COMISSÃO EUROPEIA

Bruxelas, 4.6.2012
COM(2012) 238 final

2012/0146 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno

(Texto relevante para efeitos do EEE)

{SWD(2012) 135 final}
{SWD(2012) 136 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

O presente memorando explica uma proposta de quadro legal destinado a reforçar a confiança nas transações eletrónicas no mercado interno.

Criar confiança no ambiente em linha é fundamental para o desenvolvimento económico. A falta de confiança leva os consumidores, as empresas e as administrações a hesitarem em realizar transações por via eletrónica e em adotar novos serviços.

A *Agenda Digital para a Europa*[1] identifica os obstáculos existentes ao desenvolvimento digital da Europa e propõe legislação sobre assinaturas eletrónicas (Ação-chave 3) e sobre o reconhecimento mútuo da identificação e da autenticação eletrónicas (Ação-chave 16), tendo em vista o estabelecimento de um quadro legal claro que acabe com a fragmentação e a falta de interoperabilidade, melhore a cidadania digital e previna a cibercriminalidade. A adoção de legislação que garanta o reconhecimento mútuo da identificação e da autenticação eletrónicas em toda a UE e a revisão da Diretiva relativa às assinaturas eletrónicas constituem igualmente ações fundamentais do *Ato do Mercado Único*[2], para a realização do mercado único digital. O *Roteiro para a Estabilidade e o Crescimento*[3] sublinha o papel fundamental que o futuro quadro legal comum relativo ao reconhecimento e à aceitação mútuos da identificação e da autenticação eletrónicas através das fronteiras terá no desenvolvimento da economia digital.

O quadro legal proposto, que consiste num «*Regulamento do Parlamento Europeu e do Conselho relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno*», visa possibilitar as interações eletrónicas seguras e sem descontinuidades entre as empresas, os cidadãos e as autoridades públicas, aumentando assim a eficácia dos serviços em linha públicos e privados, dos negócios eletrónicos e do comércio eletrónico na UE.

A legislação da UE em vigor sobre a matéria, nomeadamente a Diretiva 1999/93/CE relativa a *um quadro comunitário para as assinaturas eletrónicas*[4], contempla essencialmente as assinaturas eletrónicas. A UE não dispõe de qualquer quadro geral transnacional e transetorial para transações eletrónicas seguras, fiáveis e simples que englobe a identificação, a autenticação e as assinaturas eletrónicas.

O objetivo é melhorar a legislação existente e torná-la extensível ao reconhecimento e à aceitação mútuos, a nível da UE, dos sistemas de identificação eletrónica notificados e de outros serviços de confiança eletrónicos conexos essenciais.

2. RESULTADOS DAS CONSULTAS ÀS PARTES INTERESSADAS E AVALIAÇÕES DE IMPACTO

Esta iniciativa é o resultado de extensas consultas sobre a revisão do atual quadro legal das assinaturas eletrónicas durante as quais a Comissão recolheu os pontos de vista dos Estados-

1 COM(2010) 245 de 19.5.2010.
2 COM (2011) 206 final de 13.4.2011.
3 COM(2011) 669 de 12.10.2011.
4 JO L 13 de 19.1.2000, p. 12.

Membros, do Parlamento Europeu e de outras partes interessadas[5]. Uma consulta pública em linha foi complementada por um «Painel de consulta das PME» para identificar os pontos de vista e as necessidades específicos das pequenas e médias empresas e por outras consultas com objetivos específicos a certas partes interessadas[6][7]. A Comissão encomendou igualmente alguns estudos sobre a identificação, a autenticação e a assinatura eletrónicas e os serviços de confiança conexos (sigla inglesa «*eIAS*») .

As consultas mostraram claramente que a grande maioria das partes interessadas reconhece a necessidade de rever o atual quadro para corrigir as lacunas deixadas pela diretiva relativa às assinaturas eletrónicas. Entenderam os consultados que essa seria a melhor maneira de responder aos desafios colocados pelo rápido desenvolvimento de novas tecnologias (em particular as que permitem o acesso em linha e móvel) e pela crescente globalização, embora mantendo a neutralidade tecnológica do quadro legal.

Em conformidade com a sua política que tem como lema «Legislar melhor», a Comissão procedeu à avaliação do impacto das diferentes alternativas de ação. Foram avaliados três conjuntos de opções, referentes respetivamente a: 1) o âmbito do novo quadro, 2) o instrumento jurídico e 3) o nível de supervisão necessário[8]. A opção preferida provou ser a que se propunha reforçar a segurança jurídica, promover a coordenação da supervisão nacional, assegurar o reconhecimento e a aceitação mútuos dos sistemas de identificação eletrónica e incorporar os serviços de confiança conexos essenciais. A avaliação de impacto concluiu que esta opção permitiria melhorar consideravelmente a segurança jurídica, a proteção e a confiança das transações eletrónicas entre os Estados-Membros, resultando numa menor fragmentação do mercado.

3. ELEMENTOS JURÍDICOS DA PROPOSTA

3.1 Base legal

A proposta baseia-se no artigo 114.º do TFUE, que diz respeito à adoção de regras para eliminar os obstáculos existentes ao funcionamento do mercado interno. Os cidadãos, as empresas e as administrações poderão beneficiar do reconhecimento e da aceitação mútuos da identificação, da autenticação e das assinaturas eletrónicas e de outros serviços de confiança através das fronteiras, quando necessário para aceder a - e concluir - procedimentos ou transações eletrónicos.

---

5 Para pormenores sobre as consultas, ver http://ec.europa.eu/information_society/policy/esignature/eu_legislation/revision.

6 Em 10 de março de 2011, realizou-se uma *workshop* de partes interessadas na qual estiveram presentes representantes dos setores público e privado e do mundo académico para discutir quais as medidas legislativas necessárias para responder aos futuros desafios. Tratou-se de um fórum interativo para trocar pontos vista e marcar as diferentes posições sobre as questões suscitadas na consulta pública. Várias organizações enviaram espontaneamente documentos de posição.

7 Em particular, a presidência polaca da UE organizou em Varsóvia, em 9 de novembro de 2011, uma reunião com os Estados-Membros sobre assinatura eletrónica e outra em Poznan, em 17 do mesmo mês, sobre identificação eletrónica. Em 25 de janeiro de 2012, a Comissão convocou os Estados-Membros para uma *workshop* onde se discutiram as restantes questões associadas à identificação, autenticação e assinatura eletrónicas.

8 No primeiro conjunto, foram examinadas quatro opções: revogar a Diretiva relativa às assinaturas eletrónicas; nenhuma mudança; reforçar a segurança jurídica, impulsionar a coordenação da supervisão nacional e assegurar o reconhecimento e a aceitação mútuos da identificação eletrónica em toda a UE e, quarta, a extensão do âmbito a certos serviços de confiança conexos. O segundo conjunto consistiu em avaliar os méritos relativos de uma possível regulamentação através de um ou dois instrumentos e através de uma diretiva *versus* um regulamento. O terceiro conjunto examinou as possibilidades oferecidas pela aplicação de regimes de supervisão nacionais baseados em requisitos de supervisão comuns essenciais por oposição a um sistema de supervisão da UE. Cada opção política foi avaliada, com a ajuda de um grupo constituído por todas as direções-gerais da Comissão interessadas, em termos de eficácia na consecução dos objetivos políticos, impacto económico nas partes interessadas (nomeadamente no orçamento das instituições da UE), impacto social e ambiental e correspondente ónus administrativo.

Um regulamento é considerado o instrumento jurídico mais adequado. Devido à sua aplicabilidade direta, em conformidade com o artigo 288.º do TFUE, um regulamento, ao instaurar um conjunto harmonizado de regras essenciais que contribuem para o funcionamento do mercado interno, reduzirá a fragmentação do quadro legal e fornecerá maior segurança jurídica.

3.2 Subsidiariedade e proporcionalidade

Para que uma ação da UE se justifique, deve ser respeitado o princípio da subsidiariedade:

a) Dimensão transnacional do problema (critério da necessidade)

A natureza transnacional dos *eIAS* exige uma ação a nível da UE. Uma ação a nível nacional por si só não seria suficiente para atingir os objetivos e metas fixados na *estratégia Europa 2020*[9]. Pelo contrário, a experiência mostra que as medidas nacionais criaram de facto barreiras à interoperabilidade das assinaturas eletrónicas ao nível da UE e produzem atualmente o mesmo efeito na identificação e na autenticação eletrónicas e nos serviços de confiança conexos. Torna-se, assim, necessário que a UE crie um quadro que facilite a interoperabilidade transfronteiras e melhore a coordenação dos sistemas nacionais de supervisão. No entanto, a identificação eletrónica não pode ser abordada no regulamento proposto da mesma forma genérica que os outros serviços eletrónicos de confiança, dado que a produção de meios de identificação é uma prerrogativa nacional. A proposta centra-se, pois, estritamente nos aspetos transfronteiras da identificação eletrónica.

O regulamento proposto cria condições de igualdade para as empresas que prestam serviços de confiança, ao passo que as diferenças existentes atualmente nas legislações nacionais criam muitas vezes incerteza jurídica e ónus adicionais. A segurança jurídica é significativamente reforçada através da obrigação clara, para os Estados-Membros, de aceitarem os serviços de confiança qualificados, o que criará mais incentivos para que as empresas estendam a suas atividades a outros países. Por exemplo, uma empresa poderá participar por via eletrónica num concurso público lançado pela administração de outro Estado-Membro sem que a sua assinatura eletrónica fique bloqueada devido a requisitos nacionais específicos e problemas de interoperabilidade. Assim também, uma empresa terá a possibilidade de assinar contratos por via eletrónica com uma congénere estabelecida noutro Estado-Membro sem recear a imposição de requisitos legais diferentes para os serviços confiança como os selos eletrónicos, os documentos eletrónicos ou o carimbo eletrónico da hora. Um outro caso: um aviso de incumprimento será enviado de um Estado-Membro para outro com a certeza de que é legalmente válido em ambos os Estados-Membros. Por último, o comércio em linha será mais fiável quando os compradores tiverem meios para verificar que estão realmente a aceder ao sítio Web do comerciante da sua escolha em vez de um sítio Web eventualmente falso.

A existência de meios de identificação eletrónica mutuamente reconhecidos e assinaturas eletrónicas generalizadamente aceites facilitará a oferta transfronteiras de numerosos serviços no mercado interno e permitirá que as empresas desenvolvam as suas atividades fora de portas sem encontrarem obstáculos nas interações com as autoridades públicas. Na prática, estaremos perante melhorias significativas de eficiência tanto para as empresas como para os cidadãos no cumprimento de formalidades administrativas. Por exemplo, um estudante terá a possibilidade de se inscrever por via eletrónica numa universidade estrangeira, um cidadão de apresentar a sua declaração fiscal em linha a outros Estados-Membros ou um doente de aceder

[9] Comunicação da Comissão: Europa 2020 – estratégia para um crescimento inteligente, sustentável e inclusivo – COM(2010) 2020 de 3.3.2010.

aos seus dados de saúde em linha. Na inexistência de tais meios de identificação eletrónica mutuamente reconhecidos, um médico não poderá aceder aos dados de um doente para poder tratá-lo e os exames médicos e laboratoriais a que o paciente já foi submetido terão de ser repetidos.

b) Valor acrescentado (critério da eficácia)

A coordenação voluntária entre os Estados-Membros não está a permitir atingir os objetivos acima expostos, nem é muito provável que tal aconteça no futuro. Daí resulta uma duplicação de esforços, o estabelecimento de normas diferentes, características transfronteiras diferentes dos produtos gerados pelas TIC e complexidade administrativa no estabelecimento de tal coordenação por via de acordos bilaterais e multilaterais.

