteiras europeias de identidade digital deverão garantir o mais elevado nível de proteção e segurança dos dados pessoais utilizados para autenticação, independentemente de esses dados serem ou não armazenados localmente ou em soluções em nuvem, tendo em conta os diferentes níveis de risco. O tratamento de dados biométricos como fator de autenticação na autenticação forte do utilizador é um dos métodos de identificação que oferece um elevado nível de confiança, sobretudo quando utilizado em combinação com outros elementos de autenticação. Uma vez que os dados biométricos representam uma característica única de uma pessoa, o tratamento de dados biométricos só é permitido ao abrigo das exceções previstas no artigo 9.º, n.º 2, do Regulamento (UE) 2016/679 e exige salvaguardas adequadas, proporcionais ao risco que esse tratamento pode implicar para os direitos e liberdades das pessoas singulares.
- (11-A) O funcionamento das carteiras europeias de identidade digital deverá ser transparente e permitir o tratamento verificável de dados pessoais. Para o efeito, os Estados-Membros são incentivados a divulgar o código-fonte dos componentes de *software* das carteiras europeias de identidade digital relacionados com o tratamento de dados pessoais e de dados de pessoas coletivas. A divulgação desse código-fonte permite à sociedade, incluindo os utilizadores e os criadores, compreender o seu funcionamento. Tal pode também aumentar a confiança dos utilizadores no ecossistema de carteiras e contribuir para a segurança das carteiras, permitindo a qualquer pessoa comunicar vulnerabilidades e erros no código, o que incentiva os fornecedores a proporcionar e manter um produto altamente seguro. Ademais, e se for caso disso, os Estados-Membros são também incentivados a disponibilizar o código-fonte ao abrigo de uma licença de fonte aberta. Uma licença de fonte aberta permite à sociedade, incluindo utilizadores e criadores, alterar e reutilizar o código-fonte.
- (12) A fim de garantir que o Quadro Europeu para a Identidade Digital está aberto à inovação, ao desenvolvimento tecnológico e preparado para o futuro, os Estados-Membros deverão ser encorajados a criar conjuntamente ambientes de testagem para testar soluções inovadoras num ambiente controlado e seguro, em especial, para melhorar a funcionalidade, a proteção dos dados pessoais, a segurança e a interoperabilidade das soluções e contribuir para futuras atualizações de referências técnicas e requisitos legais. Este ambiente deverá promover a inclusão de pequenas e médias empresas europeias, empresas em fase de arranque e inovadores e investigadores individuais.

- (13) O Regulamento (UE) 2019/1157⁹ reforça a segurança dos bilhetes de identidade com dispositivos de segurança melhorados até agosto de 2021. Os Estados-Membros deverão ponderar a viabilidade de os notificar ao abrigo dos sistemas de identificação eletrónica para alargar a disponibilidade transfronteiriça de meios de identificação eletrónica.
- (14) O processo de notificação dos sistemas de identificação eletrónica deverá ser simplificado e acelerado para promover o acesso a soluções de autenticação e identificação convenientes, de confiança, seguras e inovadoras e, quando pertinente, para encorajar os fornecedores de identidade privados a oferecer sistemas de identificação eletrónica às autoridades dos Estados-Membros para notificação enquanto sistemas nacionais de identificação eletrónica ao abrigo do Regulamento (UE) n.º 910/2014.
- (15) A simplificação dos procedimentos atuais de notificação e avaliação pelos pares evitará abordagens heterogéneas no que respeita à avaliação dos vários sistemas de identificação eletrónica notificados e facilitará o reforço da confiança entre Estados-Membros. Mecanismos novos e simplificados deverão promover a cooperação entre Estados-Membros em matéria de segurança e interoperabilidade dos seus sistemas de identificação eletrónica notificados.
- (16) Os Estados-Membros deverão beneficiar de ferramentas novas e flexíveis para garantir a conformidade com os requisitos do presente regulamento e dos atos de execução pertinentes. O presente regulamento deverá permitir aos Estados-Membros utilizar relatórios e avaliações, realizados por organismos de avaliação da conformidade acreditados, tal como previsto nos sistemas de certificação que deverão ser criados a nível da União nos termos do Regulamento (UE) 2019/881, para fundamentar as suas alegações sobre o alinhamento dos sistemas ou parte dos mesmos com os requisitos desse regulamento em matéria de interoperabilidade e de segurança dos sistemas de identificação eletrónica notificados.

⁹ Regulamento (UE) 2019/1157 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, que visa reforçar a segurança dos bilhetes de identidade dos cidadãos da União e dos títulos de residência emitidos aos cidadãos da União e seus familiares que exercem o direito à livre circulação, JO L 188 de 12.7.2019, p. 67.

(17-A) A utilização de identificadores únicos e persistentes emitidos pelos Estados-Membros ou gerados pela carteira europeia de identidade digital, juntamente com a utilização de dados de identificação pessoal, é essencial para assegurar que é possível verificar a identidade do utilizador, em especial no setor público e quando exigido pelo direito nacional ou da União. O presente regulamento deverá assegurar que a carteira europeia de identidade digital pode proporcionar um mecanismo que permita a correspondência de registos, inclusive através da utilização de certificados eletrónicos qualificados de atributos, e permitir a inclusão de identificadores únicos e persistentes no conjunto de dados de identificação pessoal. Um identificador único e persistente pode consistir em dados de identificação únicos ou múltiplos que podem ser setoriais, desde que sirvam para identificar o utilizador de forma única em toda a União. A carteira europeia de identidade digital deverá também prever um mecanismo que permita a utilização de identificadores específicos da parte utilizadora nos casos em que a utilização de um identificador único e persistente seja exigida pela legislação nacional ou da União. Em todos os casos, o mecanismo previsto para facilitar a correspondência de registos e a utilização de identificadores únicos e persistentes deverá assegurar que o utilizador está protegido contra a utilização abusiva de dados pessoais em conformidade com o presente regulamento e o direito da União aplicável, nomeadamente o Regulamento (UE) 2016/679, nomeadamente contra o risco de definição de perfis e de rastreio relacionado com a utilização da carteira europeia de identidade digital.

(17-AA) É essencial ter em conta as necessidades dos utilizadores, aumentando assim a procura de carteiras europeias de identidade digital. Deverão existir casos de utilização significativos e serviços em linha que recorrem às carteiras europeias de identidade digital. Por razões de conveniência dos utilizadores e a fim de assegurar a disponibilidade transfronteiras desses serviços, é importante tomar medidas para facilitar uma abordagem semelhante à conceção, desenvolvimento e implementação de serviços em linha em todos os Estados-Membros. As orientações não vinculativas sobre a forma de conceber, desenvolver e implementar serviços em linha que recorrem às carteiras europeias de identidade digital têm potencial para se tornarem um instrumento útil para alcançar este objetivo. Estas orientações deverão ser elaboradas tendo em devida conta o quadro de interoperabilidade da União. Os Estados-Membros deverão desempenhar um papel de liderança na sua adoção.

- (18) Em consonância com a Diretiva (UE) 2019/882¹⁰, as pessoas com deficiência deverão poder utilizar as carteiras europeias de identidade digital, os serviços de confiança e os produtos de utilizador final utilizados na prestação desses serviços em condições iguais às dos outros utilizadores.
- (19) O presente regulamento não deverá abranger os aspetos relacionados com a celebração e a validade de contratos ou outras obrigações legais quando estes estabeleçam requisitos de carácter formal previstos na legislação nacional ou da União. Além disso, não deverá afetar os requisitos nacionais de carácter formal aplicáveis aos registos públicos, em particular, registos comerciais e prediais.
- (20) A prestação e utilização de serviços de confiança estão a tornar-se cada vez mais importantes para o comércio e a cooperação internacionais. Os parceiros internacionais da UE estão a criar quadros de confiança inspirados no Regulamento (UE) n.º 910/2014. Por conseguinte, a fim de facilitar o reconhecimento desses dispositivos e dos respetivos fornecedores, a legislação de execução pode estabelecer as condições em que os quadros de confiança de países terceiros poderão ser considerados equivalentes ao quadro de confiança para os serviços de confiança qualificados e os prestadores qualificados de serviços de confiança previsto no presente regulamento, como complemento à possibilidade de reconhecimento mútuo de serviços e prestadores de serviços de confiança estabelecidos na União e em países terceiros nos termos do artigo 218.º do Tratado. Ao estabelecer as condições em que os quadros de confiança de países terceiros podem ser considerados equivalentes ao regime de confiança para os serviços de confiança qualificados e os seus prestadores no presente regulamento, deverá também ser assegurada a conformidade com as disposições pertinentes da Diretiva XXXX/XXXX (Diretiva SRI 2) e do Regulamento (UE) 2016/679, bem como a utilização de listas de confiança como elementos essenciais para criar confiança.

¹⁰ 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.

(21) O presente regulamento deverá basear-se nos atos da União que asseguram a disputabilidade e a equidade dos mercados no setor digital. Em especial, baseia-se no Regulamento (UE) 2022/1925, que introduz regras aplicáveis a prestadores de serviços essenciais de plataforma designados os controladores de acesso e, entre outros aspetos, proíbe os controladores de acesso de exigir aos utilizadores profissionais que utilizem, proponham ou interoperem com um serviço de identificação do controlador de acesso no contexto dos serviços propostos pelos utilizadores profissionais que utilizam os serviços essenciais de plataforma desse controlador de acesso. O artigo 6.º, n.º 7, do Regulamento (UE) 2022/1925 exige que os controlares de acesso permitam aos utilizadores profissionais e aos prestadores de serviços complementares o acesso e a interoperabilidade com o mesmo sistema operativo, equipamento informático ou funcionalidades de *software* disponíveis ou utilizados na prestação de qualquer serviço complementar por parte do controlador de acesso. De acordo com o artigo 2.º, n.º 19, do Regulamento dos Mercados Digitais, os serviços de identificação constituem um tipo de serviços complementares. Os utilizadores profissionais e os prestadores de serviços complementares deverão, portanto, poder aceder a esse equipamento informático e a essas funcionalidades de *software*, nomeadamente elementos seguros em telefones inteligentes, e interoperar com as mesmas através das carteiras europeias de identidade digital ou dos meios de identificação eletrónica notificados pelos Estados-Membros.

(22) A fim de simplificar as obrigações em matéria de cibersegurança impostas aos prestadores de serviços de confiança, bem como de permitir a esses prestadores e às respetivas autoridades competentes beneficiarem do quadro legal instituído pela Diretiva XXXX/XXXX [Diretiva SRI 2], os serviços de confiança são obrigados a adotar medidas técnicas e organizacionais adequadas nos termos da Diretiva XXXX/XXXX [Diretiva SRI 2], nomeadamente medidas que respondam a falhas do sistema, erro humano, ações maliciosas ou fenómenos naturais para gerir os riscos colocados à segurança da rede e aos sistemas de informação que esses prestadores utilizam na prestação dos seus serviços, bem como para notificar incidentes significativos e ciberameaças de acordo com a Diretiva XXXX/XXXX [Diretiva SRI 2]. No que diz respeito à comunicação de incidentes, os prestadores de serviços de confiança deverão notificar todos os incidentes com um impacto significativo na prestação dos seus serviços, nomeadamente os causados por roubo ou perda de dispositivos, danos no cabo de rede ou ocorridos no contexto da identificação de pessoas. Os requisitos de gestão dos riscos de cibersegurança e as obrigações de notificação previstos na Diretiva XXXX/XXXX [Diretiva SRI 2] deverão ser considerados complementares aos requisitos impostos aos prestadores de serviços de confiança no âmbito do presente regulamento. Sempre que adequado, as práticas ou orientações nacionais estabelecidas em relação à implementação de requisitos de segurança e prestação de informações e à supervisão da conformidade com esses requisitos nos termos do Regulamento (UE) n.º 910/2014 deverão continuar a ser aplicadas pelas autoridades competentes designadas ao abrigo da Diretiva XXXX/XXXX [Diretiva SRI 2]. Os requisitos previstos no presente regulamento não afetam a obrigação de notificar violações de dados pessoais no âmbito do Regulamento (UE) 2016/679.

- (23) Deverá prestar-se a devida atenção à garantia de uma cooperação eficaz entre as autoridades SRI e eIDAS. Nos casos em que a entidade supervisora prevista no presente regulamento seja diferente das autoridades competentes designadas ao abrigo da Diretiva XXXX/XXXX [Diretiva SRI 2], essas autoridades deverão cooperar estreitamente e de forma oportuna procedendo ao intercâmbio de informações pertinentes para assegurar a supervisão eficaz e a conformidade dos prestadores de serviços de confiança com os requisitos estabelecidos no presente regulamento e na Diretiva XXXX/XXXX [Diretiva SRI 2]. Em especial, as entidades supervisoras nos termos do presente regulamento deverão estar habilitadas a pedir à autoridade competente nos termos da Diretiva XXXX/XXXX [Diretiva SRI 2] que preste as informações pertinentes necessárias para conceder o estatuto de qualificado e para levar a cabo as ações de supervisão destinadas a verificar se os prestadores de serviços de confiança cumprem os requisitos pertinentes previstos na SRI 2 ou a exigir-lhes que corrijam as situações de incumprimento.
- (24) É essencial prever um quadro legal para facilitar o reconhecimento transfronteiriço entre os sistemas jurídicos nacionais vigentes no que diz respeito aos serviços de envio registado eletrónico. Esse quadro também pode abrir novas oportunidades aos prestadores de serviços de confiança da União para oferecerem novos serviços de envio registado eletrónico pan-europeu. A fim de assegurar que os dados que utilizam um serviço de envio registado eletrónico qualificado são entregues ao destinatário correto, os serviços qualificados de envio registado eletrónico deverão assegurar com total certeza a identificação do destinatário, ao passo que para a identificação do remetente é suficiente um elevado nível de confiança. Os Estados-Membros deverão incentivar os prestadores de serviços qualificados de envio registado eletrónico a que os seus serviços sejam interoperáveis com os serviços de envio registado eletrónico qualificados prestados por outros prestadores qualificados de serviços de confiança, a fim de transferir facilmente os dados registados eletrónicos entre dois ou mais prestadores de serviços de confiança qualificados e de promover práticas leais no mercado interno.
- (25) Na maioria dos casos, os cidadãos e outros residentes não podem trocar digitalmente, além-fronteiras, informações relacionadas com a sua identidade, tais como endereços, idade e habilitações profissionais, cartas de condução e outras licenças e dados de pagamento, de forma segura e com um elevado nível de proteção dos dados.