Além disso, a necessidade de ultrapassar problemas como a) a falta de segurança jurídica, devido à heterogeneidade das disposições nacionais decorrente de interpretações divergentes da Diretiva relativa às assinaturas eletrónicas e b) a falta de interoperabilidade dos sistemas de assinatura eletrónica instituídos a nível nacional, devido à aplicação não uniforme das normas técnicas, exige um tipo de coordenação entre os Estados-Membros que pode ser mais eficazmente assegurado ao nível da UE.

3.3 Explicação pormenorizada da proposta

3.3.1 CAPÍTULO I – DISPOSIÇÕES GERAIS

O artigo 1.º define o objeto do regulamento.

O artigo 2.º define o âmbito de aplicação material do regulamento.

O artigo 3.º contém as definições dos termos utilizados no regulamento. Algumas definições são retiradas da Diretiva 1999/93/CE, outras são clarificadas, complementadas com elementos adicionais ou totalmente novas.

O artigo 4.º define os princípios do mercado interno no que respeita à aplicação territorial do regulamento. É mencionada expressamente a não imposição de restrições à liberdade de prestação de serviços e à livre circulação de produtos.

3.3.2 CAPÍTULO II – IDENTIFICAÇÃO ELETRÓNICA

O artigo 5.º prevê o reconhecimento e a aceitação mútuos dos meios de identificação eletrónica que se enquadrem num sistema notificado à Comissão nas condições estabelecidas no regulamento. A maior parte dos Estados-Membros adotou algum tipo de sistema de identificação eletrónica. No entanto, os diversos sistemas diferem em muitos aspetos. A inexistência de uma base legal comum que exija a cada Estado-Membro que reconheça e aceite os meios de identificação eletrónica produzidos noutros Estados-Membros para aceder aos serviços em linha, a par da interoperabilidade transfronteiras inadequada dos sistemas de identificação eletrónica nacionais, cria barreiras que impedem os cidadãos e as empresas de beneficiar plenamente do mercado único digital. O reconhecimento e a aceitação mútuos de qualquer meio de identificação eletrónica que se enquadre num sistema notificado nos termos do presente regulamento elimina essas barreiras legais.

O regulamento não obriga os Estados-Membros a adotarem ou a notificarem os sistemas de identificação eletrónica, mas sim a reconhecerem e aceitarem as identificações eletrónicas

notificadas para os serviços em linha cujo acesso a nível nacional exige uma identificação eletrónica. O potencial aumento das economias de escala criadas com a utilização transfronteiras dos meios de identificação eletrónica e sistemas de autenticação notificados pode estimular os Estados-Membros a notificarem os seus próprios sistemas de identificação eletrónica. O artigo 6.º estabelece as cinco condições para a notificação dos sistemas de identificação eletrónica:

Os Estados-Membros podem notificar os sistemas de identificação eletrónica que aceitam sob a sua jurisdição nos casos em que é exigida uma identificação eletrónica para aceder a serviços públicos. Outra condição é que o respetivo meio de identificação eletrónica seja produzido pelo Estado-Membro que notifica o sistema, por alguém em seu nome ou pelo menos sob a sua responsabilidade.

Os Estados-Membros devem garantir uma ligação inequívoca entre os dados da identificação eletrónica e a pessoa em causa. Esta obrigação não significa que uma pessoa não possa ter vários meios de identificação eletrónica, mas que todos eles devem estar associados à mesma pessoa.

A fiabilidade de uma identificação eletrónica depende da disponibilidade de meios de autenticação (ou seja, da possibilidade de verificar a validade dos dados da identificação eletrónica). O regulamento obriga os Estados-Membros notificantes a fornecerem a autenticação em linha gratuitamente a terceiros. A possibilidade de autenticação deve estar disponível sem interrupções. Não podem ser impostos requisitos técnicos específicos, nomeadamente em matéria de *hardware* ou *software*, às partes que recorram à autenticação. Esta disposição não se aplica aos requisitos impostos aos utilizadores (detentores) do meio de identificação eletrónica que sejam tecnicamente necessários para a utilização desse meio, como, por exemplo, um leitor de cartões.

Os Estados-Membros devem aceitar a responsabilidade pelo caráter inequívoco da ligação (ou seja, que os dados de identificação associados a uma pessoa não estejam associados a qualquer outra) e pela possibilidade de autenticação (ou seja, a possibilidade de verificar a validade dos dados da identificação eletrónica). A responsabilidade dos Estados-Membros não cobre nenhum outro aspeto do processo de identificação nem nenhuma transação que exija uma identificação.

O artigo 7.º contém regras para a notificação dos sistemas de identificação eletrónica à Comissão.

O artigo 8.º visa garantir a interoperabilidade técnica dos sistemas de identificação notificados, através de uma abordagem de coordenação, que prevê a adoção de atos delegados.

3.3.3 CAPÍTULO III – SERVIÇOS DE CONFIANÇA

3.3.3.1 Secção 1 – Disposições gerais

O artigo 9.º estabelece os princípios relativos à responsabilidade dos prestadores de serviços de confiança qualificados e não qualificados. Tendo por base o artigo 6.º da Diretiva 1999/93/CE, o artigo estende o direito a indemnização por danos aos danos causados por um prestador de serviços de confiança negligente que não tenha respeitado as boas práticas em matéria de segurança, de que resulte uma violação da segurança com impacto significativo no serviço.

O artigo 10.º descreve o mecanismo de reconhecimento e aceitação dos serviços de confiança qualificados fornecidos por um prestador estabelecido num país terceiro. A sua base é o artigo 7.º da Diretiva 1999/93/CE, mas apenas retém a única opção exequível na prática, que consiste em permitir o reconhecimento em virtude de um acordo internacional entre a União Europeia e países terceiros ou organizações internacionais.

O artigo 11.º estabelece os princípios da proteção e da limitação dos dados utilizados. A sua base é o artigo 8.º da Diretiva 1999/93/CE.

O artigo 12.º torna os serviços de confiança acessíveis às pessoas deficientes.

3.3.3.2 Secção 2 – Supervisão

O artigo 13.º obriga os Estados-Membros a instituírem entidades supervisoras, com base no artigo 3.º, n.º 3, da Diretiva 1999/93/CE, clarificando e alargando o seu mandato no que respeita aos prestadores de serviços de confiança e aos prestadores de serviços de confiança qualificados.

O artigo 14.º introduz um mecanismo específico de assistência mútua entre as entidades supervisoras dos Estados-Membros a fim de facilitar o controlo transfronteiras dos prestadores de serviços de confiança. Introduz regras para as operações conjuntas e consagra o direito das entidades supervisoras a participarem nessas operações.

O artigo 15.º instaura a obrigatoriedade, para os prestadores de serviços de confiança qualificados e não qualificados, da aplicação das medidas técnicas e organizacionais adequadas para garantirem a segurança das suas atividades. Além disso, as entidades supervisoras competentes e outras autoridades pertinentes devem ser informadas de todas as violações da segurança que ocorram. Se for caso disso, essas entidades informarão por sua vez as suas congéneres dos outros Estados-Membros e, diretamente ou através do prestador de serviços de confiança em causa, o público.

O artigo 16.º estabelece as condições para a supervisão dos prestadores de serviços de confiança qualificados e dos serviços de confiança qualificados por eles prestados. Obriga os prestadores de serviços de confiança qualificados a submeterem-se uma vez por ano a uma auditoria efetuada por um organismo independente reconhecido, para confirmar à entidade supervisora que cumprem as obrigações estabelecidas no regulamento. Além disso, o artigo 16.º, n.º 2, concede à entidade supervisora o direito de efetuar auditorias no local e em qualquer altura aos prestadores de serviços de confiança qualificados. É também atribuído à entidade supervisora o poder de emitir instruções vinculativas para os prestadores de serviços de confiança qualificados para que corrijam, de um modo proporcionado, qualquer eventual incumprimento de uma obrigação revelado por uma auditoria da segurança.

O artigo 17.º diz respeito à atividade desenvolvida pela entidade supervisora a pedido de um prestador de serviços de confiança que deseje começar a prestar um serviço de confiança qualificado.

O artigo 18.º prevê o estabelecimento de listas de confiança[10] contendo informações sobre os prestadores de serviços de confiança qualificados que estão sujeitos a supervisão e sobre os serviços que oferecem. Estas informações devem ser tornadas públicas através de um modelo

[10] A lista de confiança (ou «lista aprovada», nos termos da decisão) estabelecida pela Decisão 2009/767/CE da Comissão, com a redação que lhe foi dada pela Decisão 2010/425/UE da Comissão, será a base de uma nova decisão da Comissão relativa às listas de confiança previstas pelo presente regulamento.

comum, a fim de facilitar a sua utilização automática e garantir um nível adequado de pormenor.

O artigo 19.º estabelece os requisitos a cumprir pelos prestadores de serviços de confiança qualificados para serem reconhecidos como tal. A sua base é o anexo II da Diretiva 1999/93/CE.

3.3.3.3 Secção 3 – Assinatura eletrónica

O artigo 20.º consagra as regras relativas ao efeito legal das assinaturas eletrónicas das pessoas singulares. Clarifica e desenvolve o artigo 5.º da Diretiva 1999/93/CE instaurando a obrigação expressa de conferir às assinaturas eletrónicas qualificadas o mesmo efeito legal que as assinaturas manuscritas. Além disso, os Estados-Membros devem garantir a aceitação transfronteiras das assinaturas eletrónicas qualificadas, no contexto da oferta de serviços públicos, e não devem introduzir quaisquer requisitos adicionais que possam criar obstáculos à utilização dessas assinaturas.

O artigo 21.º estabelece os requisitos para os certificados de assinatura qualificados. Clarifica o anexo I da Diretiva 1999/93/CE e elimina as disposições que não funcionaram na prática (por exemplo, os limites ao valor das transações).

O artigo 22.º estabelece os requisitos para os dispositivos de criação de assinaturas eletrónicas qualificados. Clarifica os requisitos para os dispositivos seguros de criação de assinaturas, definidos no artigo 3.º, n.º 5, da Diretiva 1999/93/CE, que, por força do presente regulamento, têm agora de ser considerados dispositivos de criação de assinaturas qualificados. Torna também claro que o âmbito de um dispositivo de criação de assinaturas pode ser muito mais vasto do que apenas algo que contém dados para a criação de uma assinatura. A Comissão pode também estabelecer uma lista com os números de referência das normas dos requisitos de segurança para os dispositivos.

O artigo 23.º, que se baseia no artigo 3.º, n.º 4, da Diretiva 1999/93/CE, introduz o conceito de certificação dos dispositivos de criação de assinatura eletrónica qualificados para determinar a sua conformidade com os requisitos de segurança estabelecidos no anexo II. Estes dispositivos devem ser reconhecidos por todos os Estados-Membros como conformes com os requisitos sempre que um procedimento de certificação seja realizado por um organismo de certificação designado por um Estado-Membro. A Comissão publicará uma lista positiva desses dispositivos certificados, em conformidade com o artigo 24.º. A Comissão pode igualmente estabelecer uma lista com os números de referência das normas para a avaliação da segurança dos produtos informáticos referenciados no artigo 23.º, n.º 1.

O artigo 24.º diz respeito à publicação, pela Comissão, de uma lista de dispositivos de criação de assinatura eletrónica qualificados após notificação da sua conformidade pelos Estados-Membros.

O artigo 25.º baseia-se nas recomendações do anexo IV da Diretiva 1999/93/CE no sentido de se estabelecerem requisitos obrigatórios para a validação das assinaturas eletrónicas qualificadas, tendo em vista aumentar a segurança jurídica dessa validação.

O artigo 26.º estabelece as condições para os serviços de validação qualificados.

O artigo 27.º estabelece as condições para a preservação a longo prazo das assinaturas eletrónicas qualificadas. Tal é possível graças à utilização de procedimentos e tecnologias

capazes de prolongar a fiabilidade dos dados de validação das assinaturas eletrónicas qualificadas para além do prazo da sua validade tecnológica, quando se pode tornar mais fácil para os piratas informáticos a sua falsificação.

3.3.3.4 Secção 4 – Selos eletrónicos

O artigo 28.º diz respeito ao efeito legal dos selos eletrónicos das pessoas coletivas. É conferida uma presunção legal específica a um selo eletrónico qualificado que garanta a origem e a integridade dos documentos eletrónicos aos quais está associado.

O artigo 29.º estabelece os requisitos aplicáveis aos certificados qualificados de selos eletrónicos.

O artigo 30.º estabelece os requisitos para a lista dos dispositivos de criação de selos eletrónicos qualificados e para a certificação e a publicação da mesma.

O artigo 31.º estabelece as condições para a validação e preservação dos selos eletrónicos qualificados.

3.3.3.5 Secção 5 – Carimbo eletrónico da hora

O artigo 33.º diz respeito ao efeito legal dos carimbos eletrónicos da hora. É conferida uma presunção legal específica aos carimbos eletrónicos da hora qualificados no que respeita à exatidão da hora.

O artigo 33.º estabelece os requisitos para os carimbos eletrónicos da hora qualificados.

3.3.3.6 Secção 6 – Documentos eletrónicos

O artigo 34.º refere-se aos efeitos legais e às condições de aceitação dos documentos eletrónicos. Qualquer documento eletrónico assinado com uma assinatura eletrónica qualificada ou que ostente um selo eletrónico qualificado beneficia de uma presunção legal específica de autenticidade e integridade. No que respeita à aceitação de documentos eletrónicos, quando seja necessário um documento original ou uma cópia certificada para a prestação de um serviço público, serão aceites noutros Estados-Membros sem requisitos adicionais pelo menos os documentos eletrónicos emitidos pelas pessoas competentes para emitir os documentos pertinentes considerados originais ou cópias certificadas de acordo com a legislação nacional do Estado-Membro de origem.

3.3.3.7 Secção 7 – Serviços de entrega eletrónica

O artigo 35.º diz respeito ao efeito legal dos dados enviados ou recebidos utilizando um serviço de entrega eletrónica. Os serviços de entrega eletrónica qualificados beneficiam de uma presunção legal específica no que respeita à integridade dos dados enviados ou recebidos e à exatidão da hora em que os dados são enviados ou recebidos. O artigo garante também o reconhecimento mútuo dos serviços de entrega eletrónica qualificados a nível da UE.

O artigo 36.º estabelece os requisitos para os serviços de entrega eletrónica qualificados.

3.3.3.8 Secção 8 – Autenticação de sítios Web

Esta secção visa assegurar que a autenticidade de um sítio Web seja garantida no que respeita ao proprietário do sítio.

O artigo 37.º estabelece os requisitos para os certificados de autenticação de sítio Web qualificados, que podem servir para garantir a autenticidade de um sítio Web. Um certificado qualificado de autenticação de sítio Web fornece um conjunto mínimo de informações fiáveis sobre o sítio e sobre a existência legal do seu proprietário.

3.3.4 CAPÍTULO IV – ATOS DELEGADOS

O artigo 38.º contém as disposições-tipo aplicáveis ao exercício da delegação nos termos do artigo 290.º do TFUE (atos delegados). O artigo 290.º do TFUE permite ao legislador delegar na Comissão o poder de adotar atos não legislativos de aplicação geral que complementem ou alterem certos elementos não essenciais de um ato legislativo.

3.3.5 CAPÍTULO V – ATOS DE EXECUÇÃO

O artigo 39.º contém a disposição relativa ao procedimento de comité necessário para conferir competências de execução à Comissão nos casos em que, em conformidade com o artigo 291.º do TFUE, são necessárias condições uniformes para a execução de atos juridicamente vinculativos da União. Aplica-se o procedimento de exame.

3.3.6 CAPÍTULO VI – DISPOSIÇÕES FINAIS

O artigo 40.º impõe à Comissão a obrigação de avaliar o regulamento e de apresentar o relatório das suas conclusões.

O artigo 41.º revoga a Diretiva 1999/93/CE e consagra a transição harmoniosa da infraestrutura de assinatura eletrónica existente para os novos requisitos do regulamento.

O artigo 42.º fixa a data de entrada em vigor do regulamento.

4. INCIDÊNCIA ORÇAMENTAL

A incidência específica da proposta no orçamento da União Europeia prende-se com as tarefas atribuídas à Comissão Europeia, detalhadas na ficha financeira legislativa que acompanha a presente proposta.

A proposta não tem incidências nas despesas operacionais.

A ficha financeira legislativa que acompanha a presente proposta de regulamento cobre as incidências orçamentais do próprio regulamento.

2012/0146 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno

(Texto relevante para efeitos do EEE)

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 Europeu[11],

Após consulta da Autoridade Europeia para a Proteção de Dados[12],

Deliberando nos termos do processo legislativo ordinário,

Considerando o seguinte:

(1) Criar confiança no ambiente em linha é fundamental para o desenvolvimento económico. A falta de confiança leva os consumidores, as empresas e as administrações a hesitarem em realizar transações por via eletrónica e em adotar novos serviços.

(2) O presente regulamento pretende reforçar a confiança nas transações eletrónicas no mercado interno, permitindo que as interações eletrónicas entre as empresas, os cidadãos e as autoridades públicas se processem de um modo seguro e sem descontinuidades, aumentando assim a eficácia dos serviços públicos e privados em linha, os negócios eletrónicos e o comércio eletrónico na União.

(3) A Diretiva 1999/93/CE do Parlamento Europeu e do Conselho, de 13 de dezembro de 1999, relativa a um quadro legal comunitário para as assinaturas eletrónicas[13] cobria essencialmente as assinaturas eletrónicas sem oferecer um quadro transnacional e transetorial geral que garantisse transações eletrónicas seguras, fiáveis e fáceis de realizar. O presente regulamento melhora e desenvolve o acervo da diretiva.

---

11 JO C , p. .

12 JO C , p. .

13 JO L 13 de 19.1.2000, p. 12.

(4) A Agenda Digital para a Europa[14], lançada da Comissão, identificou a fragmentação do mercado digital, a falta de interoperabilidade e o aumento da cibercriminalidade como os principais obstáculos ao ciclo virtuoso da economia digital. No seu Relatório de 2010 sobre Cidadania, a Comissão foi mais longe ao sublinhar a necessidade de resolver os principais problemas que impedem os cidadãos europeus de colher os benefícios do mercado único digital e dos serviços digitais transfronteiras[15].

(5) O Conselho Europeu convidou a Comissão a criar um mercado único digital até 2015[16], para que se façam progressos rápidos em áreas fundamentais da economia digital, e a promover um mercado único digital completamente integrado[17] facilitando a utilização transfronteiras dos serviços em linha, dando particular atenção à facilitação da identificação e da autenticação eletrónicas seguras.

(6) O Conselho convidou a Comissão a contribuir para o mercado único digital criando condições adequadas para o reconhecimento mútuo entre os países de tecnologias facilitadoras fundamentais, como a identificação eletrónica, os documentos eletrónicos, as assinaturas eletrónicas e os serviços de entrega eletrónica, e para a implantação de serviços de administração pública em linha interoperáveis em toda a União Europeia[18].

(7) O Parlamento Europeu realçou a importância da segurança dos serviços eletrónicos - em especial, os de assinaturas eletrónicas - e da necessidade de criar uma infraestrutura de chave pública a nível pan-europeu e instou a Comissão a criar um portal para as autoridades de validação europeias, a fim de assegurar a interoperabilidade transfronteiras das assinaturas eletrónicas e aumentar a segurança das transações efetuadas através da Internet[19].

(8) A Diretiva 2006/123/CE do Parlamento Europeu e do Conselho, de 12 de dezembro de 2006, relativa aos serviços no mercado interno[20] exige que os Estados-Membros criem pontos de contacto únicos para garantir que todos os procedimentos e formalidades relativos ao acesso a uma atividade de prestação de serviços e ao seu exercício possam ser cumpridos facilmente, à distância e por meios eletrónicos, através do ponto de contacto único adequado e com as autoridades competentes. Muitos serviços em linha acessíveis através dos pontos de contacto únicos exigem identificação, autenticação e assinatura eletrónicas.

(9) Na maioria dos casos, os prestadores de serviços de outro Estado-Membro não podem utilizar a sua identificação eletrónica para aceder a esses serviços, porque os sistemas nacionais de identificação eletrónica no seu país não são reconhecidos nem aceites noutros Estados-Membros. Este obstáculo de cariz eletrónico impede os prestadores de serviços de tirarem pleno partido das vantagens do mercado interno. Meios de identificação eletrónica mutuamente reconhecidos e aceites facilitarão a oferta

14 COM(2010) 245 final/2.

15 Relatório de 2010 sobre a Cidadania da União: Eliminar os obstáculos ao exercício dos direitos dos cidadãos da UE, COM(2010) 603 final, ponto 2.2.2, p. 13.

16 4/2/2011: EUCO 2/1/11

17 23/10/2011: EUCO 52/1/11

18 Conclusões do Conselho sobre o plano de ação europeu para a administração pública em linha 2011–2015, 3093.ª reunião do Conselho Transportes, Telecomunicações e Energia, Bruxelas, 27 de maio de 2011.

19 Resolução do Parlamento Europeu de 21.9.2010 sobre a realização do mercado interno do comércio eletrónico, P7_TA(2010)0320, e Resolução do Parlamento Europeu de 15.6.2010 sobre o governo da Internet: as próximas etapas, P7_TA(2010)0208.

20 JO L 376 de 27.12.2006, p. 36.

transfronteiras de numerosos serviços no mercado interno e permitirão que as empresas desenvolvam as suas atividades fora de portas sem encontrarem muitos obstáculos nas interações com as autoridades públicas.