- (26) Deverá ser possível emitir e tratar atributos digitais fiáveis e contribuir para reduzir os encargos administrativos, permitindo que os cidadãos e outros residentes os utilizem nas suas transações privadas e públicas. Os cidadãos e outros residentes deverão poder, por exemplo, comprovar a titularidade de uma carta de condução válida emitida por uma autoridade de um Estado-Membro, que as autoridades competentes de outros Estados-Membros possam verificar e corroborar, e utilizar as suas credenciais de segurança social ou os futuros documentos de viagem digitais num contexto transfronteiriço.
- (27) Qualquer entidade que recolha, crie e emita atributos certificados como diplomas, licenças ou certidões de nascimento deverá poder tornar-se um fornecedor de certificados eletrónicos de atributos. As partes utilizadoras deverão utilizar os certificados eletrónicos de atributos como sendo equivalentes aos certificados em suporte de papel. Por conseguinte, não podem ser negados efeitos legais a um certificado eletrónico de atributos pelo facto de se apresentar em formato eletrónico ou de não cumprir os requisitos do certificado eletrónico qualificado de atributos. Para esse efeito, deverão ser estabelecidos requisitos gerais que garantam que um certificado eletrónico qualificado de atributos tem um efeito legal equivalente ao dos certificados emitidos legalmente em suporte de papel. Contudo, esses requisitos deverão aplicar-se sem prejuízo da legislação da União ou nacional que defina requisitos setoriais específicos suplementares no tocante ao formato com efeitos legais subjacentes e, em especial, ao reconhecimento transfronteiriço de certificados eletrónicos qualificados de atributos, se for caso disso.

(28) A ampla disponibilidade e usabilidade das carteiras europeias de identidade digital implica a sua aceitação pelos prestadores de serviços privados. As partes utilizadoras privadas que prestem serviços 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 deverão aceitar a utilização das carteiras europeias de identidade digital para a prestação de serviços sempre que a legislação nacional ou da União ou uma obrigação contratual exijam a autenticação forte do utilizador para efeitos de identificação em linha. A fim de facilitar a utilização e a aceitação da carteira europeia de identidade digital, deverão ser tidas em conta as normas e especificações do setor amplamente aceites. Sempre que plataformas em linha de muito grande dimensão, conforme definidas no artigo 25.º, n.º 1, do Regulamento [referência Regulamento Serviços Digitais], exijam que os utilizadores se autentiquem para aceder a serviços em linha, deverão ser obrigadas a aceitar a utilização de carteiras europeias de identidade digital mediante pedido voluntário do utilizador. Os utilizadores não deverão ter a obrigação de utilizar a carteira para aceder a serviços privados, mas se o pretenderem, as plataformas em linha de muito grande dimensão deverão aceitar a carteira europeia de identidade digital para esta finalidade, respeitando simultaneamente o princípio da minimização dos dados. Atendendo à importância das plataformas em linha de muito grande dimensão, devido ao seu alcance, expresso, nomeadamente, em termos de número de destinatários do serviço e de transações económicas, tal é necessário para aumentar a proteção dos utilizadores contra fraudes e garantir um elevado nível de proteção dos dados. Deverão ser elaborados códigos de conduta de autorregulação a nível da União ("códigos de conduta") para contribuir para a ampla disponibilidade e usabilidade de meios de identificação eletrónica, nomeadamente carteiras europeias de identidade digital, no âmbito do presente regulamento. Os códigos de conduta deverão facilitar a ampla aceitação dos meios de identificação eletrónica, incluindo das carteiras europeias de identidade digital, pelos prestadores de serviços que não se qualificam como plataformas de muito grande dimensão e que dependem de serviços de identificação eletrónica de terceiros para a autenticação dos utilizadores. Esses códigos deverão ser elaborados no prazo de 12 meses a contar da data de adoção do presente regulamento. A Comissão deverá avaliar a eficácia dessas disposições no respeitante à disponibilidade e usabilidade das carteiras europeias de identidade digital para o utilizador decorridos 24 meses da sua implantação.

- (29) A divulgação seletiva é um conceito que habilita o proprietário dos dados a divulgar apenas determinadas partes de um conjunto de dados mais vasto, para que a entidade recetora obtenha apenas as informações necessárias, por exemplo, para que um utilizador divulgue a uma parte utilizadora apenas os dados necessários para a prestação de um serviço solicitado pelo utilizador. A carteira europeia de identidade digital deverá permitir tecnicamente a divulgação seletiva de atributos às partes utilizadoras. Esses atributos divulgados seletivamente, inclusive caso sejam originalmente partes de vários certificados eletrónicos distintos, podem ser subsequentemente combinados e apresentados às partes utilizadoras. Esta funcionalidade deverá tornar-se uma funcionalidade da conceção de base, permitindo assim reforçar a conveniência e a proteção de dados pessoais, incluindo a minimização de dados.
- (30) Os atributos fornecidos pelos prestadores qualificados de serviços de confiança no âmbito do certificado qualificado de atributos deverão ser verificados por confronto com as fontes autênticas diretamente pelo prestador qualificado do serviço de confiança ou através de intermediários designados reconhecidos a nível nacional em conformidade com a legislação nacional ou da União para efeitos de intercâmbio seguro de atributos certificados entre prestadores de serviços de identidade ou de certificados de atributos e partes utilizadoras. Os Estados-Membros deverão estabelecer mecanismos adequados a nível nacional para assegurar que os prestadores qualificados de serviços de confiança que emitem certificados eletrónicos qualificados de atributos possam, com base no consentimento da pessoa a quem o certificado é emitido, verificar a autenticidade dos atributos com base em fontes autênticas. Os mecanismos adequados podem incluir a utilização de intermediários específicos ou soluções técnicas em conformidade com a legislação nacional que permitam o acesso a fontes autênticas. Assegurar a disponibilidade de um mecanismo que permita a verificação de atributos por confronto com fontes autênticas deverá facilitar o cumprimento pelos prestadores qualificados de certificados eletrónicos qualificados de atributos das obrigações que lhes incumbem por força do presente regulamento. O anexo VI contém uma lista de categorias de atributos relativamente às quais os Estados-Membros deverão assegurar que são tomadas medidas para permitir que os fornecedores qualificados de certificados eletrónicos de atributos verifiquem, por via eletrónica, a pedido do utilizador, a sua autenticidade face à fonte autêntica pertinente. Os atributos específicos abrangidos por estas categorias deverão ser acordados com os Estados-Membros.

- (31) A identificação eletrónica segura e o fornecimento de certificados de atributos deverão oferecer flexibilidade e soluções adicionais ao setor dos serviços financeiros, a fim de permitir a identificação de clientes e o intercâmbio de atributos específicos necessários para cumprir, por exemplo, os requisitos de vigilância da clientela nos termos do Regulamento Antibrandeamento de Capitais [referência a aditar após a adoção da proposta], os requisitos de adequação decorrentes da legislação em matéria de proteção dos investidores, ou para apoiar o cumprimento dos requisitos de autenticação forte dos clientes para a identificação em linha para efeitos de início de sessão ou início de transações no domínio dos serviços de pagamento.
- (31-A) A fim de assegurar a coerência das práticas de certificação em toda a UE, a Comissão deverá emitir orientações sobre a certificação e a recertificação dos dispositivos qualificados de criação de assinaturas eletrónicas e dos dispositivos de criação de selos eletrónicos qualificados, incluindo a sua validade e limitações temporais. O presente regulamento não impede os Estados-Membros de autorizarem os organismos públicos ou privados que tenham certificado dispositivos qualificados de criação de assinaturas eletrónicas a prorrogar temporariamente a validade da certificação quando a recertificação do mesmo dispositivo não puder ser efetuada dentro do prazo legalmente definido por um motivo que não seja uma violação ou incidente de segurança, e sem prejuízo da prática de certificação aplicável.

(32) Os serviços de autenticação de sítios Web dão aos utilizadores um elevado nível de garantia de que existe uma entidade genuína e legítima responsável pelo sítio Web, independentemente da plataforma utilizada para a apresentar. Estes serviços contribuem para a criação de segurança e confiança na realização de negócios em linha e na redução dos casos de fraude em linha. A utilização de serviços de autenticação de sítios Web pelos sítios Web deverá ser voluntária. Contudo, para que a autenticação de sítios Web venha a constituir um meio de reforçar a confiança, proporcionar uma melhor experiência ao utilizador e incentivar o crescimento no mercado interno, o presente regulamento deverá estabelecer obrigações mínimas em matéria de segurança e responsabilidade a cumprir pelos prestadores de serviços de autenticação de sítios Web e pelos serviços que prestam. Para o efeito, os fornecedores de navegadores Web deverão assegurar apoio e interoperabilidade com certificados qualificados de autenticação de sítios Web de acordo com o Regulamento (UE) n.º 910/2014. Deverão reconhecer certificados qualificados de autenticação de sítios Web e permitir a apresentação dos dados de identificação certificados ao utilizador final no ambiente do navegador Web com base nas especificações estabelecidas em conformidade com o presente regulamento. O reconhecimento de um certificado qualificado de autenticação de sítios Web como um certificado qualificado emitido por um prestador qualificado de serviços de confiança deverá assegurar que os dados de identificação incluídos no certificado possam ser autenticados e verificados em conformidade com o presente regulamento. Tal não deverá afetar a possibilidade de os fornecedores de navegadores Web darem resposta às principais situações de não conformidade relacionadas com a violação da segurança e a perda de integridade de certificados individuais, contribuindo assim para a segurança em linha dos utilizadores finais. Para proteger melhor os cidadãos e promover ainda mais a sua utilização, as autoridades públicas dos Estados-Membros deverão equacionar incorporar certificados qualificados de autenticação de sítios Web nos respetivos sítios Web.

(33) Muitos Estados-Membros introduziram requisitos nacionais para os serviços que asseguram um arquivo digital seguro e fiável, a fim de permitir a conservação a longo prazo de dados eletrónicos e serviços de confiança associados. A fim de garantir a segurança jurídica, a confiança e a harmonização entre os Estados-Membros, deverá ser estabelecido um quadro jurídico para os serviços de arquivo eletrónico qualificados, inspirado no quadro dos outros serviços de confiança estabelecido no presente regulamento. Este quadro deverá proporcionar aos prestadores de serviços de confiança e aos utilizadores um conjunto de instrumentos eficiente que inclua requisitos funcionais para o serviço de arquivo eletrónico, bem como efeitos jurídicos claros quando é utilizado um serviço de arquivo eletrónico qualificado. Estas disposições deverão aplicar-se aos documentos em suporte eletrónico, bem como aos documentos em papel que tenham sido digitalizados. Se for necessário, estas disposições deverão permitir que os dados eletrónicos conservados sejam transferidos em diferentes suportes ou formatos, a fim de alargar a sua durabilidade e legibilidade para além do período de validade tecnológica, minimizando ao mesmo tempo, tanto quanto possível, a perda e a alteração. Se os dados eletrónicos apresentados ao serviço de arquivo digital contiverem uma ou mais assinaturas eletrónicas qualificadas ou selos eletrónicos qualificados, o serviço deverá utilizar procedimentos e tecnologias capazes de alargar a sua fiabilidade durante o período de conservação desses dados, eventualmente com base na utilização de outros serviços de confiança eletrónicos qualificados estabelecidos pelo presente regulamento. Para a criação de provas de conservação em caso de utilização de assinaturas eletrónicas, selos eletrónicos ou selos temporais eletrónicos, deverão ser utilizados serviços de confiança eletrónicos qualificados. Na medida em que os serviços de arquivo eletrónico não estejam harmonizados pelo presente regulamento, os Estados-Membros podem manter ou introduzir disposições nacionais, em conformidade com o direito da União, relativas a esses serviços, tais como disposições específicas que permitam algumas derrogações para serviços integrados numa organização e estritamente utilizados para "arquivos internos" dessa organização. O presente regulamento não deverá distinguir entre documentos em suporte eletrónico e documentos físicos que tenham sido digitalizados.