(10) A Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços[21] institui uma rede de autoridades nacionais responsáveis pela saúde em linha. Para aumentar a segurança e a continuidade dos cuidados de saúde transfronteiras, essa rede deve estabelecer orientações sobre o acesso transfronteiras aos dados e serviços eletrónicos de saúde, nomeadamente apoiando «*medidas comuns de identificação e autenticação destinadas a facilitar a transferibilidade dos dados no âmbito de cuidados de saúde transfronteiriços*». O reconhecimento e a aceitação mútuos da identificação e da autenticação eletrónicas são fundamentais para tornar realidade a prestação de cuidados de saúde aos cidadãos europeus a nível transnacional. Quando as pessoas se deslocam a outro país para receberem tratamento, é necessário que os seus dados médicos estejam acessíveis nesse país. Para isso, é indispensável que exista um quadro sólido, seguro e de confiança para a identificação eletrónica.

(11) Um dos objetivos do presente regulamento é eliminar os obstáculos existentes à utilização transnacional dos meios de identificação eletrónica utilizados nos Estados-Membros para aceder, pelo menos, a serviços públicos. O presente regulamento não visa intervir nos sistemas de gestão da identidade eletrónica e infraestruturas conexas estabelecidos nos Estados-Membros. O seu objetivo é garantir que, para aceder aos serviços em linha transfronteiras oferecidos pelos Estados-Membros, seja possível utilizar com segurança a identificação e a autenticação eletrónicas.

(12) Os Estados-Membros devem continuar a ter a liberdade de utilizar ou de introduzir, para fins de identificação eletrónica, meios de acesso aos serviços em linha. Devem igualmente poder decidir envolver ou não o setor privado na oferta desses meios. Os Estados-Membros não devem ser obrigados a notificar os seus sistemas de identificação eletrónica. A decisão de notificar todos, alguns ou nenhum dos meios de identificação eletrónica abrangidos pelo sistema utilizado a nível nacional para aceder a, pelo menos, serviços públicos ou serviços específicos em linha compete aos Estados-Membros.

(13) Há que estabelecer no regulamento algumas condições respeitantes aos meios de identificação eletrónica que têm de ser aceites e ao modo como os sistemas devem ser notificados. Essas condições deverão ajudar os Estados-Membros a criar a confiança necessária nos sistemas de identificação eletrónica uns dos outros e a reconhecer e aceitar mutuamente os meios de identificação eletrónica previstos nos seus sistemas notificados. O princípio do reconhecimento e da aceitação mútuos deverá aplicar-se se o Estado-Membro notificante satisfizer as condições de notificação e se a notificação tiver sido publicada no Jornal Oficial da União Europeia. No entanto, o acesso a esses serviços em linha e a sua entrega final ao requerente deverão estar estreitamente ligados ao direito de receber tais serviços nas condições estabelecidas pela legislação nacional.

[21] JO L 88 de 4.4.2011, p. 45.

(14) Os Estados-Membros deverão poder decidir envolver o setor privado na produção de meios de identificação eletrónica e autorizar o setor privado a utilizar meios de identificação eletrónica no âmbito de um sistema notificado para fins de identificação sempre que necessário para serviços em linha ou transações eletrónicas. A possibilidade de utilizar esses meios de identificação eletrónica permitirá que o setor privado recorra à identificação e à autenticação eletrónicas já amplamente utilizadas em muitos Estados-Membros pelo menos para os serviços públicos e que seja mais fácil para as empresas e para os cidadãos acederem aos seus serviços em linha noutros países. Para facilitar a utilização desses meios de identificação eletrónica a nível transfronteiras pelo setor privado, a possibilidade de autenticação oferecida pelos Estados-Membros deve estar disponível para as partes utilizadoras sem discriminações entre o setor público e o privado.

(15) A utilização transnacional de meios de identificação eletrónica no âmbito de um sistema notificado exige aos Estados-Membros que cooperem para assegurar a interoperabilidade técnica. Tal exclui a existência de regras técnicas nacionais específicas que exijam às partes não nacionais que, por exemplo, obtenham *hardware* ou *software* específicos para verificar e validar a identificação eletrónica notificada. Em contrapartida, a imposição de requisitos técnicos aos utilizadores, decorrentes das especificações inerentes ao tipo de dispositivo/testemunho utilizado (por exemplo, cartões inteligentes), é inevitável.

(16) A cooperação entre os Estados-Membros deve visar garantir a interoperabilidade técnica dos sistemas de identificação eletrónica notificados, a fim de criar um nível elevado de confiança e segurança, adequado ao grau de risco. A troca de informações e a partilha das melhores práticas entre os Estados-Membros tendo em vista o seu reconhecimento mútuo deverão facilitar essa cooperação.

(17) O presente regulamento deve igualmente estabelecer um quadro legal geral para a utilização dos serviços de confiança eletrónicos. No entanto, não deve criar uma obrigação geral de utilização dos mesmos. Designadamente, não deve abranger a oferta de serviços baseada em acordos voluntários de direito privado. Também não deve abranger aspetos relacionados com a conclusão e a validade de contratos ou outras obrigações legais caso existam requisitos de caráter formal prescritos pelo direito nacional ou da União,

(18) A fim de contribuir para a utilização transfronteiras generalizada dos serviços de confiança eletrónicos, deve ser possível utilizá-los como prova em justiça em todos os Estados-Membros.

(19) Os Estados-Membros devem permanecer livres de definir outros tipos de serviços de confiança para além dos que figuram na lista fechada de serviços de confiança prevista no presente regulamento, tendo em vista o seu reconhecimento a nível nacional como serviços de confiança qualificados.

(20) Devido ao ritmo da evolução tecnológica, o presente regulamento deve adotar uma abordagem aberta às inovações.

(21) O presente regulamento deve ser tecnologicamente neutro. Os efeitos legais que o presente regulamento confere devem poder ser atingidos por qualquer meio técnico, desde que os requisitos do regulamento sejam cumpridos.

(22) Para aumentar a confiança do público no mercado interno e promover a utilização de serviços e produtos de confiança, devem ser introduzidas as noções de serviço de confiança qualificado e de prestador de serviço de confiança qualificado, tendo em vista indicar os requisitos e obrigações a cumprir para assegurar um nível elevado de segurança em todos os serviços e produtos de confiança qualificados que sejam utilizados ou fornecidos.

(23) Em consonância com as obrigações previstas na Convenção das Nações Unidas sobre os direitos das pessoas com deficiência, que entrou em vigor na UE, as pessoas com deficiência devem poder utilizar os serviços de confiança oferecidos e os produtos de utilizador final utilizados nesses serviços em condições idênticas às dos outros consumidores.

(24) Um prestador de serviços de confiança é responsável pelo tratamento de dados pessoais e, como tal, tem que cumprir as obrigações estabelecidas na Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[22]. A recolha de dados, em particular, deve ser reduzida ao mínimo possível, tendo em conta a finalidade do serviço prestado.

(25) As entidades supervisoras deverão cooperar e trocar informações com as autoridades responsáveis pela proteção de dados a fim de garantir a correta aplicação da legislação relativa à proteção de dados pelos prestadores de serviços. A troca de informações deverá, nomeadamente, abranger os incidentes de segurança e as violações dos dados pessoais.

(26) Deverá competir a todos os prestadores de serviços de confiança aplicar boas práticas de segurança, adequadas aos riscos inerentes às suas atividades, de modo a incutirem nos utilizadores confiança no mercado único.

(27) As disposições relativas à utilização de pseudónimos nos certificados não devem impedir os Estados-Membros de exigirem a identificação das pessoas nos termos da legislação da União ou nacional.

(28) Todos os Estados-Membros deverão cumprir requisitos essenciais comuns em matéria de supervisão, a fim de garantir, para os serviços de confiança qualificados, um nível de segurança comparável. Para facilitar a aplicação coerente desses requisitos em toda a União, os Estados-Membros deverão adotar procedimentos comparáveis e trocar informações sobre as suas atividades de supervisão e as melhores práticas neste domínio.

(29) A notificação das violações da segurança e das avaliações dos riscos para a segurança é essencial para fornecer informações adequadas às partes em causa em caso de violação da segurança ou de perda de integridade.

(30) Para permitir à Comissão e aos Estados-Membros avaliar a eficácia do mecanismo de notificação das violações da segurança instaurado pelo presente regulamento, deve exigir-se às entidades supervisoras que forneçam informações sucintas à Comissão e à Agência Europeia para a Segurança das Redes e da Informação (ENISA).

---

22 JO L 281 de 23.11.1995, p. 31.

(31) Para permitir à Comissão e aos Estados-Membros avaliar o impacto do presente regulamento, deve exigir-se à entidades supervisoras que forneçam dados estatísticos sobre os serviços de confiança qualificados e sobre a sua utilização.

(32) Para permitir à Comissão e aos Estados-Membros avaliar a eficácia do mecanismo de reforço da supervisão instaurado pelo presente regulamento, deve exigir-se às entidades supervisoras que façam relatório das suas atividades. Essa obrigação será fundamental para facilitar o intercâmbio de boas práticas entre as entidades supervisoras e garantirá a verificação de que os requisitos essenciais da supervisão são aplicados de modo coerente e eficiente em todos os Estados-Membros.

(33) Para garantir a sustentabilidade e a durabilidade dos serviços de confiança qualificados e promover a confiança dos utilizadores na sua continuidade, as entidades supervisoras devem garantir que os dados dos prestadores de serviços de confiança qualificados sejam preservados e mantidos acessíveis durante um período de tempo adequado mesmo que um prestador de serviços de confiança qualificados deixe de existir.

(34) Para facilitar a fiscalização dos prestadores de serviços de confiança qualificados, por exemplo no caso de um prestador oferecer os seus serviços no território de outro Estado-Membro onde não está sujeito a supervisão, ou no caso de os computadores de um prestador estarem localizados no território de um Estado-Membro diferente daquele em que se encontra estabelecido, deve ser criado um sistema de assistência mútua entre as entidades supervisoras dos Estados-Membros.

(35) Os prestadores de serviços de confiança são responsáveis pelo cumprimento dos requisitos estabelecidos pelo presente regulamento para a prestação de serviços de confiança, em particular serviços de confiança qualificados. As entidades supervisoras têm a responsabilidade de fiscalizar o cumprimento desses requisitos pelos prestadores de serviços de confiança.

(36) Para permitir um processo de iniciação eficaz, que deverá levar à inclusão em listas de confiança dos prestadores de serviços de confiança qualificados e dos serviços de confiança qualificados que eles prestam, deverão ser encorajadas as interações preliminares entre os futuros prestadores de serviços de confiança qualificados e a entidade supervisora competente, no intuito de facilitar as diligências necessárias para a oferta de serviços de confiança qualificados.

(37) As listas de confiança são elementos essenciais para a criação de confiança entre os operadores do mercado, uma vez que indicam o estatuto de qualificado do prestador do serviço atribuído por ocasião da fiscalização, mas, por outro lado, não constituem um requisito prévio para que um prestador atinja o estatuto de qualificado e preste serviços de confiança qualificados, que resulta do facto de respeitar os requisitos do presente regulamento.

(38) Uma vez que tenha sido objeto de uma notificação, um serviço de confiança qualificado não pode ser recusado para o cumprimento de um procedimento ou de uma formalidade administrativos pelo organismo público em causa pelo facto de não estar incluído nas listas de confiança elaboradas pelos Estados-Membros. Para efeitos do presente regulamento, um organismo do setor público é qualquer autoridade pública ou outra entidade à qual é confiada a prestação de serviços de administração pública

em linha, como declarações fiscais em linha, pedidos de certidões de nascimento em linha, participação em concursos públicos eletrónicos, etc.