- (33-A) Os arquivos e as instituições da memória nacionais, na sua qualidade de organizações dedicadas à preservação do património documental de interesse público, são normalmente mandatados para realizar as suas atividades nos termos do direito nacional e não prestam necessariamente serviços de confiança na aceção do presente regulamento. Na medida em que estas instituições não prestem tais serviços, o presente regulamento não prejudica o seu funcionamento.
- (34) Os livros-razão eletrónicos são uma sequência de registos eletrónicos de dados que assegura a sua integridade e a exatidão da sua ordem sequencial. O objetivo dos livros-razão eletrónicos é estabelecer uma sequência cronológica de registos de dados para evitar que os ativos digitais sejam copiados e vendidos a vários destinatários. Os livros-razão eletrónicos podem, por exemplo, ser utilizados para registos digitais de propriedade no comércio mundial, financiamento da cadeia de abastecimento, digitalização dos direitos de propriedade intelectual ou de produtos de base como a eletricidade. Em conjugação com outras tecnologias, podem contribuir para soluções para serviços públicos mais eficientes e transformadores, tais como a votação eletrónica, a cooperação transfronteiras das autoridades aduaneiras, a cooperação transfronteiras das instituições académicas ou o registo da propriedade de bens imóveis em registos prediais descentralizados. Os livros-razão eletrónicos qualificados criam uma presunção legal para a ordem cronológica única e precisa e para a integridade dos registos de dados no livro-razão. Os atributos específicos dos livros-razão eletrónicos, ou seja, a ordem cronológica sequencial de registos de dados, distinguem os livros-razão eletrónicos de outros serviços de confiança, como os selos temporais eletrónicos e os serviços de envio registado eletrónico. Nomeadamente, nem o carimbo temporal dos documentos digitais nem a sua transferência através de serviços de envio registado eletrónico poderiam, sem outras medidas técnicas ou organizativas, impedir suficientemente o mesmo ativo digital de ser copiado e vendido mais do que uma vez a diferentes partes. O processo de criação e atualização de um livro-razão eletrónico depende do tipo de livro-razão utilizado (centralizado ou distribuído).

(35) Para evitar a fragmentação do mercado interno, há que criar um quadro legal pan-europeu que permita o reconhecimento transfronteiriço de serviços de confiança para o registo de dados em livros-razão eletrónicos qualificados. Os prestadores de serviços de confiança para livros-razão eletrónicos deverão ser mandatados para verificar o registo sequencial dos dados no livro-razão. O presente regulamento não prejudica quaisquer obrigações legais que os utilizadores de livros-razão eletrónicos possam ter de cumprir ao abrigo do direito da União e do direito nacional. Por exemplo, os casos de utilização que envolvam o tratamento de dados pessoais deverão cumprir o disposto no Regulamento (UE) 2016/679. Os casos de utilização que envolvam criptoativos deverão ser compatíveis com todas as regras financeiras aplicáveis, por exemplo, a Diretiva Mercados de Instrumentos Financeiros¹¹, a Diretiva Serviços de Pagamento¹², a Diretiva Moeda Eletrónica¹³, bem como com a eventual futura legislação relativa aplicável aos mercados de criptoativos e com as regras respeitantes à luta contra o branqueamento de capitais que poderiam ser incluídas no Regulamento Transferência de Fundos¹⁴, e poderiam exigir que os prestadores de serviços de criptoativos verifiquem a identidade dos utilizadores de livros-razão eletrónicos para cumprir as normas internacionais em matéria de luta contra o branqueamento de capitais.

¹¹ Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE, JO L 173 de 12.6.2014, p. 349-496.

¹² Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE, JO L 337 de 23.12.2015, p. 35-127.

¹³ Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, que altera as Diretivas 2005/60/CE e 2006/48/CE e revoga a Diretiva 2000/46/CE (JO L 267 de 10.10.2009, p. 7-17).

¹⁴ Ver a [proposta da Comissão de 20.7.2021 de reformulação](#) do Regulamento (UE) 2015/847 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativo às informações que acompanham as transferências, COM/2021/422 final.

(36) A fim de evitar a fragmentação e os entraves decorrentes da existência de normas divergentes e de restrições técnicas, e com vista a assegurar um processo coordenado para evitar comprometer a execução do futuro Quadro Europeu para a Identidade Digital, afigura-se necessário um processo de cooperação estreita e estruturada entre a Comissão, os Estados-Membros e o setor privado. Para alcançar este objetivo, os Estados-Membros deverão cooperar no âmbito do quadro estabelecido na Recomendação XXX/XXXX da Comissão [relativa a um conjunto de instrumentos comuns a nível da União para uma abordagem coordenada do Quadro Europeu para a Identidade Digital]¹⁵, a fim de identificar um conjunto de instrumentos para um Quadro Europeu para a Identidade Digital. O conjunto de instrumentos deverá incluir uma arquitetura técnica abrangente e um quadro de referência, um conjunto de normas comuns e referências técnicas, e um conjunto de orientações e descrições de boas práticas que contemplem, pelo menos, todos os aspetos das funcionalidades e da interoperabilidade das carteiras europeias de identidade digital, incluindo as assinaturas eletrónicas, e do serviço de confiança qualificado de certificados de atributos conforme estabelecido no presente regulamento. Neste contexto, os Estados-Membros deverão também chegar a acordo sobre elementos comuns de um modelo de negócio e da estrutura de taxas das carteiras europeias de identidade digital, para facilitar a adesão, em especial pelas pequenas e médias empresas num contexto transfronteiriço. O conteúdo do conjunto de instrumentos deverá evoluir em paralelo e refletir o resultado do debate e do processo de adoção do Quadro Europeu para a Identidade Digital.

(36-A) Os Estados-Membros deverão estabelecer regras em matéria de sanções aplicáveis pelas infrações, tais como práticas diretas ou indiretas que conduzam a confusão entre serviços de confiança não qualificados e qualificados ou à utilização abusiva da marca de confiança da UE por prestadores de serviços de confiança não qualificados. A marca de confiança da UE não deverá ser utilizada em condições que, direta ou indiretamente, levem à convicção de que quaisquer serviços de confiança não qualificados oferecidos por este prestador são qualificados.

¹⁵ [inserir referência quando adotada]

- (36-B) O presente regulamento deverá assegurar um nível harmonizado de qualidade, fiabilidade e segurança dos serviços de confiança qualificados, independentemente do local onde as operações são realizadas. Por conseguinte, um prestador de serviços de confiança qualificado deverá ser autorizado a externalizar as suas operações relacionadas com a prestação de um serviço de confiança qualificado fora da União, caso forneça garantias, assegurando que as atividades de supervisão e as auditorias possam ser executadas como se essas operações fossem realizadas na União. Se o cumprimento do regulamento não puder ser plenamente assegurado, as entidades supervisoras deverão poder adotar medidas proporcionadas e justificadas, incluindo a retirada do estatuto de qualificado do serviço de confiança prestado.
- (36-C) Para garantir a segurança jurídica no que respeita à validade de assinaturas eletrónicas avançadas com base em certificados qualificados, é essencial especificar os componentes das assinaturas eletrónicas avançadas com base em certificados qualificados que deverão ser avaliados pela parte utilizadora que procede à validação.
- (36-D) Os prestadores de serviços de confiança deverão utilizar algoritmos criptográficos que reflitam as boas práticas atuais e aplicações fiáveis desses algoritmos, a fim de garantir a segurança e a fiabilidade dos seus serviços de confiança.
- (36-E) O presente regulamento deverá estabelecer a obrigação de os prestadores qualificados de serviços de confiança verificarem a identidade de uma pessoa singular ou coletiva a quem o certificado qualificado é emitido com base em vários métodos harmonizados em toda a UE. Um método dessa natureza pode incluir o recurso a meios de identificação eletrónica que satisfaçam os requisitos de nível de garantia "substancial" em combinação com procedimentos adicionais harmonizados à distância que garantam a identificação da pessoa com um elevado nível de confiança.

- (36-F) Os emitentes 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 prestados por controladores de acesso para efeitos de fornecer bens ou prestar serviços a utilizadores finais, ou no decurso desse fornecimento ou prestação, deverão ser considerados utilizadores profissionais em conformidade com o artigo 2.º, parágrafo 21 do Regulamento (UE) 2022/1925. Por conseguinte, os controladores de acesso deverão ser obrigados a assegurar, a título gratuito, a interoperabilidade efetiva com as mesmas funcionalidades do sistema operativo, do equipamento informático ou do *software*, bem como o acesso para efeitos da interoperabilidade a essas mesmas funcionalidades, disponíveis ou utilizadas na prestação dos seus próprios serviços complementares e de apoio e no fornecimento do seu próprio equipamento informático. Tal deverá permitir que os emitentes de carteiras europeias de identidade digital e os emitentes de meios de identificação eletrónica notificados se interliguem, através de interfaces ou soluções semelhantes, às respetivas funcionalidades de forma tão eficaz como os serviços ou o equipamento informático do próprio controlador de acesso.
- (36-G) A fim de manter o presente regulamento em consonância com a evolução atual e seguir as práticas no mercado interno, os atos delegados e de execução adotados pela Comissão deverão ser revistos e, se necessário, atualizados regularmente. A avaliação da necessidade destas atualizações deverá ter em conta as novas tecnologias, práticas, normas ou especificações técnicas surgidas no mercado interno.
- (37) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 42.º, n.º 1, do Regulamento (UE) 2018/1525 do Parlamento Europeu e do Conselho¹⁶.
- (38) O Regulamento (UE) 910/2014 deve, por conseguinte, ser alterado em conformidade,

¹⁶ Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, JO L 295 de 21.11.2018, p. 39.

ADOTARAM O PRESENTE REGULAMENTO:

Artigo 1.º

O Regulamento (UE) n.º 910/2014 é alterado do seguinte modo:

1) O artigo 1.º passa a ter a seguinte redação:

"O presente regulamento visa assegurar o correto funcionamento do mercado interno e alcançar um nível adequado de segurança dos meios de identificação eletrónica e dos serviços de confiança. Para este efeito, o presente regulamento:

- a-A) Estabelece as condições em que os Estados-Membros prestam, reconhecem e aceitam os meios de identificação eletrónica para identificar pessoas singulares e coletivas no quadro de um sistema de identificação eletrónica notificado de outro Estado-Membro;
- a-B) Estabelece as condições em que os Estados-Membros fornecem e reconhecem as carteiras europeias de identidade digital;
- b) Estabelece normas aplicáveis aos serviços de confiança, nomeadamente às transações eletrónicas;
- c) Institui um quadro legal para as assinaturas eletrónicas, os selos eletrónicos, os selos temporais eletrónicos, os documentos eletrónicos, os serviços de envio registado eletrónico e os serviços de certificados para autenticação de sítios Web, a validação eletrónica de assinaturas eletrónicas, selos eletrónicos e respetivos certificados, a validação eletrónica dos certificados de autenticação de sítios Web, a preservação eletrónica de assinaturas eletrónicas, selos eletrónicos e respetivos certificados, o arquivo eletrónico, o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos;

2) O artigo 2.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

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

b) O n.º 3 passa a ter a seguinte redação:

"3. O presente regulamento não prejudica as disposições legislativas nacionais ou da União em matéria de celebração e validade de contratos nem outras obrigações legais ou de natureza processual relacionadas com a forma ou requisitos setoriais específicos relativos à forma.";

3) O artigo 3.º é alterado do seguinte modo:

X) O ponto 1 passa a ter a seguinte redação:

"1) "Identificação eletrónica": o processo de utilização dos dados de identificação pessoal em formato eletrónico que representam de modo único uma pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa singular ou coletiva;"

a) O ponto 2 passa a ter a seguinte redação:

"2) "Meio de identificação eletrónica": uma unidade material e/ou imaterial, incluindo as carteiras europeias de identidade digital, que contenha os dados de identificação pessoal e que seja utilizada para autenticação de um serviço em linha ou, se for caso disso, para um serviço fora de linha;"

a-A) O ponto 3 passa a ter a seguinte redação:

"3) "Dados de identificação pessoal": um conjunto de dados, emitido de acordo com a legislação nacional ou da União, que permitam determinar a identidade de uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa singular ou coletiva;

b) O ponto 4 passa a ter a seguinte redação:

"4) "Sistema de identificação eletrónica": um sistema de identificação eletrónica ao abrigo do qual sejam produzidos meios de identificação eletrónica para as pessoas singulares ou coletivas, ou para as pessoas singulares que representem pessoas singulares ou coletivas;"

b-A) O ponto 5 passa a ter a seguinte redação:

5) "Autenticação": o processo eletrónico que permite a identificação eletrónica de uma pessoa singular ou coletiva a confirmar ou da origem e integridade de um dado em formato eletrónico a confirmar;

b-B) É inserido o seguinte ponto 5-A:

5-A) "Utilizador": uma pessoa singular ou coletiva, ou uma pessoa singular que represente uma pessoa singular ou coletiva, que utilize serviços de confiança ou meios de identificação eletrónica, prestados nos termos do presente regulamento;

c) O ponto 14 passa a ter a seguinte redação:

"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;"

d) O ponto 16 passa a ter a seguinte redação:

"16) "Serviço de confiança": um serviço eletrónico geralmente prestado mediante remuneração, que consiste:

a) Na emissão de certificados para assinaturas eletrónicas, certificados para selos eletrónicos, certificados de autenticação de sítios Web ou certificados para a prestação de outros serviços de confiança;

a-A) Na validação de certificados para assinaturas eletrónicas, certificados para selos eletrónicos, certificados de autenticação de sítios Web ou certificados para a prestação de outros serviços de confiança;

b) Na criação de assinaturas eletrónicas ou de selos eletrónicos;

c) Na validação de assinaturas eletrónicas ou de selos eletrónicos;

d) Na preservação das assinaturas eletrónicas, dos selos eletrónicos, dos certificados de assinaturas eletrónicas ou dos certificados de selos eletrónicos;

e) Na gestão de dispositivos qualificados de criação de assinaturas eletrónicas à distância ou de dispositivos de criação de selos eletrónicos qualificados à distância;

f) Na emissão de certificados eletrónicos de atributos;

- f-A) Na validação de certificados eletrónicos de atributos;
- g) Na criação de selos temporais eletrónicos;
- g-A) Na validação de selos temporais eletrónicos;
- g-B) Na prestação de serviços de envio registado eletrónico;
- g-C) Na validação dos dados transmitidos através de serviços de envio registado eletrónico e elementos de prova conexos;
- h) No arquivo eletrónico de dados eletrónicos; ou
- i) No registo de dados eletrónicos num livro-razão eletrónico;

d-A) O ponto 18 passa a ter a seguinte redação:

(18) "Organismo de avaliação da conformidade": o organismo definido no artigo 2.º, n.º 13, do Regulamento (CE) n.º 765/2008, que é acreditado nos termos do mesmo regulamento como sendo competente para realizar a avaliação da conformidade dos prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados, ou para proceder à certificação de carteiras europeias de identidade digital ou de meios de identificação eletrónica;

e) O ponto 21 passa a ter a seguinte redação:

"21) "Produto": equipamento informático ou *software*, ou componentes pertinentes de equipamento informático e/ou *software*, que se destinem a ser utilizados para a prestação de serviços de identificação eletrónica e de serviços de confiança;"

f) São inseridos os seguintes pontos 23-A e 23-B:

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

"23-B) "Dispositivo qualificado de criação de selos eletrônicos à distância": um dispositivo qualificado de criação de selos eletrônicos gerido por um prestador qualificado de serviços de confiança nos termos do artigo 39.º-A em nome de um criador do selo;

g) O ponto 29 passa a ter a seguinte redação:

"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;"

h) O ponto 41 passa a ter a seguinte redação:

"41) "Validação": o processo pelo qual é verificada e confirmada a validade dos dados em formato eletrónico de acordo com os requisitos do presente regulamento";

i) São aditados os pontos 42 a 55-B que se seguem:

"42) "Carteira europeia de identidade digital": um meio de identificação eletrónica que permite ao utilizador armazenar e extrair dados de identidade, incluindo dados de identificação pessoal, certificados eletrónicos de atributos associados à sua identidade, com vista a fornecê-los a partes utilizadoras mediante pedido e a utilizá-los para autenticação, em linha e, se for caso disso, fora de linha, para um serviço em conformidade com o artigo 6.º-A; e permite assinar através de assinaturas eletrónicas qualificadas e utilizar selos através de selos eletrónicos qualificados;"

- 43) "Atributo": a característica, a qualidade, o direito ou a 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 seja emitido por um prestador qualificado de serviços de confiança e satisfaça os requisitos estabelecidos no anexo V;
- 45-A) "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-DA, e que cumpre os requisitos estabelecidos no anexo VII;
- 46) "Fonte autêntica": um repositório ou sistema, sob a responsabilidade de um organismo do setor público ou de uma entidade privada, que contém e fornece os atributos relativos a uma pessoa singular ou coletiva e é considerado uma fonte principal dessa informação ou reconhecido como autêntico de acordo com a legislação nacional ou da União, incluindo a prática administrativa;
- 47) "Arquivo eletrónico": um serviço que assegura a receção, o armazenamento, a recuperação e a supressão de dados eletrónicos, a fim de garantir a sua durabilidade e legibilidade, bem como para preservar a sua integridade, confidencialidade e prova de origem durante todo o período de conservação;

- 48) "Serviço qualificado de arquivo eletrónico": um serviço de arquivo eletrónico que satisfaça os requisitos estabelecidos no artigo 45.º-GA;
- 49) "Marca de confiança de carteira de identidade digital da UE": uma indicação verificável de um modo simples, reconhecível e claro de que uma carteira europeia de identidade digital foi fornecida em conformidade com o presente regulamento;
- 50) "Autenticação forte do utilizador": uma autenticação baseada na utilização de pelo menos dois fatores de autenticação pertencentes a categorias diferentes, quer de conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) ou de inerência (algo que o utilizador é), 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;
- 53) "Livro-razão eletrónico": uma sequência de registos eletrónicos de dados que assegura a sua integridade e a exatidão da sua ordem sequencial";
- 53-A) "Livro-razão eletrónico qualificado": um livro-razão eletrónico que satisfaça os requisitos estabelecidos no artigo 45.º-I;
- 54) "Dados pessoais": qualquer informação na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679";
- 55) "Correspondência de registos": um processo em que os dados de identificação pessoal, os meios de identificação pessoal, os certificados eletrónicos qualificados de atributos ou os certificados de atributos emitidos por ou em nome de um organismo do setor público responsável por uma fonte autêntica são correspondidos ou ligados a uma conta existente pertencente à mesma pessoa";

- 55-A) "Identificador único e persistente": um identificador que pode consistir em dados de identificação nacionais ou setoriais únicos ou múltiplos, está associado a um único utilizador num determinado sistema e é persistente no tempo;
- 55-B) "Registo de dados": os dados eletrónicos registados com metadados (ou atributos) conexos que apoiam o tratamento dos dados.
- 55-C) "Utilização fora de linha das carteiras europeias de identidade digital": uma interação entre um utilizador e uma parte utilizadora num local físico, em que a carteira não é obrigada a aceder a sistemas remotos através de redes de comunicações eletrónicas para efeitos da interação.

"Artigo 5.º

Pseudónimos em transações eletrónicas

Sem prejuízo dos efeitos legais conferidos aos pseudónimos nos termos das legislações nacionais, não é proibido utilizar pseudónimos em transações eletrónicas.";

- 5) No capítulo II, é inserido o seguinte título antes do artigo 6.º-A:

"SECÇÃO I

Carteira europeias de identidade digital;

7) São inseridos os seguintes artigos (6.º-A, 6.º-B, 6.º-C e 6.º-D):

"Artigo 6.º-A

Carteiras europeias de identidade digital

1. A fim de assegurar que todas as pessoas singulares e coletivas na União dispõem de acesso transfronteiras seguro, contínuo e de confiança a serviços públicos e privados, cada Estado-Membro assegura que a carteira europeia de identidade digital é fornecida no prazo de 24 meses após a entrada em vigor dos atos de execução a que se refere o n.º 11 e o artigo 6.º-C, n.º 4.
2. As carteiras europeias de identidade digital são fornecidas:
 - a) Por um Estado-Membro;
 - b) Por mandato de um Estado-Membro; ou
 - c) De forma independente de um Estado-Membro, mas reconhecida por um Estado-Membro.
3. As carteiras europeias de identidade digital são meios de identificação eletrónica que permitem ao utilizador, de um modo que seja transparente e rastreável pelo utilizador:
 - a) Solicitar, selecionar, combinar, armazenar, apagar e apresentar de forma segura certificados eletrónicos de atributos e dados de identificação pessoal às partes utilizadoras, incluindo a autenticação em linha e, se for caso disso, fora de linha, a fim de utilizar serviços públicos e privados, assegurando simultaneamente a possibilidade de divulgação seletiva de dados;
 - b) Assinar através de assinaturas eletrónicas qualificadas e utilizar selos através de selos eletrónicos qualificados.

4. Nomeadamente, as carteiras de identidade digital:
- a) Fornecem um conjunto de interfaces comum:
 - 1) 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;
 - 2) Às partes utilizadoras, para pedirem dados de identificação pessoal e certificados eletrónicos de atributos;
 - 3) Para a apresentação às partes utilizadoras de dados de identificação pessoal ou de certificados eletrónicos de atributos em linha e, se for caso disso, também fora de linha;
 - 4) Ao utilizador, para permitir a interação com a carteira europeia de identidade digital e exibir uma "marca de confiança de carteira de identidade digital da UE";
 - b) Não fornecem quaisquer informações aos prestadores de serviços de confiança de certificados eletrónicos de atributos sobre a utilização desses atributos após a sua emissão;
 - b-A) Asseguram que a identidade das partes utilizadoras possa ser validada através da aplicação de mecanismos de autenticação em conformidade com o artigo 6.º-B;
 - c) Cumprem os requisitos estabelecidos no artigo 8.º no que diz respeito ao nível de garantia "elevado" aplicável *mutatis mutandis* à gestão e utilização de dados de identificação pessoal através da carteira, incluindo a identificação e autenticação eletrónicas;
 - e) Asseguram que os dados de identificação pessoal a que se refere o artigo 12.º, n.º 4, alínea d), representam única e persistentemente a pessoa singular ou coletiva ou uma pessoa singular que represente uma pessoa singular ou coletiva associada à carteira.

- 4-A. Os Estados-Membros preveem procedimentos que permitam ao utilizador comunicar eventuais perdas ou utilizações abusivas da sua carteira e solicitar a sua revogação.
5. Os Estados-Membros fornecem mecanismos de validação para as carteiras europeias de identidade digital:
- a) Para garantir que a sua autenticidade e validade podem ser verificadas;
 - d) Para permitir ao utilizador autenticar as partes utilizadoras em conformidade com o artigo 6.º-B;
6. As carteiras europeias de identidade digital são emitidas ao abrigo de um sistema de identificação eletrónica notificado com nível de garantia "elevado".
- 6-A. A emissão e utilização para autenticação e revogação das carteiras europeias de identidade digital é gratuita para pessoas singulares.
- 6-B. Sem prejuízo do artigo 6.º-DB, 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.
7. Os utilizadores controlam plenamente a utilização da carteira europeia de identidade digital e dos dados da sua carteira europeia de identidade digital. O emitente da carteira europeia de identidade digital não recolhe informações sobre a utilização da carteira que não sejam necessárias para a prestação dos serviços da carteira, nem combina os dados de identificação pessoal e 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, salvo pedido expresso do utilizador. Os dados pessoais relacionados com o fornecimento de carteiras europeias de identidade digital são conservados e são logicamente separados de quaisquer outros dados detidos pelo emitente das carteiras europeias 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), o disposto no artigo 45.º-F, n.º 4, aplica-se *mutatis mutandis*.

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

a) O organismo responsável pela elaboração e manutenção da lista das partes utilizadoras notificadas que recorrem às carteiras europeias de identidade digital, em conformidade com o artigo 6.º-B, n.º 2;

b) Os organismos responsáveis pelo fornecimento das carteiras europeias de identidade digital, em conformidade com o artigo 6.º-A, n.º 1;

c) Os organismos responsáveis por assegurar que os dados de identificação da pessoa estão associados à carteira, em conformidade com o artigo 6.º-A, n.º 4, alínea e);

A notificação também contém informações sobre o mecanismo que permite a validação dos dados de identificação da pessoa a que se refere o artigo 12.º, n.º 4, e sobre a identidade das partes utilizadoras.

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

8. O artigo 11.º aplica-se *mutatis mutandis* à carteira europeia de identidade digital.
9. O artigo 24.º, n.º 2, alíneas b), e), g) e h), aplica-se *mutatis mutandis* aos emitentes que emitam carteiras europeias de identidade digital.
10. A carteira europeia de identidade digital é disponibilizada a pessoas com deficiência em conformidade com os requisitos de acessibilidade constantes da Diretiva (UE) 2019/882.

11. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão estabelece especificações técnicas e operacionais e normas de referência para os requisitos referidos nos n.ºs 3, 4, 5 e 7 mediante um ato de execução relativo à implementação da carteira europeia de identidade digital. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.
- 11-A. A Comissão estabelece especificações técnicas e operacionais, bem como normas de referência, a fim de facilitar a integração na carteira europeia de identidade digital dos utilizadores utilizando meios de identificação eletrónica conformes com o nível "elevado" ou meios de identificação eletrónica conformes com o nível "substancial", em conjugação com procedimentos de integração à distância adicionais que, em conjunto, cumpram os requisitos de nível de garantia "elevado". Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

Artigo 6.º-B

Partes utilizadoras de carteiras europeias de identidade digital

1. Sempre que as partes utilizadoras que prestam serviços privados ou públicos pretendam recorrer a carteiras europeias de identidade digital emitidas de acordo com o presente regulamento, notificam a sua intenção ao Estado-Membro onde estão estabelecidas.
- 1-A. O procedimento de notificação é eficaz em termos de custos e proporcional ao risco e assegura que as partes utilizadoras fornecem, pelo menos, as informações necessárias para autenticar as carteiras europeias de identidade digital. Tal inclui, no mínimo, o Estado-Membro em que se encontram estabelecidos e o nome da parte utilizadora e, se for caso disso, o seu número de registo, tal como indicado nos registos oficiais.