(39) Embora seja necessário um nível elevado de segurança para garantir o reconhecimento mútuo das assinaturas eletrónicas, em casos específicos, como no contexto da Decisão 2009/767/CE da Comissão, de 16 de outubro 2009, que determina medidas destinadas a facilitar a utilização de procedimentos informatizados através de balcões únicos nos termos da Diretiva 2006/123/CE do Parlamento Europeu e do Conselho relativa aos serviços no mercado interno[23], deverão igualmente ser aceites assinaturas eletrónicas com menor garantia de segurança.

(40) Os dispositivos de criação de assinaturas eletrónicas qualificados devem poder ser confiados pelo signatário a um terceiro, desde que sejam aplicados mecanismos e procedimentos adequados para garantir que o signatário tem o controlo exclusivo da utilização dos dados necessários para a criação da sua assinatura eletrónica e que a utilização do dispositivo cumpre os requisitos da assinatura qualificada.

(41) Para garantir segurança jurídica no que respeita à validade da assinatura, é essencial especificar quais os componentes de uma assinatura eletrónica qualificada que devem ser avaliados pela parte utilizadora que procede à validação. Além disso, a definição dos requisitos para os prestadores de serviços de confiança qualificados que podem prestar um serviço de validação qualificado a partes utilizadoras que não desejem ou não possam efetuar elas mesmas a validação das assinaturas eletrónicas qualificadas deverá estimular os setores público e privado a investirem em tais serviços. Ambos os setores devem tornar a validação das assinaturas eletrónicas qualificadas fácil e conveniente para todas as partes a nível da União.

(42) Quando uma transação exigir um selo eletrónico qualificado de uma pessoa coletiva, deverá ser igualmente aceitável uma assinatura eletrónica qualificada do representante autorizado da pessoa coletiva.

(43) Os selos eletrónicos devem servir de prova de que um documento eletrónico foi produzido por uma pessoa coletiva, garantindo a veracidade da origem e da integridade do documento.

(44) O presente regulamento deve assegurar a preservação a longo prazo das informações, ou seja, a validade legal das assinaturas e dos selos eletrónicos durante períodos de tempo alargados, garantindo que possam ser validados independentemente da evolução tecnológica futura.

(45) Para melhorar a utilização transfronteiras de documentos eletrónicos, o presente regulamento deve prever o efeito legal dos documentos eletrónicos, que devem ser considerados equivalentes a documentos em papel, dependendo da avaliação do risco e desde que a autenticidade e integridade dos documentos estejam asseguradas. Para o futuro desenvolvimento das transações eletrónicas transfronteiras no mercado interno, é também importante que os documentos eletrónicos originais ou as cópias certificadas produzidos num Estado-Membro por organismos competentes nos termos do direito nacional sejam também aceites enquanto tal nos outros Estados-Membros. O presente regulamento não deve afetar o direito dos Estados-Membros de determinarem o que

[23] JO L 274 de 20.10.2009, p. 36.

constitui um original ou uma cópia a nível nacional, mas garante que estes possam também ser utilizados enquanto tal fora do território nacional.

(46) Como as autoridades competentes dos Estados-Membros utilizam atualmente diferentes formatos de assinatura eletrónica avançada para assinar eletronicamente os seus documentos, é necessário garantir que pelo menos alguns formatos de assinatura eletrónica avançada possam ser tecnicamente aceites pelos Estados-Membros sempre que recebam documentos assinados eletronicamente. Do mesmo modo, se as autoridades competentes dos Estados-Membros utilizarem selos eletrónicos avançados, será necessário garantir a sua compatibilidade técnica com, pelo menos, alguns formatos de selo eletrónico avançado.

(47) Para além de autenticarem o documento produzido pela pessoa coletiva, os selos eletrónicos podem ser utilizados para autenticar qualquer bem digital da pessoa coletiva, como, por exemplo, um código de *software* ou um servidor.

(48) Ao possibilitar-se a autenticação de sítios Web e da pessoa que é sua proprietária, torna-se mais difícil a falsificação desses sítios e reduz-se, por conseguinte, a fraude.

(49) Para complementar, de um modo flexível e rápido, certos aspetos técnicos detalhados do presente regulamento, deve ser delegado na Comissão o poder de adotar atos em conformidade com o artigo 290.º do Tratado sobre o Funcionamento da União Europeia no que respeita à interoperabilidade da identificação eletrónica, às medidas de segurança exigidas aos prestadores de serviços de confiança, aos organismos independentes reconhecidos responsáveis pelas auditorias aos prestadores de serviços, às listas de confiança, às exigências relativas aos níveis de segurança das assinaturas eletrónicas, aos requisitos dos certificados qualificados para assinaturas eletrónicas, sua validação e preservação, aos organismos responsáveis pela certificação dos dispositivos de criação de assinaturas eletrónicas qualificados, às exigências relativas aos níveis de segurança dos selos eletrónicos e aos certificados qualificados de selos eletrónicos e à interoperabilidade dos serviços de entrega. É particularmente importante que a Comissão proceda a consultas adequadas durante os seus trabalhos preparatórios, inclusive a nível de peritos.

(50) Quando preparar e redigir atos delegados, a Comissão deverá assegurar a transmissão simultânea, atempada e adequada dos documentos pertinentes ao Parlamento Europeu e ao Conselho.

(51) Para garantir condições uniformes de aplicação do presente regulamento, devem ser conferidos à Comissão poderes de execução, nomeadamente para especificar os números de referência das normas cuja utilização conferirá uma presunção de conformidade com certos requisitos estabelecidos no presente regulamento ou definidos em atos delegados. Esses poderes devem ser exercidos em conformidade com o Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão[24].

(52) Por razões de segurança jurídica e de clareza, a Diretiva 1999/93/CE deve ser revogada.

---

[24] JO L 55 de 28.2.2011, p. 13.

(53) Para garantir segurança jurídica aos operadores do mercado que já utilizam certificados qualificados emitidos em conformidade com a Diretiva 1999/93/CE, é necessário prever um período de tempo suficiente para a transição. É também necessário dotar a Comissão de meios que lhe permitam adotar os atos de execução e os atos delegados antes dessa data.

(54) Atendendo a que os objetivos do presente regulamento não podem ser suficientemente realizados pelos Estados-Membros e podem, pois, devido à dimensão da ação prevista, ser mais bem alcançados ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não vai além do necessário para atingir esse objetivo, em especial no que respeita ao papel da Comissão enquanto coordenadora das atividades nacionais,

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

1. O presente regulamento estabelece regras para a identificação eletrónica e os serviços de confiança eletrónicos utilizados nas transações eletrónicas, tendo em vista assegurar o correto funcionamento do mercado interno.

2. O presente regulamento estabelece as condições em que um Estado-Membro deve reconhecer e aceitar os meios de identificação eletrónica de pessoas singulares e coletivas no quadro de um sistema de identificação eletrónica notificado de outro Estado-Membro.

3. O presente regulamento institui um quadro legal para as assinaturas eletrónicas, os selos eletrónicos, os carimbos eletrónicos da hora, os documentos eletrónicos, os serviços de entrega eletrónica e a autenticação de sítios Web.

4. O presente regulamento garante que os serviços e produtos de confiança conformes com as suas disposições sejam autorizados a circular livremente no mercado interno.

Artigo 2.º

Âmbito de aplicação

1. O presente regulamento aplica-se à identificação eletrónica fornecida pelos, em nome dos ou sob a responsabilidade dos Estados-Membros e aos prestadores de serviços de confiança estabelecidos na União.

2. O presente regulamento não se aplica à oferta de serviços de confiança eletrónicos com base em acordos voluntários de direito privado.

3. O presente regulamento não abrange aspetos relacionados com a conclusão e a validade de contratos ou outras obrigações legais em que existam requisitos de caráter formal prescritos pelo direito nacional ou da União.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Identificação eletrónica»: o processo de utilização de dados de identificação pessoal em formato eletrónico que representam inequivocamente uma pessoa singular ou coletiva;

2) «Meio de identificação eletrónico»: uma unidade material ou imaterial que contém os dados referidos no ponto 1) do presente artigo e que é utilizada para aceder a serviços em linha nos termos previstos no artigo 5.º;

3) «Sistema de identificação eletrónica»: um sistema em que são produzidos meios de identificação eletrónica para as pessoas referidas no ponto 1) do presente artigo;

4) «Autenticação»: processo eletrónico que permite a validação da identificação eletrónica de uma pessoa singular ou coletiva ou da origem e integridade de um dado eletrónico;

5) «Signatário»: pessoa singular que cria uma assinatura eletrónica;

6) «Assinatura eletrónica»: dados em forma eletrónica que se ligam ou estão logicamente associados a outros dados eletrónicos e que são utilizados pelo signatário para assinar;

7) «Assinatura eletrónica avançada»: uma assinatura eletrónica que obedece aos seguintes requisitos:

(a) está associada de forma única ao signatário;

(b) permite identificar o signatário;

(c) é criada utilizando dados para a criação de uma assinatura eletrónica que o signatário pode, com um elevado nível de confiança, utilizar sob o seu controlo exclusivo; e

(d) está ligada aos dados a que diz respeito de tal modo que qualquer alteração subsequente dos dados é detetável;

8) «Assinatura eletrónica qualificada»: uma assinatura eletrónica avançada que é criada por um dispositivo de criação de assinaturas eletrónicas qualificado e que se baseia num certificado qualificado de assinatura eletrónica;

9) «Dados para a criação de uma assinatura eletrónica»: dados exclusivos que são utilizados pelo signatário para criar uma assinatura eletrónica;

10) «Certificado»: um atestado eletrónico que associa os dados de validação da assinatura eletrónica ou do selo eletrónico respetivamente de uma pessoa singular ou coletiva a um certificado e confirma os dados dessa pessoa;

11) «Certificado qualificado de assinatura eletrónica»: um atestado que é utilizado como suporte das assinaturas eletrónicas, é emitido por um prestador de serviços de confiança qualificado e satisfaz os requisitos estabelecidos no anexo I;

12) «Serviço de confiança»: qualquer serviço eletrónico que vise a criação, verificação, validação, tratamento e preservação de assinaturas eletrónicas, selos eletrónicos, carimbos eletrónicos da hora, documentos eletrónicos, serviços de entrega eletrónica, autenticação de sítios Web e certificados eletrónicos, incluindo certificados de assinatura eletrónica e de selos eletrónicos;

13) «Serviço de confiança qualificado»: um serviço de confiança que satisfaz os requisitos aplicáveis previstos no presente regulamento;

14) «Prestador de serviços de confiança»: uma pessoa singular ou coletiva que presta um ou mais do que um serviço de confiança;

15) «Prestador de serviços de confiança qualificado»: um prestador de serviços de confiança que satisfaz os requisitos estabelecidos no presente regulamento;

16) «Produto»: *hardware* ou *software*, ou componentes pertinentes dos mesmos, que se destinam a ser utilizados para a oferta de serviços de confiança;

17) «Dispositivo de criação de assinaturas eletrónicas»: *software* ou *hardware* configurados, utilizados para criar assinaturas eletrónicas;

18) «Dispositivo de criação de assinaturas eletrónicas qualificado»: um dispositivo para criação de assinaturas eletrónicas conforme com os requisitos constantes do anexo II;