- 1-B. A obrigação de notificação não prejudica outros requisitos de notificação e registo em conformidade com a legislação nacional ou da União, como os aplicáveis a categorias especiais de dados pessoais, que podem exigir requisitos de autorização adicionais.
- 1-C. Os Estados-Membros podem isentar as partes utilizadoras da obrigação de notificação nos casos em que a legislação nacional ou da União não preveja requisitos específicos de notificação ou registo para aceder às informações fornecidas através da carteira europeia de identidade digital. As partes utilizadoras isentas podem não ter de se autenticar na carteira europeia de identidade digital.
- 1-D. As partes utilizadoras notificadas nos termos do presente artigo informam sem demora o Estado-Membro de qualquer alteração subsequente das informações inicialmente prestadas.
2. As partes utilizadoras asseguram a aplicação dos mecanismos de autenticação referidos no artigo 6.º-A, n.º 4, alínea b-A).
3. As partes utilizadoras são responsáveis por executar o procedimento de autenticação de pessoas e de validar certificados eletrónicos de atributos com origem em carteiras europeias de identidade digital, obtidos através da interface comum, em conformidade com o artigo 6.º-A, n.º 4, alínea a), parágrafo 2.
4. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão estabelece especificações técnicas e operacionais para os requisitos referidos nos n.ºs 1, 1-A e 1-D mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital, como referido no artigo 6.º-A, n.º 11. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

Artigo 6.º-C

Certificação de carteiras europeias de identidade digital

1. A conformidade das carteiras europeias de identidade digital com os requisitos estabelecidos no artigo 6.º-A, n.ºs 3, 4 e 5, com o requisito de separação lógica estabelecido no artigo 6.º-A, n.º 7, e, se for caso disso, com os requisitos estabelecidos no artigo 6.º-A, n.º 11-A, é certificada por organismos de avaliação da conformidade acreditados nos termos do artigo 60.º do Regulamento Cibersegurança e com os sistemas, especificações, normas e procedimentos referenciados nos termos do n.º 4, alíneas a), a-A) e a-AA), e designados pelos Estados-Membros. A certificação não excede cinco anos, sob reserva de uma avaliação regular das vulnerabilidades de dois anos. Sempre que sejam identificadas vulnerabilidades e as mesmas não sejam sanadas no prazo de três meses, a certificação é cancelada.
2. No que diz respeito ao cumprimento dos requisitos em matéria de proteção de dados previstos no artigo 6.º-A, n.º 7, a certificação nos termos do n.º 1 pode ser complementada por uma certificação nos termos do artigo 42.º do Regulamento (UE) 2016/679.
3. A conformidade das carteiras europeias de identidade digital, ou de partes destas, com os requisitos pertinentes em matéria de cibersegurança estabelecidos no artigo 6.º-A, n.ºs 3, 4, 5, 6 e 7 e, quando aplicável 11-A, é certificada pelos organismos de avaliação da conformidade a que se refere o n.º 1, ao abrigo dos sistemas de certificação da cibersegurança pertinentes nos termos do Regulamento (UE) 2019/881, tal como são referenciados nos termos dos n.ºs 4, alínea a), e a-A).
- 3-A. As carteiras europeias de identidade digital certificadas não estão sujeitas aos requisitos a que se referem os artigos 7.º e 9.º.

4. No prazo de 6 meses após a entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução:
- a) Uma lista dos sistemas de certificação da cibersegurança nos termos do Regulamento (UE) 2019/881, exigidos para a certificação das carteiras europeias de identidade digital a que se refere o n.º 3;
 - a-A) As especificações, procedimentos e normas de referência para a sua utilização ao abrigo dos sistemas de certificação da cibersegurança pertinentes enumerados em conformidade com a alínea a);
 - a-AA) Uma lista de especificações, procedimentos e normas de referência que estabelecem requisitos comuns de certificação não abrangidos pelos sistemas de certificação da cibersegurança pertinentes nos termos do Regulamento (UE) 2019/881 para efeitos da certificação a que se refere o n.º 1, com o objetivo de demonstrar que uma carteira europeia de identidade digital cumpre os requisitos a que se refere o n.º 1;
 - b) Especificações técnicas, processuais, organizativas e operacionais para a designação dos organismos de avaliação da conformidade a que se refere o n.º 1 e, no que respeita aos requisitos de certificação estabelecidos nos termos da alínea a-AA), para o controlo e revisão dos sistemas de certificação e dos métodos de avaliação conexos utilizados por esses organismos, bem como dos certificados e relatórios de certificação que emitem;
5. Os Estados-Membros comunicam à Comissão a denominação e o endereço das entidades públicas ou privadas a que se refere o n.º 1. A Comissão põe a informação à disposição dos Estados-Membros.
6. Os atos de execução referidos no n.º 4 são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

Artigo 6.º-D

Publicação de uma lista de carteiras europeias de identidade digital certificadas

1. Os Estados-Membros informam a Comissão sem demora injustificada sobre as carteiras europeias de identidade digital que foram fornecidas nos termos do artigo 6.º-A e certificadas pelas entidades a que se refere o artigo 6.º-C, n.º 1. Informam igualmente a Comissão sem demora injustificada se a certificação for cancelada.
2. Com base nas informações recebidas, a Comissão elabora, publica e atualiza uma lista de carteiras europeias de identidade digital certificadas legível por máquina.
3. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão define formatos e procedimentos aplicáveis para efeitos dos n.ºs 1 e 2 mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital conforme referido no artigo 6.º-A, n.º 11. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

Artigo 6.º-DA

Violação da segurança das carteiras europeias de identidade digital

1. Se as carteiras europeias de identidade digitais fornecidas nos termos do artigo 6.º-A ou de acordo com os mecanismos de validação a que se refere o artigo 6.º-A, n.º 5, alíneas a), d) e e), forem violadas ou ficarem parcialmente comprometidas de uma forma que afete a sua fiabilidade ou a fiabilidade das demais carteiras europeias de identidade digital, o emitente das carteiras em causa suspende, sem demora, a emissão e a utilização da carteira europeia de identidade digital. O Estado-Membro em que foram fornecidas as carteiras em causa informa sem demora injustificada os Estados-Membros e a Comissão. O emitente das carteiras em causa ou o Estado-Membro em causa informa as partes utilizadoras e os utilizadores em conformidade.

2. Se a violação ou o comprometimento referidos no n.º 1 forem sanados, o emitente da carteira restabelece a emissão e utilização da carteira europeia de identidade digital. O Estado-Membro em que foram fornecidas as carteiras em causa informa sem demora injustificada os Estados-Membros e a Comissão. O emitente das carteiras em causa ou o Estado-Membro em causa informa, sem demora injustificada, as partes utilizadoras e os utilizadores.
3. Se a violação ou o comprometimento a que se refere o n.º 1 não forem sanados no prazo de três meses a contar da suspensão, o Estado-Membro em causa retira a carteira de identidade europeia digital em questão e informa em conformidade os outros Estados-Membros e a Comissão. Sempre que a gravidade da violação o justifique, a carteira europeia de identidade digital em questão é retirada sem demora injustificada.
4. A Comissão publica no *Jornal Oficial da União Europeia*, sem demora indevida, as alterações correspondentes à lista a que se refere o artigo 6.º-D.
5. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão especifica mais pormenorizadamente as medidas referidas nos n.ºs 1, 2 e 3 mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital como previsto no artigo 6.º-A, n.º 11. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

Artigo 6.º-DB

Recurso transfronteiriço às carteiras europeias de identidade digital

1. Sempre que os Estados-Membros exigirem uma identificação eletrónica baseada num meio de identificação eletrónica e numa 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 para a autenticação do utilizador.
2. Sempre que as partes utilizadoras privadas prestadoras de serviços, com exceção das microempresas e das pequenas empresas, tal como definidas na Recomendação 2003/361/CE da Comissão, forem obrigadas pela legislação nacional ou da União a utilizar autenticação forte do utilizador para identificação em linha, ou sempre que a autenticação forte do utilizador for exigida por obrigação contratual, nomeadamente nos domínios dos transportes, da energia, do serviços bancários, serviços financeiros, da segurança social, da saúde, da água potável, dos serviços postais, das infraestruturas digitais, da educação ou das telecomunicações, as partes utilizadoras privadas aceitam, o mais tardar 12 meses após a data de fornecimento das carteiras europeias de identidade digital nos termos do artigo 6.º-A, n.º 1, e, estritamente mediante pedido voluntário do utilizador, aceitam igualmente a utilização de carteiras europeias de identidade digital fornecidas em conformidade com o presente regulamento no que diz respeito aos dados mínimos necessários para o serviço em linha específico para o qual é solicitada a autenticação do utilizador.
3. Sempre que as plataformas de muito grande dimensão, conforme definidas no artigo 25.º, n.º 1, do Regulamento [referência Regulamento Serviços Digitais], exigirem que os utilizadores se autenticem para aceder a serviços em linha, aceitam igualmente a utilização de carteiras europeias de identidade digital fornecidas de acordo com o presente regulamento para a autenticação do utilizador, estritamente mediante pedido voluntário do utilizador e respeitando os dados mínimos necessários para o serviço em linha específico para o qual é pedida a autenticação.

4. Em cooperação com os Estados-Membros, a Comissão encoraja e facilita a elaboração de códigos de conduta, a fim de contribuir para a ampla disponibilidade e usabilidade de carteiras europeias de identidade digital previstas no âmbito do presente regulamento. Esses códigos de conduta facilitam a aceitação de meios de identificação eletrónica, incluindo as carteiras europeias de identidade digital previstas no âmbito do presente regulamento, em especial por parte dos prestadores de serviços que dependem de serviços de identificação eletrónica de terceiros para autenticar os utilizadores. A Comissão facilitará a elaboração desses códigos de conduta em estreita cooperação com todas as partes interessadas e incentivará os prestadores de serviços a concluírem a elaboração dos códigos de conduta no prazo de 12 meses a contar da adoção do presente regulamento e a aplicá-los efetivamente no prazo de 18 meses a contar da adoção do regulamento.
5. Com base em dados que demonstram a procura, disponibilidade e usabilidade das carteiras europeias de identidade digital, a Comissão avalia, no prazo de 24 meses após a sua implantação, se outros prestadores de serviços em linha privados devem ser obrigados a aceitar a utilização da carteira europeia de identidade digital estritamente mediante pedido voluntário do utilizador. Os critérios de avaliação incluem a dimensão da base de utilizadores, a presença transfronteiriça de prestadores de serviços, o desenvolvimento tecnológico, a evolução dos padrões de utilização e a procura dos utilizadores.

8) Antes do artigo 7.º, é inserido o seguinte título:

"SECÇÃO II

SISTEMAS DE IDENTIFICAÇÃO ELETRÓNICA";

9) O proémio do artigo 7.º passa a ter a seguinte redação:

"Nos termos do artigo 9.º, n.º 1, os Estados-Membros que ainda não o tenham feito notificam, no prazo de 24 meses após a entrada em vigor dos atos de execução referidos no artigo 6.º-A, n.º 11, e no artigo 6.º-C, n.º 4, pelo menos um sistema de identificação eletrónica que inclua, no mínimo, um meio de identificação com um nível de garantia "elevado". Um sistema de identificação eletrónica é elegível para notificação nos termos do artigo 9.º, n.º 1, desde que estejam reunidas todas as seguintes condições:";

10) No artigo 9.º, os n.ºs 2 e 3 passam a ter a seguinte redação:

"2. A Comissão publica no *Jornal Oficial da União Europeia* uma lista dos sistemas de identificação eletrónica que tenham sido notificados nos termos do n.º 1 do presente artigo e as informações básicas a eles respeitantes.

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

12) É inserido o seguinte artigo 11.º-A:

"*Artigo 11.º-A*

Correspondência de registos

1. Quando os meios de identificação eletrónica notificados ou as carteiras europeias de identidade digital forem utilizados para autenticação, os Estados-Membros, quando atuam como partes utilizadoras, asseguram a correspondência de registos.

2. Para efeitos da prestação de carteiras europeias de identidade digital, os Estados-Membros incluem no conjunto mínimo de dados de identificação pessoal a que se refere o artigo 12.º, n.º 4, alínea d), pelo menos um identificador único e persistente em conformidade com a legislação da União e com a legislação nacional, para identificar o utilizador a seu pedido nos casos em que a identificação do utilizador seja obrigatória por lei.
- 2-A. Os Estados-Membros preveem medidas técnicas e organizativas para assegurar um elevado nível de proteção dos dados pessoais utilizados para a correspondência de registos e para impedir a definição de perfis dos utilizadores.
- 2-AA. Os Estados-Membros podem prever, em conformidade com o direito nacional, que o utilizador da carteira europeia de identidade digital possa solicitar que um identificador único e persistente incluído no conjunto mínimo de dados de identificação pessoal e associado à carteira, em conformidade com o artigo 6.º-A, n.º 4, alínea e), seja substituído por outro identificador único e persistente emitido pelo Estado-Membro.
3. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão especifica mais pormenorizadamente as medidas referidas nos n.º 1 mediante um ato de execução. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.
- 3-A. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão especifica as medidas referidas nos n.º 2 e 2-AA mediante um ato de execução. Esse ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

13) O artigo 12.º é alterado do seguinte modo:

Cooperação e interoperabilidade

a) No n.º 3, é suprimida a alínea d);

b) No n.º 4, a alínea d) passa a ter a seguinte redação:

"d) A referência a um conjunto mínimo de dados de identificação necessários para representar de modo único e persistente uma pessoa singular ou coletiva ou de uma pessoa singular que represente uma pessoa singular ou coletiva;"

b-A) No n.º 5, é inserida a alínea c):

"c) A abordagem semelhante em relação aos serviços em linha que aceitam a utilização de carteiras europeias de identidade digital fornecidas em conformidade com o presente regulamento;"

c) No n.º 6, a alínea a) passa a ter a seguinte redação:

"a) O intercâmbio de informações, experiências e boas práticas relativamente aos sistemas de identificação eletrónica, nomeadamente no que respeita aos requisitos técnicos relacionados com a interoperabilidade, a correspondência de registos e os níveis de garantia;"

c-A) No n.º 6, é inserida a alínea e):

"e) O intercâmbio de informações, experiências e boas práticas e a emissão de orientações sobre a forma como os serviços em linha podem ser concebidos, desenvolvidos e aplicados com o objetivo de recorrer às carteiras europeias de identidade digital."

14) São aditados os artigos 12.º-A e 12.º-B seguintes:

"Artigo 12.º-A

Certificação de sistemas de identificação eletrónica

1. A conformidade dos sistemas de identificação eletrónica a notificar com os requisitos estabelecidos no presente regulamento é certificada para demonstrar a conformidade desses sistemas ou partes dos mesmos com os requisitos estabelecidos no artigo 8.º, n.º 2, no que diz respeito aos níveis de garantia dos sistemas de identificação eletrónica ao abrigo de um sistema de certificação da cibersegurança pertinente nos termos do Regulamento (UE) 2019/881, ou partes do mesmo, na medida em que o certificado de cibersegurança ou partes do mesmo abrangam os requisitos estabelecidos no artigo 8.º, n.º 2, no que diz respeito aos níveis de garantia dos sistemas de identificação eletrónica. A certificação não excede cinco anos, sob reserva de uma avaliação regular das vulnerabilidades de dois anos. Sempre que sejam identificadas vulnerabilidades e as mesmas não sejam sanadas no prazo de três meses, a certificação é cancelada.