19) «Criador de um selo»: uma pessoa coletiva que cria um selo eletrónico;

20) «Selo eletrónico»: dados em forma eletrónica que são apensos ou logicamente associados a outros dados eletrónicos para garantir a origem e a integridade dos dados associados;

21) «Selo eletrónico avançado»: um selo eletrónico que obedece aos seguintes requisitos:

(a) está associado de forma única ao seu criador;

(b) permite identificar o seu criador;

(c) é criado utilizando dados para a criação de um selo eletrónico que o criador do selo pode, com um elevado nível de confiança e sob o seu controlo, utilizar para a criação de um selo eletrónico; e

(d) está ligado aos dados a que diz respeito de tal modo que qualquer alteração subsequente dos dados é detetável;

22) «Selo eletrónico qualificado»: um selo eletrónico avançado que é criado por um dispositivo de criação de selos eletrónicos qualificado e que se baseia num certificado qualificado de selo eletrónico;

23) «Dados para a criação de um selo eletrónico»: dados únicos que são utilizados pelo criador do selo eletrónico para criar um selo eletrónico;

24) «Certificado qualificado de selo eletrónico»: um atestado que é utilizado como suporte de um selo eletrónico, é emitido por um prestador de serviços de confiança qualificado e satisfaz os requisitos estabelecidos no anexo III;

25) «Carimbo eletrónico da hora»: dados em forma eletrónica que vinculam outros dados eletrónicos a uma hora específica, criando uma prova de que esses dados existiam nesse momento;

26) «Carimbo eletrónico da hora qualificado»: um carimbo eletrónico da hora que satisfaz os requisitos estabelecidos no artigo 33.º;

27) «Documento eletrónico»: um documento num qualquer formato eletrónico;

28) «Serviço de entrega eletrónica»: um serviço que torna possível a transmissão de dados por meios eletrónicos e fornece prova do tratamento dos dados transmitidos, nomeadamente a prova do envio ou da receção dos mesmos, e que protege os dados transferidos contra o risco de perda, roubo, dano ou alterações não autorizadas;

29) «Serviço de entrega eletrónica qualificado»: um serviço de entrega eletrónica que satisfaz os requisitos estabelecidos no artigo 36.º;

30) «Certificado qualificado de autenticação de sítio Web»: um atestado que torna possível autenticar um sítio Web e que associa o sítio Web à pessoa para a qual o certificado é emitido, é emitido por um prestador de serviços de confiança qualificado e satisfaz os requisitos estabelecidos no anexo IV;

31) «Dados de validação»: dados que são utilizados para validar uma assinatura eletrónica ou um selo eletrónico.

Artigo 4.º

Princípios relativos ao mercado interno

1. Não pode haver restrições à oferta de serviços de confiança no território de um Estado-Membro por um prestador de serviços de confiança estabelecido noutro Estado-Membro por razões que se enquadrem nos domínios cobertos pelo presente regulamento.

2. Os produtos que estejam conformes com o presente regulamento estão autorizados a circular livremente no mercado interno.

CAPÍTULO II

IDENTIFICAÇÃO ELETRÓNICA

Artigo 5.º

Reconhecimento e aceitação mútuos

Quando, para aceder a um serviço em linha, seja exigida, nos termos da legislação ou da prática administrativa nacionais, uma identificação eletrónica baseada num meio de identificação eletrónica e numa autenticação, qualquer meio de identificação eletrónica produzido noutro Estado-Membro e que se enquadre num sistema constante da lista publicada pela Comissão de acordo com o procedimento referido no artigo 7.º deve ser reconhecido e aceite para efeitos de acesso a esse serviço.

Artigo 6.º

Condições de notificação dos sistemas de identificação eletrónica

1. Os sistemas de identificação eletrónica são elegíveis para notificação nos termos do artigo 7.º se estiverem reunidas todas as seguintes condições:

(a) os meios de identificação eletrónica são produzidos pelo Estado-Membro notificante, em seu nome ou sob a sua responsabilidade;

(b) os meios de identificação eletrónica podem ser utilizados para aceder pelo menos a serviços públicos que exigem identificação eletrónica no Estado-Membro notificante;

(c) o Estado-Membro notificante garante que os dados da identificação da pessoa sejam atribuídos inequivocamente à pessoa singular ou coletiva referida no artigo 3.º, ponto 1);

(d) o Estado-Membro notificante garante a disponibilidade de uma possibilidade de autenticação em linha, em qualquer altura e gratuitamente, para que qualquer parte utilizadora possa validar os dados de identificação da pessoa recebidos em forma eletrónica. Os Estados-Membros não podem impor requisitos técnicos específicos às partes utilizadores estabelecidas fora do seu território que tencionam efetuar essa autenticação. Se o sistema de identificação notificado ou a possibilidade de autenticação forem violados ou parcialmente afetados, os Estados-Membros devem suspender ou revogar sem demora o sistema de identificação notificado ou a possibilidade de autenticação ou as partes afetadas em causa e informar do facto os outros Estados-Membros e a Comissão em conformidade com o artigo 7.º;

(e) o Estado-Membro notificante é responsável:

– (i) pela atribuição inequívoca dos dados de identificação da pessoa referidos na alínea c); e

– (ii) pela possibilidade de autenticação especificada na alínea d).

2. A alínea e) do n.º 1 não prejudica a responsabilidade das partes numa transação em que sejam utilizados meios de identificação eletrónica abrangidos pelo sistema notificado.

Artigo 7.º

Notificação

1. Os Estados-Membros que notifiquem um sistema de identificação eletrónica devem enviar à Comissão as seguintes informações e, sem atrasos indevidos, todas as eventuais alterações subsequentes às mesmas:

(a) uma descrição do sistema de identificação eletrónica notificado;

(b) as autoridades responsáveis pelo sistema de identificação eletrónica notificado;

(c) informações sobre quem gere o registo dos identificadores inequívocos da pessoa;

(d) uma descrição da possibilidade de autenticação;

(e) as disposições previstas para a suspensão ou a revogação do sistema de identificação notificado, da possibilidade de autenticação ou das partes afetadas em causa.

2. Seis meses após a entrada em vigor do regulamento, a Comissão publica no *Jornal Oficial da União Europeia* a lista dos sistemas de identificação eletrónica que foram notificados nos termos do n.º 1 e as informações básicas a eles respeitantes.

3. Caso receba uma notificação após o termo do prazo referido no n.º 2, a Comissão altera a lista num prazo de três meses.

4. A Comissão pode, através de atos de execução, definir as circunstâncias, os formatos e os procedimentos da notificação referida nos n.^{os} 1 e 3. Esses atos de execução são adotados em conformidade com o procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 8.º

Coordenação

1. Os Estados-Membros devem cooperar no sentido de garantir a interoperabilidade dos meios de identificação eletrónica abrangidos por um sistema notificado e melhorar a segurança desses meios.

2. A Comissão estabelecerá, através de atos de execução, as necessárias modalidades de facilitação da cooperação entre os Estados-Membros a que se refere o n.º 1, tendo em vista promover um nível elevado de confiança e segurança, adequado ao grau de risco. Esses atos de execução versarão, nomeadamente, sobre a troca de informações, experiências e boas práticas em matéria de sistemas de identificação eletrónica, a avaliação pelos pares dos sistemas de identificação eletrónica notificados e o exame, pelas autoridades competentes dos Estados-Membros, dos desenvolvimentos importantes que surjam no setor da identificação eletrónica. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

3. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 38.º no que respeita à facilitação da interoperabilidade transfronteiras dos meios de identificação eletrónica através do estabelecimento de requisitos técnicos mínimos.

CAPÍTULO III

SERVIÇOS DE CONFIANÇA

Secção 1

Disposições gerais

Artigo 9.º

Responsabilidade

1. Um prestador de serviços de confiança é responsável por qualquer dano direto causado a uma pessoa singular ou coletiva devido ao não cumprimento das obrigações previstas no artigo 15.º, n.º 1, a menos que prove que não agiu com negligência.

2. Um prestador de serviços de confiança qualificado é responsável por qualquer dano direto causado a uma pessoa singular ou coletiva devido ao não cumprimento dos requisitos do presente regulamento, em particular os previstos no artigo 19.º, a menos que prove que não agiu com negligência.

Artigo 10.º

Prestadores de serviços de confiança de países terceiros

1. Os serviços de confiança qualificados e os certificados qualificados fornecidos por prestadores de serviços de confiança qualificados estabelecidos num país terceiro devem ser aceites como serviços de confiança qualificados e certificados qualificados fornecidos por prestadores de serviços de confiança qualificados estabelecidos no território da União Europeia, se os serviços de confiança qualificados ou os certificados qualificados originários do país terceiro forem reconhecidos ao abrigo de um acordo entre a União e os países terceiros ou organizações internacionais em conformidade com o artigo 218.º do TFUE.

2. No que respeita ao n.º 1, tais acordos devem garantir que os requisitos aplicáveis aos serviços de confiança qualificados e aos certificados qualificados fornecidos por prestadores de serviços de confiança qualificados estabelecidos no território da União sejam cumpridos pelos prestadores de serviços de confiança dos países terceiros ou organizações internacionais, especialmente no que se refere à proteção dos dados pessoais, à segurança e à supervisão.

Artigo 11.º

Tratamento e proteção dos dados

1. Os prestadores de serviços de confiança e as entidades supervisoras devem garantir um tratamento leal e lícito dos dados pessoais processados, em conformidade com a Diretiva 95/46/CE.

2. Os prestadores de serviços de confiança devem tratar os dados pessoais de acordo com a Diretiva 95/46/CE. Esse tratamento estará estritamente limitado aos dados mínimos necessários para emitir e manter atualizado um certificado ou fornecer um serviço de confiança.

3. Os prestadores de serviços de confiança devem garantir a confidencialidade e a integridade dos dados relativos à pessoa à qual o serviço de confiança é prestado.

4. Sem prejuízo dos efeitos legais conferidos aos pseudónimos nos termos das legislações nacionais, os Estados-Membros não poderão impedir que os prestadores de serviços de confiança indiquem nos certificados de assinatura eletrónica um pseudónimo em vez do nome do signatário.

Artigo 12.º

Acessibilidade para as pessoas com deficiência

Os serviços de confiança oferecidos e os produtos de utilizador final utilizados na oferta desses serviços devem, sempre que possível, ser tornados acessíveis às pessoas com deficiência.

Secção 2

Supervisão

Artigo 13.º

Entidade supervisora

1. Os Estados-Membros designam uma entidade adequada estabelecida no seu território ou, por mútuo acordo, noutro Estado-Membro sob a responsabilidade do Estado-Membro que procede à designação. As entidades supervisoras serão dotadas de todos os poderes de fiscalização e investigação necessários para o exercício das suas funções.

2. A entidade supervisora é responsável pelo exercício das seguintes funções:

(a) fiscalizar os prestadores de serviços de confiança estabelecidos no território do Estado-Membro que procede à designação para garantir que cumprem os requisitos estabelecidos no artigo 15.º;

(b) fiscalizar os prestadores de serviços de confiança qualificados estabelecidos no território do Estado-Membro que procede à designação e dos serviços de confiança qualificados que oferecem, por forma a garantir que os ditos prestadores e os serviços de confiança qualificados que oferecem cumprem os requisitos aplicáveis estabelecidos no presente regulamento;

(c) garantir que as informações e os dados pertinentes referidos no artigo 19.º, n.º 2, alínea g), e registados pelos prestadores de serviços de confiança qualificados sejam preservados e mantidos acessíveis durante um prazo adequado depois de cessarem as atividades do prestador de serviços de confiança qualificado, com o intuito de garantir a continuidade do serviço.