A certificação é efetuada por organismos de avaliação da conformidade acreditados, públicos ou privados, designados pelos Estados-Membros e em conformidade com o Regulamento (CE) n.º 765/2008.

2. A avaliação pelos pares dos sistemas de identificação eletrónica a que se refere o artigo 12.º, n.º 6, alínea c), não se aplica aos sistemas de identificação eletrónica ou a parte desses sistemas certificados em conformidade com o n.º 1.
- 2-A. Não obstante o disposto no n.º 2 do presente artigo, os Estados-Membros podem solicitar ao Estado-Membro notificante informações adicionais sobre os sistemas de identificação eletrónica, ou parte dos mesmos, certificados nos termos do n.º 2 do presente artigo.
3. 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.";

"Artigo 12.º-B

Acesso a funcionalidades de equipamento informático e de *software*

Os emitentes 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, n.º 2, do Regulamento (UE) 2022/1925 para efeitos da prestação de serviços de carteira europeia de identidade digital e de meios de identificação eletrónica aos utilizadores finais, ou no decurso dessa prestação, são utilizadores profissionais em conformidade com o artigo 2.º, parágrafo 21 do Regulamento (UE) 2022/1925.

17) No artigo 13.º, o n.º 1 passa a ter a seguinte redação:

"1. Não obstante o disposto no n.º 2 do presente artigo, os prestadores de serviços de confiança respondem pelos danos causados deliberadamente ou por negligência a todas as pessoas singulares ou coletivas por incumprimento das obrigações previstas no presente regulamento";

O ónus da prova da intenção 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 intenção ou negligência de um prestador qualificado de serviços de confiança, exceto se este provar que os danos referidos no primeiro parágrafo não foram causados por sua intenção ou negligência.

18) O artigo 14.º passa a ter a seguinte redação:

"Artigo 14.º

Aspetos 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 nos termos de uma decisão de execução ou de um acordo celebrado entre a União e o país terceiro em causa ou uma organização internacional em conformidade com o artigo 218.º do TFUE.
2. As decisões de execução e os acordos 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 ou organizações internacionais e pelos serviços de confiança que fornecerem. Os países terceiros e as organizações internacionais, em especial, estabelecem, mantêm e publicam uma lista de prestadores de serviços de confiança reconhecidos.

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 organizações internacionais com os quais tenham sido celebrados acordos.
3. As decisões de execução referidas no n.º 1 são adotadas pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

19) O artigo 15.º passa a ter a seguinte redação:

"Artigo 15.º

Acessibilidade para as pessoas com deficiência

A prestação de serviços de confiança e os produtos de utilizador final utilizados na prestação desses serviços serão acessíveis às pessoas com deficiência em conformidade com os requisitos de acessibilidade constantes I da Diretiva (UE) 2019/882 relativa aos requisitos de acessibilidade dos produtos e serviços.";

20) O artigo 17.º é alterado do seguinte modo:

a) O n.º 4 é alterado do seguinte modo:

1) A alínea c) do n.º 4 passa a ter a seguinte redação:

"c) Informar as autoridades nacionais competentes do Estado-Membro em causa, designadas nos termos da Diretiva (UE) XXXX/XXXX [SRI 2], sobre quaisquer violações significativas da segurança ou perdas de integridade de que tenham tido conhecimento no exercício das suas funções. Sempre que a violação significativa da segurança ou perda da integridade afete outros Estados-Membros, a entidade supervisora informa o ponto de contacto único do Estado-Membro em causa, designado nos termos da Diretiva (UE) XXXX/XXXX (SRI 2), e as entidades supervisoras designadas nos termos do artigo 17.º do presente regulamento nos outros Estados-Membros em causa. A entidade supervisora notificada informa o público ou exige que o prestador do serviço de confiança o faça, se considerar que a divulgação da violação da segurança ou perda de integridade é do interesse público;"

2) A alínea f) passa a ter a seguinte redação:

"f) Para cooperar com as autoridades de controlo competentes criadas nos termos 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;"

b) O n.º 6 passa a ter a seguinte redação:

"6. Até 31 de março de cada ano, as entidades supervisoras apresentam à Comissão um relatório sobre as principais atividades do ano anterior.";

c) O n.º 8 passa a ter a seguinte redação:

"8. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão adota orientações sobre o exercício pelos órgãos de supervisão das atribuições referidas no n.º 4 e, por meio de atos de execução adotados em conformidade com o procedimento de exame a que se refere o artigo 48.º, n.º 2, define os formatos e os procedimentos para o relatório a que se refere o n.º 6.";

21) O artigo 18.º é alterado do seguinte modo:

a) O título do artigo 18.º passa a ter a seguinte redação:

"Assistência mútua e cooperação";

b) O n.º 1 passa a ter a seguinte redação:

"1. As entidades supervisoras cooperam tendo em vista o intercâmbio de boas práticas e informações relativas à prestação de serviços de confiança.";

c) São aditados os seguintes n.ºs 4 e 5:

- "4. As entidades supervisoras e as autoridades nacionais competentes previstas na Diretiva (UE) XXXX/XXXX do Parlamento Europeu e do Conselho [SRI 2] cooperam e auxiliam-se mutuamente para assegurar que os prestadores de serviços de confiança cumprem os requisitos estabelecidos no presente regulamento e na Diretiva (UE) XXXX/XXXX [SRI 2]. Os órgãos de supervisão solicitam às autoridades nacionais competentes previstas na Diretiva XXXX/XXXX [SRI 2] que realizem ações de supervisão para verificar se os prestadores de serviços de confiança cumprem os requisitos previstos na Diretiva XXXX/XXXX (SRI 2), que exijam aos prestadores de serviços de confiança que sanem todos os incumprimentos desses requisitos, que transmitam oportunamente os resultados de todas as atividades de supervisão associadas a prestadores de serviços de confiança e que informem as entidades supervisoras sobre incidentes relevantes notificados de acordo com a Diretiva XXXX/XXXX [SRI 2].
5. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as necessárias modalidades processuais de facilitação da cooperação entre as autoridades supervisoras a que se refere o n.º 1. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.º";

21-A) É inserido o seguinte 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. Não obstante o disposto no artigo 18.º da Diretiva (UE) XXXX/XXX [SRI 2], essas medidas incluem, no mínimo, o seguinte:
 - i) medidas relacionadas com os procedimentos de registo e integração num serviço,
 - ii) medidas relacionadas com controlos processuais ou administrativos,
 - iii) medidas relacionadas com a gestão e implementação de serviços;
 - b) Notificam a entidade supervisora, as pessoas afetadas identificáveis, o público, se for de interesse público, e, se for caso disso, outros organismos competentes, de quaisquer violações ou perturbações na prestação do serviço ou na aplicação das medidas referidas no n.º, alínea a), subalíneas i), ii) e iii), que tenham um impacto significativo no serviço de confiança prestado ou nos dados pessoais nele conservados, sem demora injustificada e, em qualquer caso, o mais tardar 24 horas após terem tomado conhecimento dessas violações.
2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão específica, por meio de atos de execução, as características técnicas relativas às medidas a que se refere o n.º 1, alínea a). Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

22) O artigo 20.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

"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 deve confirmar 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 18.º da Diretiva (UE) XXXX/XXXX [SRI 2]. Os prestadores qualificados de serviços de confiança apresentam o relatório de avaliação da conformidade à entidade supervisora no prazo de três dias úteis depois de o terem recebido.";

a-A) É inserido o seguinte número:

1-A. Os Estados-Membros podem prever que os prestadores qualificados de serviços de confiança informem previamente a entidade supervisora sobre as auditorias previstas e permitam a participação da entidade supervisora na qualidade de observador, mediante pedido.

b) No n.º 2, a última frase passa a ter a seguinte redação:

"Em caso de suspeita de violação das regras de proteção de dados pessoais, a entidade supervisora informa, sem demora injustificada, as autoridades de controlo competentes previstas no Regulamento (UE) 2016/679.";

c) Os n.ºs 3 e 4 passam a ter a seguinte redação:

"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 no prazo fixado pela entidade supervisora, se aplicável, esta pode – tendo em conta, nomeadamente, a extensão, a duração e as consequências desse incumprimento – retirar o estatuto de qualificado ao prestador ou ao serviço afetado por ele prestado.

3-A. Se a entidade supervisora for informada pelas autoridades nacionais competentes – nos termos da Diretiva (UE) XXXX/XXXX [SRI 2] – de que o prestador qualificado de serviços de confiança não cumpre algum dos requisitos estabelecidos pelo artigo 18.º da Diretiva (UE) XXXX/XXXX [SRI 2], a entidade supervisora – tendo em conta, nomeadamente, a extensão, a duração e as consequências desse incumprimento – pode retirar o estatuto de qualificado ao prestador ou ao serviço afetado por ele prestado.

3-B. Se a entidade supervisora for informada pelas autoridades supervisoras, nos termos do Regulamento (UE) 2016/679, de que o prestador qualificado de serviços de confiança não cumpre algum dos requisitos estabelecidos pelo Regulamento (UE) 2016/679, a entidade supervisora – tendo em conta, nomeadamente, a extensão, a duração e as consequências desse incumprimento – pode retirar o estatuto de qualificado ao prestador ou ao serviço afetado 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 a que se refere o artigo 22.º, n.º 3, para efeitos de atualização das listas de confiança referidas no artigo 22.º, n.º 1 e a autoridade nacional competente a que se refere a Diretiva XXXX [SRI2].
4. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as seguintes especificações técnicas e os números de referência das normas:
- 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 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.

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

23) O artigo 21.º é alterado do seguinte modo:

"1. Sempre que os prestadores de serviços de confiança tencionem começar a prestar um serviço de confiança qualificado, apresentam à entidade supervisora uma notificação da sua intenção, juntamente com um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade que confirme o cumprimento dos requisitos estabelecidos no presente regulamento e no artigo 18.º da Diretiva (UE) XXXX/XXXX [SRI 2].";

a) O n.º 2 passa a ter a seguinte redação:

"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, designadamente os requisitos previstos para os prestadores qualificados de serviços de confiança e para os serviços de confiança qualificados por eles prestados.

A fim de verificar se o prestador de serviços de confiança cumpre os requisitos estabelecidos no artigo 18.º da Diretiva XXXX [SRI 2], a entidade supervisora solicita às autoridades competentes a que se refere a Diretiva XXXX [SRI 2] que realizem ações de supervisão nesse sentido e prestem informações sobre o resultado no prazo de três dias a contar da sua conclusão, sem demora injustificada e, o mais tardar, no prazo de dois meses a contar da receção desse pedido pelas autoridades competentes referidas na Diretiva XXXX [SRI 2]. Se a verificação não ficar concluída no prazo de dois meses a contar da notificação, a autoridade competente a que se refere a Diretiva XXXX [SRI 2] informa a autoridade supervisora, indicando as razões do atraso e o prazo dentro do qual a verificação estará concluída.

Se a entidade supervisora 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) O n.º 4 passa a ter a seguinte redação:

"4. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão define, por meio de atos de execução, os formatos e procedimentos de notificação e verificação para efeitos do disposto nos n.ºs 1 e 2. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

25) O artigo 24.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

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

As informações referidas no primeiro parágrafo são verificadas pelos prestadores qualificados de serviços de confiança, pelos seus próprios meios ou recorrendo a um terceiro, de uma das seguintes formas:

- 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) Por meio de certificados eletrónicos qualificados de atributos, de um certificado de assinatura eletrónica qualificada ou de um selo eletrónico qualificado emitidos nos termos das alíneas a), b), c) ou d);
- c) Utilizando outros métodos de identificação que garantam a identificação da pessoa com um elevado nível de confiança, cuja conformidade será confirmada por um organismo de avaliação da conformidade;
- d) Através da presença física da pessoa singular ou de um representante autorizado da pessoa coletiva mediante procedimentos adequados e em conformidade com a legislação nacional.";

b) É inserido o seguinte n.º 1-A:

"1-A. No prazo de 12 meses após a entrada em vigor do presente Regulamento, a Comissão estabelece, por meio de atos de execução, especificações técnicas mínimas, normas e procedimentos no atinente à verificação da identidade e dos atributos em conformidade com o n.º 1, alínea c). Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

c) O n.º 2 é alterado do seguinte modo:

0) A alínea a) é alterada do seguinte modo:

"a) Informam a entidade supervisora pelo menos um mês antes de implementar qualquer alteração na prestação dos seus serviços de confiança qualificados ou, pelo menos, três meses em caso de intenção de cessar essas atividades. A entidade supervisora pode solicitar informações adicionais ou o resultado de uma avaliação da conformidade antes de conceder a autorização para aplicar as alterações pretendidas aos 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 estará concluída.