3. Cada entidade supervisora deve apresentar à Comissão e aos Estados-Membros, até ao final do primeiro trimestre do ano seguinte, um relatório anual sobre as atividades de supervisão do último ano. O relatório deve incluir, pelo menos:

(a) informações sobre as suas atividades de supervisão;

(b) um resumo das notificações de violações recebidas dos prestadores de serviços de confiança em conformidade com o disposto no artigo 15.º, n.º 2;

(c) dados estatísticos sobre o mercado e a utilização dos serviços de confiança qualificados, incluindo informações sobre os próprios prestadores de serviços de confiança qualificados, os serviços de confiança qualificados que oferecem, os produtos que utilizam e uma descrição geral dos seus clientes.

4. Os Estados-Membros devem notificar à Comissão e aos outros Estados-Membros os nomes e os endereços das respetivas entidades supervisoras designadas.

5. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, no que diz respeito à definição dos procedimentos aplicáveis às funções referidas no n.º 2.

6. A Comissão pode, através de atos de execução, definir as circunstâncias, os formatos e os procedimentos para o relatório referido no n.º 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 14.º

Assistência mútua

1. As entidades supervisoras devem cooperar tendo em vista o intercâmbio de boas práticas e o fornecimento mútuo, no mais curto prazo possível, de informações pertinentes e assistência para que as respetivas atividades possam ser levadas a cabo de uma maneira coerente. A assistência mútua deve abranger, em particular, pedidos de informações e medidas de supervisão, tais como pedidos para efetuar inspeções relacionadas com as auditorias de segurança, referidas nos artigos 15.º, 16.º e 17.º.

2. Uma entidade supervisora à qual tenha sido dirigido um pedido de assistência não pode recusar dar-lhe cumprimento, salvo se:

(a) não for competente para dar resposta ao pedido; ou

(b) a satisfação do pedido for incompatível com o presente regulamento.

3. Quando adequado, as entidades supervisoras podem efetuar investigações conjuntas nas quais participem quadros das entidades supervisoras de outros Estados-Membros.

A entidade supervisora do Estado-Membro em que se realizará a investigação, em conformidade com a sua própria legislação nacional, pode delegar tarefas de investigação no pessoal da entidade supervisora assistida. Esses poderes apenas podem ser exercidos sob a orientação e na presença de pessoal da entidade supervisora anfitriã. O pessoal da entidade supervisora assistida está sujeito à legislação nacional da entidade supervisora anfitriã. A entidade supervisora anfitriã assume a responsabilidade pelas ações do pessoal da entidade supervisora assistida.

4. A Comissão pode especificar, por meio de atos de execução, as modalidades e os procedimentos da assistência mútua a que se refere o presente artigo. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 15.º

Requisitos de segurança aplicáveis aos prestadores de serviços de confiança

1. Os prestadores de serviços de confiança que estejam estabelecidos no território da União devem tomar as medidas técnicas e organizacionais adequadas para gerir os riscos que se colocam à segurança dos serviços de confiança que prestam. Tendo em conta o estado da técnica, essas medidas devem assegurar um nível de segurança adequado ao grau de risco existente. Em particular, devem ser tomadas medidas para impedir ou reduzir ao mínimo o

impacto dos incidentes de segurança e informar as partes interessadas dos efeitos adversos dos eventuais incidentes.

Sem prejuízo do artigo 16.º, n.º 1, qualquer prestador de serviços de confiança pode submeter o relatório de uma auditoria de segurança realizada por um organismo independente reconhecido à apreciação da entidade supervisora, para que esta confirme que foram tomadas as medidas de segurança adequadas.

2. Os prestadores de serviços de confiança devem notificar, sem demora indevida e, se possível, no prazo máximo de 24 horas após terem tomado conhecimento do ocorrido, a entidade supervisora competente, a entidade nacional competente em matéria de segurança da informação e terceiros relevantes, como as autoridades responsáveis pela proteção de dados, de todas as violações da segurança ou perdas de integridade que tenham um impacto significativo no serviço de confiança prestado e nos dados pessoais por ele mantidos.

Se adequado, em particular se uma violação da segurança ou uma perda de integridade disserem respeito a dois ou mais Estados-Membros, a entidade supervisora em causa informa do facto as entidades supervisoras dos outros Estados-Membros e a Agência Europeia para a Segurança das Redes e da Informação (ENISA).

A entidade supervisora em causa pode igualmente informar o público ou exigir que o prestador do serviço de confiança o faça, caso considere que a divulgação da violação é do interesse público.

3. A entidade supervisora deve fornecer à ENISA e à Comissão, uma vez por ano, um resumo das notificações de violações recebidas dos prestadores de serviços de confiança.

4. Para pôr em prática o disposto nos números 1 e 2, a entidade supervisora tem poderes para emitir instruções vinculativas para os prestadores de serviços de confiança.

5. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, que visem uma maior especificação das medidas referidas no n.º 1.

6. A Comissão pode, através de atos de execução, definir as circunstâncias, os formatos e os procedimentos, incluindo os prazos, aplicáveis para efeitos de cumprimento do disposto nos n.os 1 a 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 16.º

Fiscalização dos prestadores de serviços de confiança qualificados

1. Os prestadores de serviços de confiança qualificados são auditados uma vez por ano por um organismo independente reconhecido, para confirmar que eles, prestadores, e os serviços de confiança qualificados que prestam cumprem os requisitos estabelecidos pelo presente regulamento, devendo apresentar o relatório da auditoria de segurança à entidade supervisora.

2. Sem prejuízo do disposto no n.º 1, a entidade supervisora pode, em qualquer altura, por iniciativa própria ou em resposta a um pedido da Comissão, auditar os prestadores de serviços de confiança qualificados para confirmar que eles, prestadores, e os serviços de confiança qualificados que prestam continuam a satisfazer as condições estabelecidas no presente

regulamento. A entidade supervisora informa as autoridades responsáveis pela proteção de dados dos resultados das suas auditorias, caso suspeite de que tenham sido violadas as regras de proteção dos dados pessoais.

3. A entidade supervisora tem poderes para emitir instruções vinculativas aos prestadores de serviços de confiança qualificados para que corrijam os eventuais incumprimentos dos requisitos, mencionados no relatório da auditoria de segurança.

4. No respeitante ao disposto no n.º 3, se o prestador de serviços de confiança qualificado não corrigir o incumprimento dentro de um prazo fixado pela entidade supervisora, perde o seu estatuto de qualificado e será informado pela entidade supervisora de que o seu estatuto será alterado em conformidade nas listas de confiança a que se refere o artigo 18.º.

5. A Comissão tem poderes para adotar atos delegados em conformidade com o artigo 38.º no que respeita à especificação das condições em que o organismo independente que efetua a auditoria referida no n.º 1 do presente artigo, no artigo 15.º, n.º 1 e no artigo 17.º, n.º 1, será reconhecido.

6. A Comissão pode, através de atos de execução, definir as circunstâncias, os formatos e os procedimentos aplicáveis para efeitos do disposto nos n.os 1, 2 e 4. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 17.º

Início de um serviço de confiança qualificado

1. Os prestadores de serviços de confiança qualificados devem notificar a entidade supervisora da sua intenção de começarem a prestar um serviço de confiança qualificado, devendo apresentar à dita entidade o relatório de uma auditoria de segurança efetuada por um organismo independente reconhecido, como previsto no artigo 16.º, n.º 1. Os prestadores de serviços de confiança qualificados podem começar a prestar o serviço de confiança qualificado após terem entregue a notificação e o relatório de auditoria de segurança à entidade supervisora.

2. Uma vez entregues à entidade supervisora os documentos pertinentes, em conformidade com o n.º 1, os prestadores de serviços qualificados são incluídos nas listas de confiança a que se refere o artigo 18.º indicando que a notificação foi entregue.

3. A entidade supervisora verifica a conformidade do prestador de serviços de confiança qualificado e dos serviços qualificados que ele presta com os requisitos do regulamento.

A entidade supervisora indica, nas listas de confiança, o estatuto de qualificado dos prestadores de serviços qualificados e dos serviços de confiança qualificados que eles prestam após a conclusão positiva da verificação, o mais tardar um mês após a notificação efetuada em conformidade com o n.º 1.

Se a verificação não ficar concluída no prazo de um mês, a entidade supervisora informa do facto o prestador de serviços de confiança qualificado, especificando as razões do atraso e a data prevista para a conclusão da verificação.

4. Um serviço de confiança qualificado que tenha sido objeto de notificação nos termos do n.º 1 não pode ser recusado para o cumprimento de um procedimento ou de uma formalidade administrativos pelo organismo público em causa pelo facto de não estar incluído nas listas referidas no n.º 3.

5. A Comissão pode, através de atos de execução, definir as circunstâncias, os formatos e os procedimentos aplicáveis para efeitos do disposto nos n.os 1, 2 e 3. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 18.º

Listas de confiança

1. Cada Estado-Membro estabelece, mantém e publica listas de confiança contendo informações relativas aos prestadores de serviços de confiança qualificados para os quais é competente, assim como informações relacionadas com os serviços de confiança qualificados que eles prestam.

2. Os Estados-Membros estabelecem, mantêm e publicam, de um modo seguro, as listas de confiança, eletronicamente assinadas ou seladas, previstas no n.º 1, num formato adequado ao tratamento automático.

3. Os Estados-Membros comunicam à Comissão, sem atrasos indevidos, informações sobre a entidade responsável pelo estabelecimento, a manutenção e a publicação das listas de confiança nacionais, assim como pormenores do local em que tais listas se encontram publicadas, o certificado utilizado para assinar ou selar as listas de confiança e as eventuais alterações às mesmas.

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

5. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, no que diz respeito à definição das informações referidas no n.º 1.

6. A Comissão pode, através de atos de execução, definir as especificações técnicas e os formatos das listas de confiança, aplicáveis para efeitos do disposto nos n.os 1 a 4. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Artigo 19.º

Requisitos aplicáveis aos prestadores de serviços de confiança qualificados

1. Ao emitir um certificado qualificado, um prestador de serviços de confiança qualificado deve verificar, através de meios adequados e de acordo com a legislação nacional, a identidade e, se aplicável, os atributos específicos da pessoa singular ou coletiva para a qual é emitido o certificado qualificado.

Essas informações são verificadas pelo prestador de serviços qualificado ou por um terceiro autorizado que aja sob a responsabilidade do prestador de serviços qualificado:

(a) pela comparência física da pessoa singular ou de um representante autorizado da pessoa coletiva, ou

(b) à distância, utilizando meios de identificação eletrónica abrangidos por um sistema notificado, produzidos em conformidade com a alínea a).