1) As alíneas d) e e) passam a ter a seguinte redação:

"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 garantem a segurança técnica e a fiabilidade dos processos por eles suportados, incluindo a utilização de algoritmos criptográficos adequados, comprimentos de chave e funções de dispersão nos sistemas, produtos e nos processos por eles suportados;"

2) São inseridas as seguintes novas alíneas f-A) e f-B):

"f-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 qualificados. Não obstante o disposto no artigo 18.º da Diretiva (UE) XXXX/XXX [SRI 2], essas medidas incluem, no mínimo, o seguinte:

i) medidas relacionadas com os procedimentos de registo e integração num serviço,

ii) medidas relacionadas com controlos processuais ou administrativos,

iii) medidas relacionadas com 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 ou perturbações na prestação do serviço ou na aplicação das medidas referidas no n.º, alínea f-A), subalíneas i), ii) e iii), que tenham um impacto significativo no serviço de confiança prestado ou nos dados pessoais nele conservados, sem demora injustificada e, em qualquer caso, o mais tardar 24 horas após terem tomado conhecimento do incidente.";

3) As alíneas g) e h) passam a ter a seguinte redação:

"g) Tomam as medidas adequadas para prevenir a falsificação, o roubo ou a apropriação indevida dos dados, ou a eliminação, a alteração ou o tornar inacessíveis 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 deixado de prestar esses serviços, 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 eletronicamente;"

4) É suprimida a alínea j);

d) É inserido o seguinte n.º 4-A:

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

e) O n.º 5 passa a ter a seguinte redação:

"5. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas, os procedimentos e os números de referência das normas relativas aos requisitos a que se refere o n.º 2. Sempre que essas especificações técnicas, procedimentos e normas forem cumpridos, beneficiam da presunção de conformidade com os requisitos estabelecidos neste artigo. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

f) É inserido o seguinte n.º 6:

"6. A Comissão fica habilitada a adotar atos de execução que especifiquem as características técnicas das medidas adicionais referidas no n.º 2, alínea f-A).";

25-A) O artigo 26.º é alterado do seguinte modo:

2. No prazo de 12 meses após a entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência para as assinaturas eletrónicas avançadas. Presume-se a conformidade com os requisitos aplicáveis às assinaturas eletrónicas avançadas quando uma assinatura eletrónica avançada satisfaz essas especificações e normas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

25-B) O artigo 27.º é alterado do seguinte modo:

O n.º 4 é suprimido.

26) No artigo 28.º, o n.º 6 passa a ter a seguinte redação:

"6. No prazo de 12 meses após a entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência para os certificados qualificados de assinatura eletrónica. Os certificados qualificados de assinatura eletrónica conformes com as referidas especificações e normas beneficiam da presunção de conformidade com os requisitos estabelecidos no anexo I. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

27) Ao artigo 29.º, é aditado o seguinte n.º 1-A:

"1-A. A geração, a gestão de dados para a criação de uma assinatura eletrónica em nome do signatário ou a duplicação desses dados de criação de assinaturas para efeitos de salvaguarda só podem ser efetuadas 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.";

28) É inserido o seguinte artigo 29.º-A:

"Artigo 29.º-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) Sem prejuízo do ponto 1, alínea d), do anexo II, pode duplicar 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;
 - c) Cumpra todos os requisitos identificados no relatório de certificação do dispositivo qualificado de criação de assinaturas eletrónicas à distância emitido nos termos do artigo 30.º.
2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas para efeitos do disposto no n.º 1.";
- 29) No artigo 30.º, é inserido o seguinte n.º 3-A:

"3-A. A validade da certificação a que se refere o n.º 1 não excede o período de cinco anos, e sujeita a uma avaliação periódica das vulnerabilidades a cada dois anos. Sempre que sejam identificadas vulnerabilidades e as mesmas não sejam sanadas, a certificação é cancelada.";

30) No artigo 31.º, o n.º 3 passa a ter a seguinte redação:

"3. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão define, por meio de atos de execução, os formatos e os procedimentos aplicáveis para efeitos do disposto no n.º 1. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

31) O artigo 32.º é alterado do seguinte modo:

a) Ao n.º 1, é aditado o seguinte parágrafo:

"A validação de assinaturas eletrónicas qualificadas que seja conforme com as normas referidas no n.º 3 beneficia da presunção de conformidade com as especificações e os requisitos estabelecidos no primeiro parágrafo.";

b) O n.º 3 passa a ter a seguinte redação:

"3. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão fornece, por meio de atos de execução, as especificações e os números de referência das normas para a validação de assinaturas eletrónicas qualificadas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

31-A) É inserido o seguinte 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 no certificado qualificado que confirma a validade de um sistema eletrónico avançado na assinatura baseada num certificado qualificado, desde que:

- a) No momento da assinatura, o certificado que lhe serve de suporte seja um certificado qualificado de 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 ser válido no momento da assinatura;
- c) Os dados para a validação da assinatura correspondam aos dados fornecidos à parte utilizadora;
- d) O conjunto único de dados que representam o signatário no certificado sejam corretamente fornecidos à parte utilizadora;
- e) A utilização de um pseudónimo no momento da assinatura seja claramente indicada à parte utilizadora;
- f) A integridade dos dados assinados não tenha sido afetada;
- g) Os requisitos previstos no artigo 26.º se encontrem preenchidos no momento da assinatura. A validação de assinaturas eletrónicas avançadas com base em certificados qualificados que seja conforme com as normas referidas no n.º 3 beneficia da presunção de conformidade com as especificações e os requisitos estabelecidos no primeiro parágrafo.";
2. O sistema utilizado para validar a assinatura eletrónica avançada com base em certificados qualificados fornece à parte utilizadora o resultado correto do processo de validação e permite-lhe detetar eventuais problemas de segurança.
3. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão fornece, por meio de atos de execução, as especificações e os números de referência das normas para a validação de assinaturas eletrónicas avançadas com base em certificados qualificados. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2."

31-B) O artigo 33.º é alterado do seguinte modo:

- "1. Os serviços qualificados de validação de assinaturas eletrónicas qualificadas só podem ser prestados por prestadores qualificados de serviços de confiança que:";
- "2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas relativas ao serviço qualificado de validação a que se refere o n.º 1. O serviço de validação de assinaturas eletrónicas qualificadas que seja conforme com essas especificações e normas beneficia da presunção de conformidade com os requisitos estabelecidos no n.º 1. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2."

32) O artigo 34.º passa a ter a seguinte redação:

"Artigo 34.º

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.
2. As disposições aplicáveis ao serviço qualificado de preservação de assinaturas eletrónicas qualificadas que sejam conformes com as especificações e normas referidas no n.º 3 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.º 1.
3. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas para o serviço qualificado de preservação de assinaturas eletrónicas qualificadas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

32-A) Ao artigo 36.º, é aditado o seguinte n.º 2:

2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, especificações técnicas e números de referência das normas aplicáveis aos selos eletrónicos avançados.

Presume-se a conformidade com os requisitos aplicáveis aos selos eletrónicos avançados quando um selo eletrónico avançado satisfaz essas especificações e normas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

33) O artigo 37.º é alterado do seguinte modo:

O n.º 4 é suprimido.

34) O artigo 38.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

"1. Os certificados qualificados de selos eletrónicos cumprem os requisitos estabelecidos no anexo III. Os certificados qualificados de selos eletrónicos que sejam conformes com as especificações e as normas referidas no n.º 6 beneficiam da presunção de conformidade com os requisitos estabelecidos no anexo III.";

b) O n.º 6 passa a ter a seguinte redação:

"6. No prazo de 12 meses após a entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as seguintes especificações técnicas e os números de referência para os certificados qualificados de selos eletrónicos. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

35) É inserido o seguinte artigo 39.º-A:

"Artigo 39.º-A

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

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

35-A) É inserido o seguinte artigo 40.º-A:

"Artigo 40.º-A

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

(1) O artigo 32.º-A aplica-se, *mutatis mutandis*, à validação dos selos eletrónicos avançados com base em certificados qualificados.";

36) O artigo 42.º é alterado do seguinte modo:

a) É inserido o seguinte novo n.º 1-A:

"1-A. A vinculação da data e da hora aos dados e à fonte horária exata que sejam conformes com as especificações e normas referidas no n.º 2 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.º 1.";

b) O n.º 2 passa a ter a seguinte redação:

"2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas relativas à vinculação da data e da hora aos dados e às fontes horárias precisas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

36-A) No artigo 43.º, é aditado o seguinte n.º 3:

2-A. O serviço qualificado de envio registado eletrónico num Estado-Membro é reconhecido como serviço qualificado de envio registado eletrónico em qualquer outro Estado-Membro.";

37) O artigo 44.º é alterado do seguinte modo:

a) É inserido o seguinte n.º 1-A:

"1-A. O processo de envio e receção de dados que esteja conforme com as especificações e normas referidas no n.º 2 beneficia da presunção de conformidade com os requisitos estabelecidos no n.º 1.";

b) O n.º 2 passa a ter a seguinte redação:

"2. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas para os processos de envio e receção de dados. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

c) São aditados os seguintes n.ºs 3 e 4:

"3. Os prestadores de serviços qualificados de envio registado eletrónico podem acordar na interoperabilidade entre os serviços qualificados de envio registado eletrónico que prestam. Esse quadro de interoperabilidade cumpre os requisitos estabelecidos no n.º 1. O cumprimento é confirmado por um organismo de avaliação da conformidade.";

"4. A Comissão pode, por meio de um ato de execução, estabelecer especificações técnicas e números de referência das normas, a fim de facilitar a transferência de dados entre dois ou mais prestadores qualificados de serviços de confiança. As especificações técnicas e o conteúdo das normas são eficazes em termos de custos e proporcionados. O ato de execução é adotado pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.º;"

38) O artigo 45.º passa a ter a seguinte redação:

"Artigo 45.º

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 dos requisitos estabelecidos no anexo IV é efetuada em conformidade com as especificações e normas referidas no n.º 4.
2. Os certificados qualificados de autenticação de sítios Web a que se refere o n.º 1 devem ser reconhecidos pelos navegadores Web. Para o efeito, os navegadores Web garantem que os dados de identidade fornecidos utilizando qualquer um dos métodos são apresentados de um modo fácil de consultar. Os navegadores Web asseguram a compatibilidade e a interoperabilidade com os certificados qualificados de autenticação de sítios Web a que se refere o n.º 1, esta disposição não se aplica às empresas consideradas microempresas e pequenas empresas em conformidade com a Recomendação 2003/361/CE da Comissão, durante os primeiros cinco anos de atividade como prestadores de serviços de navegação Web.
4. No prazo de 12 meses a contar da entrada em vigor do presente regulamento, a Comissão fornece, por meio de atos de execução, as especificações e os números de referência das normas relativas aos certificados qualificados de autenticação de sítios Web a que se refere os n.ºs 1 e 2. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.º;"

39) Após o artigo 45.º, são inseridas as seguintes secções 9, 10 e 11:

"SECÇÃO 9

CERTIFICADO ELETRÓNICO DE ATRIBUTOS

Artigo 45.º-A

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 se apresentar em formato eletrónico 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 ou em nome de um organismo do setor público responsável por uma fonte autêntica têm o mesmo efeito jurídico que os certificados legalmente emitidos em papel.
3. O certificado eletrónico qualificado de atributos emitido num Estado-Membro é reconhecido como certificado eletrónico qualificado de atributos em qualquer outro Estado-Membro.
4. Os certificados de atributos emitidos por ou em nome de um organismo do setor público responsável por uma fonte autêntica 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-B

Certificado eletrónico de atributos em serviços públicos

Quando a legislação 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, os certificados eletrónicos qualificados de atributos de outros Estados-Membros também são aceites.

Artigo 45.º-C

Requisitos aplicáveis aos certificados eletrónicos qualificados de atributos

1. O certificado eletrónico qualificado de atributos satisfaz os requisitos estabelecidos no anexo V.
 - 1-A. A avaliação do cumprimento dos requisitos estabelecidos no anexo V é efetuada em conformidade com as especificações e normas referidas no n.º 4.
2. Os certificados eletrónicos qualificados de atributos não podem estar sujeitos a requisitos obrigatórios para além dos requisitos estabelecidos no anexo V.
3. 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 nenhuma circunstância.
4. No prazo de seis meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece as especificações técnicas e os números de referência das normas relativas aos certificados eletrónicos qualificados de atributos, mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital a que se refere o artigo 6.º-A, n.º 11.

Artigo 45.º-D

Verificação de atributos por confronto com fontes autênticas

1. Os Estados-Membros asseguram, no prazo de 24 meses após a entrada em vigor dos atos de execução referidos no artigo 6.º-A, n.º 11, e no artigo 6.º-C, n.º 4, 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 permitam aos prestadores qualificados de certificados eletrónicos de atributos verificar a autenticidade desses atributos com recurso a meios eletrónicos, mediante pedido do utilizador e em conformidade com a legislação nacional ou da União.
2. No prazo de seis meses a contar da entrada em vigor do presente regulamento, tendo em conta as normas internacionais aplicáveis, a Comissão estabelece as especificações técnicas mínimas, as normas e os procedimentos no que respeita ao catálogo de atributos, aos sistemas de certificação de atributos e aos procedimentos de verificação referentes aos certificados eletrónicos qualificados de atributos mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital a que se refere o artigo 6.º-A, n.º 11.

Artigo 45.º-DA

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 cumpre os seguintes requisitos:
 - a) Os requisitos estabelecidos no anexo VII;

b) O certificado qualificado de suporte da assinatura eletrónica qualificada ou do selo eletrónico qualificado do organismo do setor público a que se refere o artigo 3.º, n.º 45-A, 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 automatizado que:

- i) indica que o organismo emissor está estabelecido, em conformidade com o direito nacional ou da União, 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 a legislação nacional ou da União referida na subalínea i).

2. O Estado-Membro em que estão estabelecidos os organismos do setor público a que se refere o artigo 3.º, n.º 45-A, assegura que os organismos do setor público que emitem certificados eletrónicos de atributos têm um nível de fiabilidade equivalente ao dos prestadores qualificados de serviços de confiança nos termos do artigo 24.º.

2-A. Os Estados-Membros notificam à Comissão os organismos do setor público referidos no artigo 3.º, n.º 45-A. Essa notificação inclui um relatório de avaliação da conformidade emitido por um organismo de avaliação da conformidade que confirme 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, n.º 45-A, num formato eletronicamente assinado ou selado, adequado ao tratamento automático.

3. 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. Após a revogação, o estatuto revogado de um certificado eletrónico não é revertido.

4. Um certificado eletrónico de atributos emitido por ou em nome de um organismo do setor público responsável por uma fonte autêntica é considerado conforme com os requisitos estabelecidos no n.º 1 do presente artigo se cumprir as normas referidas no n.º 5.

5. No prazo de seis meses a contar da entrada em vigor do presente regulamento, a Comissão estabelece as especificações técnicas e os números de referência das normas relativas ao certificado eletrónico de atributos emitido por ou em nome de um organismo do setor público responsável por uma fonte autêntica, mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital a que se refere o artigo 6.º-A, n.º 11.

5-A. No prazo de seis meses após a entrada em vigor do presente regulamento, a Comissão define formatos, procedimentos especificações e normas para efeitos do n.º 2-A mediante um ato de execução relativo à implementação das carteiras europeias de identidade digital conforme referido no artigo 6.º-A, n.º 11.

6. Os organismos do setor público referidos no artigo 3.º, n.º 45-A que emitem o certificado eletrónico qualificado de atributos facultam uma interface com as carteiras europeias de identidade digital fornecidas nos termos do artigo 6.º-A.

Artigo 45.º-E

Emissão de certificados eletrónico de atributos para as carteiras europeias de identidade digital

Os fornecedores de certificados eletrónicos qualificados de atributos facultam uma interface com as carteiras europeias de identidade digital fornecidas nos termos do artigo 6.º-A.

Artigo 45.º-F

Regras adicionais para a prestação de serviços de certificados eletrónicos de atributos

1. Os prestadores de serviços de certificados eletrónicos qualificados e não qualificados de atributos não combinam dados pessoais relacionados com a prestação desses serviços com dados pessoais de quaisquer outros serviços que prestem ou 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 prestador qualificado de certificados eletrónicos de atributos.
4. Os prestadores de serviços de certificados eletrónicos qualificados de atributos implementam uma separação funcional para a prestação desses serviços.

SECÇÃO 10

SERVIÇOS DE ARQUIVO ELETRÓNICO

Artigo 45.º-G

Efeito legal de um serviço de arquivo eletrónico

1. Não podem ser negados efeitos jurídicos nem admissibilidade como prova em processos judiciais aos dados eletrónicos armazenados através de um serviço de arquivo eletrónico pelo simples facto de se encontrarem em formato eletrónico ou de não serem armazenados através de um serviço qualificado de arquivo eletrónico.
2. Os dados eletrónicos armazenados 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.
3. O serviço qualificado de arquivo eletrónico num Estado-Membro é reconhecido como serviço qualificado de arquivo eletrónico em qualquer outro Estado-Membro.

Artigo 45.º-GA

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 prolongar a durabilidade e a legibilidade dos dados eletrónicos para além do período de validade tecnológica e, pelo menos, ao longo do período de conservação legal ou contratual, mantendo simultaneamente a sua integridade e origem;

- c) Asseguram que os dados eletrónicos são conservados de modo a serem protegidos contra a perda e a alteração, exceto no que diz respeito ao seu suporte ou formato eletrónico;
- d) Permitem que as partes utilizadoras autorizadas recebam um relatório automatizado que confirme que um dado eletrónico extraído de um arquivo eletrónico qualificado goza da presunção de integridade dos dados desde o início do período de conservação até ao momento da sua recuperação. Esse relatório 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. No prazo de 12 meses após a entrada em vigor do presente regulamento, a Comissão estabelece, por meio de atos de execução, as seguintes especificações técnicas e os números de referência para os serviços qualificados de arquivo eletrónico. Presume-se a conformidade com os requisitos aplicáveis aos serviços de arquivo eletrónico qualificados quando um serviço qualificado de arquivo eletrónico cumpre essas especificações e normas. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.

SECÇÃO 11

LIVROS-RAZÃO ELETRÓNICOS

Artigo 45.º-H

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 se apresentar em formato eletrónico ou de não cumprir os requisitos dos livros-razão eletrónicos qualificados.
2. Os registos de dados contidos num livro-razão eletrónico qualificado gozam da presunção da sua ordem cronológica única e exata e da sua integridade.
3. Um livro-razão eletrónico qualificado num Estado-Membro é reconhecido como livro-razão eletrónico qualificado em qualquer outro Estado-Membro.

Artigo 45.º-I

Requisitos aplicáveis aos livros-razão eletrónicos qualificados

1. Os livros-razão eletrónicos qualificados cumprem os seguintes requisitos:
 - a) São criados por um ou mais prestadores qualificados de serviços de confiança;
 - b) Estabelecem a origem dos registos de dados no registo;
 - 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 sejam conformes com as especificações e as normas referidas no n.º 3 beneficiam da presunção de conformidade com os requisitos estabelecidos no n.º 1.
3. A Comissão estabelece, por meio de atos de execução, as especificações técnicas e os números de referência das normas para a operação de um livro-razão eletrónico qualificado. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 48.º, n.º 2.";

40) É inserido o seguinte artigo 48.º-A:

"Artigo 48.º-A

Requisitos de prestação de informações

1. Uma vez fornecidas no seu território, os Estados-Membros asseguram a recolha de estatísticas relativas ao funcionamento das carteiras europeias de identidade digital.
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) Um relatório de síntese, incluindo dados sobre incidentes que impedem a utilização da carteira europeia de identidade digital;
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 disposto no n.º 2.";

41) O artigo 49.º passa a ter a seguinte redação:

"Artigo 49.º

Revisão

1. A Comissão analisa a aplicação do presente regulamento e apresenta um relatório ao Parlamento Europeu e ao Conselho no prazo de 36 meses após a sua entrada em vigor. A Comissão avalia nomeadamente o âmbito de aplicação dos artigos 6.º e 6.º-DB e se é adequado modificar o âmbito do presente regulamento ou as suas disposições especiais, tendo em conta a experiência adquirida na aplicação do presente regulamento, bem como a procura do consumidor, a evolução da tecnologia, do mercado e da legislação. Se necessário, o relatório é acompanhado de uma proposta de alteração do presente regulamento.
2. O relatório de avaliação inclui uma avaliação da disponibilidade e usabilidade das carteiras europeias de identidade digital previstas no âmbito do presente regulamento e afere se todos os prestadores privados de serviços em linha que dependem de serviços de identificação eletrónica de terceiros para a autenticação de utilizadores devem ser obrigados a aceitar a utilização das carteiras europeias de identidade digital.
3. Além disso, a intervalos de quatro anos a contar do relatório a que se refere o primeiro parágrafo, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a realização dos objetivos do presente regulamento.";

42) O artigo 51.º passa a ter a seguinte redação:

"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 36 meses após a entrada em vigor do presente regulamento.
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 24 meses após a entrada em vigor do presente regulamento."
- 2-A. 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 de criação de assinaturas eletrónicas e selos eletrónicos à distância em conformidade com os artigos 29.º-A e 39.º-A continua a ser considerada como não tendo a necessidade de obter o estatuto de qualificado para a prestação desses serviços de gestão até 24 meses após a entrada em vigor do presente regulamento.
- 2-B. Os prestadores qualificados de serviços de confiança aos quais tenha sido concedido o estatuto de qualificado ao abrigo do presente regulamento antes de [data de entrada em vigor do regulamento modificativo], utilizando métodos de verificação da identidade para a emissão de certificados qualificados em conformidade com o artigo 24.º, n.º 1, apresentam à entidade supervisora um relatório de avaliação da conformidade que comprove a conformidade com o artigo 24.º, n.º 1, o mais rapidamente possível e, o mais tardar, 30 meses após a entrada em vigor do regulamento modificativo. Até à apresentação desse relatório de avaliação da conformidade e à conclusão da sua avaliação pela entidade supervisora, o prestador qualificado de serviços de confiança pode continuar a recorrer aos métodos de verificação da identidade previstos no artigo 24.º, n.º 1, do Regulamento (UE) n.º 910/2014.

- 43) O anexo I é alterado em conformidade com o anexo I do presente regulamento;
- 44) O anexo II é substituído pelo texto constante do anexo II do presente regulamento;
- 45) O anexo III é alterado em conformidade com o anexo III do presente regulamento;
- 46) O anexo IV é alterado em conformidade com o anexo IV do presente regulamento;
- 47) É aditado um novo anexo V, cujo texto consta do anexo V do presente regulamento;
- 48) É aditado um novo anexo VI ao presente regulamento.

Artigo 52.º

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

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

Feito em Bruxelas, em

Pelo Parlamento Europeu

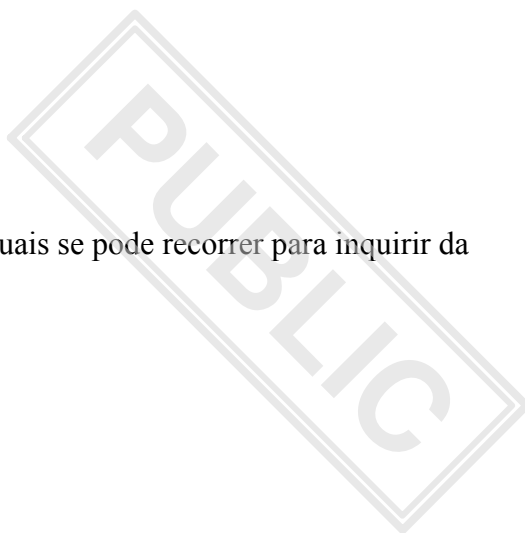
Pelo Conselho

A Presidente O Presidente

ANEXO I

No anexo I, a alínea i) passa a ter a seguinte redação:

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



ANEXO II

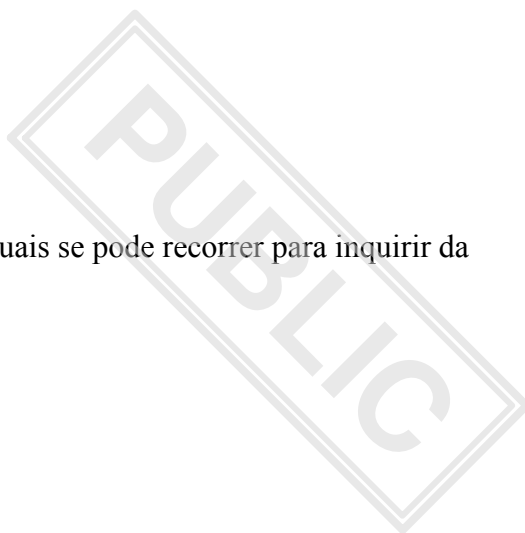
REQUISITOS APLICÁVEIS AOS DISPOSITIVOS QUALIFICADOS DE CRIAÇÃO DE ASSINATURAS ELETRÓNICAS

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.

ANEXO III

No anexo III, a alínea i) passa a ter a seguinte redação:

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



ANEXO IV

No anexo IV, a alínea j) passa a ter a seguinte redação:

- "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.".

ANEXO V

REQUISITOS APLICÁVEIS AOS CERTIFICADOS ELETRÓNICOS QUALIFICADOS DE ATRIBUTOS

Os certificados eletrónicos qualificados de atributos contêm:

- (e) Uma indicação, pelo menos num formato adequado ao tratamento automático, de que o certificado foi emitido como certificado eletrónico qualificado de atributos;
- (f) 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:
 - para as pessoas coletivas: a designação e, eventualmente, o número de registo conforme constam dos registos oficiais,
 - para as pessoas singulares: o nome da pessoa;
- (g) Um conjunto de dados que representem inequivocamente a entidade a que os atributos certificados se referem; a utilização de um pseudónimo é claramente indicada;
- (h) O ou os atributos certificados, incluindo, se for caso disso, as informações necessárias para identificar o âmbito desses atributos;
- (i) A indicação do início e do termo da validade do certificado;

- (j) 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;
- (k) A assinatura eletrónica qualificada ou o selo eletrónico qualificado do prestador qualificado de serviços de confiança emitente;
- (l) 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);
- (m) A informação ou a localização dos serviços aos quais se pode recorrer para inquirir da validade do certificado qualificado.

ANEXO VI

LISTA MÍNIMA DE ATRIBUTOS

Em conformidade com o artigo 45.º-D, os Estados-Membros asseguram que sejam tomadas medidas que permitam aos prestadores qualificados de certificados eletrónicos de atributos verificar por via eletrónica, a pedido do utilizador, 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 a legislação nacional ou da União, e nos casos em que esses atributos se baseiem em fontes autênticas do setor público:

1. Endereço;
2. Idade;
3. Sexo;
4. Estado civil;
5. Composição do agregado familiar;
6. Nacionalidade ou cidadania;
7. Habilitações literárias, títulos e licenças;
8. Qualificações profissionais, títulos e licenças;
9. Autorizações e licenças públicas;
10. Dados financeiros e das empresas.

ANEXO VII

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

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

- a) Uma indicação, pelo menos numa forma adequada ao tratamento automatizado, de que o certificado foi emitido sob a forma de certificado eletrónico de atributos, emitido por ou em nome de um organismo público responsável por uma fonte autêntica;
- 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; a utilização de um pseudónimo é claramente indicada;
- 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 organismo público emissor e, se aplicável, a 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 emissor;
- 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.