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

(a) empregar pessoal que possua a especialização, a experiência e as qualificações necessárias, aplique procedimentos administrativos e de gestão que correspondam às normas europeias ou internacionais e tenha recebido formação adequada em matéria de regras de segurança e de proteção de dados pessoais;

(b) suportar o risco da responsabilidade por danos mantendo recursos financeiros suficientes ou recorrendo a um sistema adequado de seguro de responsabilidade;

(c) antes de estabelecerem uma relação contratual, informar as pessoas que pretendem utilizar um serviço de confiança qualificado dos termos e condições exatos da utilização desse serviço;

(d) utilizar sistemas e produtos fiáveis que estejam protegidos contra modificações e que garantam a segurança e a fiabilidade técnicas do processo de que são suporte;

(e) utilizar sistemas fiáveis de armazenamento dos dados que lhes são fornecidos, num formato verificável, de modo a que:

- os dados apenas estejam publicamente disponíveis para extração se tiver sido obtido o consentimento da pessoa para a qual os dados foram emitidos;
- apenas as pessoas autorizadas possam introduzir dados e alterações;
- a autenticidade das informações possa ser verificada;

(f) tomar medidas contra a falsificação e o roubo dos dados;

(g) registar, durante um período de tempo adequado, todas as informações pertinentes relativas aos dados emitidos e recebidos pelo prestador de serviços de confiança qualificado, em particular para efeitos de produção de prova em processos judiciais. Esse registo poderá ser feito eletronicamente;

(h) dispor de um plano de cessação de atividades atualizado que garanta a continuidade do serviço de acordo com as disposições emitidas pela entidade supervisora nos termos do artigo 13.º, n.º 2, alínea c);

(i) garantir um tratamento lícito dos dados pessoais em conformidade com o artigo 11.º.

3. Os prestadores de serviços de confiança qualificados que emitam certificados qualificados devem registar na sua base de dados de certificados a revogação do certificado no prazo de dez minutos após a efetivação da revogação.

4. No que respeita ao disposto no n.º 3, os prestadores de serviços de confiança qualificados que emitam certificados qualificados devem fornecer a qualquer parte utilizadora informações

sobre o estatuto de válido ou de revogado dos certificados qualificados por eles emitidos. Estas informações devem ser disponibilizadas em qualquer altura, para cada certificado pelo menos, de uma maneira automática que seja fiável, gratuita e eficaz.

5. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos sistemas e produtos fiáveis. Os sistemas e produtos fiáveis conformes com essas normas beneficiam da presunção de conformidade com os requisitos estabelecidos no artigo 19.º. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Secção 3

Assinatura eletrónica

Artigo 20.º

Efeitos legais e aceitação das assinaturas eletrónicas

1. A forma eletrónica de uma assinatura, por si só, não pode ser motivo para que lhe sejam negados efeitos legais e a admissibilidade enquanto prova em processos judiciais.

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

3. As assinaturas eletrónicas qualificadas devem ser reconhecidas e aceites em todos os Estados-Membros.

4. Se for exigida uma assinatura eletrónica com um nível de garantia de segurança inferior ao de uma assinatura eletrónica qualificada, nomeadamente por um Estado-Membro, para se aceder a um serviço em linha oferecido por um organismo público, com base numa avaliação adequada dos riscos envolvidos em tal serviço, devem ser reconhecidas e aceites todas as assinaturas eletrónicas que ofereçam pelo menos o mesmo nível de garantia de segurança.

5. Os Estados-Membros não poderão exigir, para o acesso transfronteiras a um serviço em linha oferecido por um organismo público, uma assinatura eletrónica com um nível de garantia de segurança superior ao de uma assinatura eletrónica qualificada.

6. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, no que diz respeito à definição dos diferentes níveis de segurança das assinaturas eletrónicas referidos no n.º 4.

7. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos níveis de segurança das assinaturas eletrónicas. Uma assinatura eletrónica conforme com essas normas beneficia da presunção de conformidade com o nível de segurança definido no ato delegado adotado em conformidade com o n.º 6. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 21.º

Certificados qualificados de assinatura eletrónica

1. Os certificados qualificados de assinatura eletrónica devem cumprir os requisitos estabelecidos no anexo I.

2. Os certificados qualificados de assinatura eletrónica não podem estar sujeitos a qualquer requisito obrigatório que exceda os requisitos estabelecidos no anexo I.

3. Um certificado qualificado de assinatura eletrónica que tenha sido revogado após a ativação inicial perde a validade, não podendo o seu estatuto ser revertido, em nenhuma circunstância, através da renovação da sua validade.

4. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para uma especificação mais detalhada dos requisitos estabelecidos no anexo I.

5. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos certificados qualificados de assinatura eletrónica. Um certificado qualificado de assinatura eletrónica que seja conforme com essas normas beneficia 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 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 22.º

Requisitos aplicáveis aos dispositivos de criação de assinaturas eletrónicas qualificados

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

2. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos dispositivos de criação de assinaturas eletrónicas qualificados. Um dispositivo de criação de assinaturas eletrónicas qualificado que seja conforme com essas normas beneficia da presunção de conformidade com os requisitos estabelecidos no anexo II. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 23.º

Certificação dos dispositivos de criação de assinaturas eletrónicas qualificados

1. Os dispositivos de criação de assinaturas eletrónicas qualificados podem ser certificados por entidades públicas ou privadas competentes designadas pelos Estados-Membros, desde que tenham sido submetidos a um processo de avaliação da segurança realizado de acordo com uma das normas para a avaliação da segurança dos produtos informáticos incluídas numa lista a estabelecer pela Comissão através de atos de execução. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

2. Os Estados-Membros devem notificar a Comissão e os outros Estados-Membros do nome e endereço da entidade pública ou privada por eles designada, referida no n.º 1.

3. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para o estabelecimento dos critérios específicos a cumprir pelas entidades designadas referidas no n.º 1.

Artigo 24.º

Publicação de uma lista de dispositivos de criação de assinaturas eletrónicas qualificados e certificados

1. Os Estados-Membros devem notificar à Comissão, sem atrasos indevidos, informações sobre os dispositivos de criação de assinaturas eletrónicas qualificados que tenham sido certificados pelas entidades referidas no artigo 23.º. Devem também notificar à Comissão, sem atrasos indevidos, informações sobre os dispositivos de criação de assinaturas eletrónicas que deixem de estar certificados.

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

3. A Comissão pode, através de atos de execução, definir as circunstâncias, 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 39.º, n.º 2.

Artigo 25.º

Requisitos para a validação das assinaturas eletrónicas qualificadas

1. Uma assinatura eletrónica qualificada é considerada válida caso se possa estabelecer com um elevado nível de certeza que, no momento da assinatura:

(a) o certificado, que serve de suporte à assinatura, é um certificado de assinatura eletrónica qualificado conforme com o disposto no anexo I;

(b) o certificado qualificado exigido é autêntico e válido;

(c) os dados para validação da assinatura correspondem aos dados fornecidos à parte utilizadora;

(d) o conjunto de dados que representam inequivocamente o signatário é corretamente fornecido à parte utilizadora;

(e) a utilização de um pseudónimo, se for esse o caso, é claramente indicada à parte utilizadora;

(f) a assinatura eletrónica foi criada por um dispositivo de criação de assinatura eletrónica qualificado;

(g) a integridade dos dados assinados não foi afetada;

(h) os requisitos previstos no artigo 3.º, alínea 7), estão cumpridos;

(i) o sistema utilizado para validar a assinatura fornece à parte utilizadora o resultado correto do processo de validação e permite-lhe detetar eventuais problemas de segurança pertinentes.

2. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para uma especificação mais detalhada dos requisitos estabelecidos no n.º 1.

3. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas para a validação de assinaturas eletrónicas qualificadas. A validação de assinaturas eletrónicas qualificadas que seja conforme com essas 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 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 26.º

Serviço de validação qualificado para assinaturas eletrónicas qualificadas

1. Um serviço de validação qualificado para assinaturas eletrónicas qualificadas deve ser prestado por um prestador de serviços de confiança qualificado que:

(a) efetue a validação em conformidade com o artigo 25.º, n.º 1, e

(b) permita às partes utilizadoras receber o resultado do processo de validação de um modo automático que seja fiável e eficaz e que inclua a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador do serviço de validação qualificado.

2. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas ao serviço de validação qualificado referido no n.º 1. O serviço de validação de assinaturas eletrónicas qualificadas que seja conforme com essas normas beneficia da presunção de conformidade com os requisitos estabelecidos no n.º 1, alínea b). Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 27.º

Preservação das assinaturas eletrónicas qualificadas

1. Um serviço de preservação de assinaturas eletrónicas qualificadas deve ser prestado por um prestador de serviços de confiança qualificado que utilize procedimentos e tecnologias capazes de prolongar a fiabilidade dos dados de validação das assinaturas eletrónicas qualificadas para além do prazo de validade tecnológica.

2. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para uma especificação mais detalhada dos requisitos estabelecidos no n.º 1.

3. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas à preservação de assinaturas eletrónicas qualificadas. As disposições para a

preservação de assinaturas eletrónicas qualificadas que sejam conformes com essas normas beneficiam 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 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Secção 4

Selos eletrónicos

Artigo 28.º

Efeitos legais do selo eletrónico

1. A forma eletrónica de um selo, por si só, não pode ser motivo para que lhe sejam negados efeitos legais e a admissibilidade enquanto prova em processos judiciais.

2. Um selo eletrónico qualificado beneficia da presunção legal de garantir a origem e a integridade dos dados aos quais está associado.

3. Um selo eletrónico qualificado deve ser reconhecido e aceite em todos os Estados-Membros.

4. Se for exigido um selo eletrónico com um nível de garantia de segurança inferior ao de um selo eletrónico qualificado, nomeadamente por um Estado-Membro, para aceder a um serviço em linha oferecido por um organismo público, com base numa avaliação adequada dos riscos envolvidos em tal serviço, devem ser aceites todos os selos eletrónicos que ofereçam pelo menos o mesmo nível de garantia de segurança.

5. Os Estados-Membros não poderão exigir para o acesso a um serviço em linha oferecido por um organismo do setor público um selo eletrónico com um nível de garantia de segurança superior ao dos selos eletrónicos qualificados.

6. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para a definição dos diferentes níveis de garantia de segurança dos selos eletrónicos, conforme referidos no n.º 4.

7. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos níveis de garantia de segurança dos selos eletrónicos. Um selo eletrónico conforme com essas normas beneficia da presunção de conformidade com o nível de garantia de segurança definido num ato delegado adotado nos termos do n.º 6. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 29.º

Requisitos aplicáveis aos certificados qualificados de selo eletrónico

1. Os certificados qualificados de selo eletrónico devem cumprir os requisitos estabelecidos no anexo III.

2. Os certificados qualificados de selo eletrónico não podem estar sujeitos a requisitos obrigatórios que excedam os requisitos estabelecidos no anexo III.

3. Um certificado qualificado de selo eletrónico que tenha sido revogado após a ativação inicial perde a validade, não podendo o seu estatuto ser, em nenhuma circunstância, revertido através da renovação da sua validade.

4. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para uma especificação mais detalhada dos requisitos estabelecidos no anexo III.

5. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos certificados qualificados de selo eletrónico. Um certificado qualificado de selo eletrónico que esteja conforme com essas normas beneficia da presunção de conformidade com os requisitos estabelecidos no anexo III. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Artigo 30.º

Dispositivos de criação de selo eletrónico qualificados

1. O artigo 22.º aplica-se *mutatis mutandis* aos requisitos exigidos para os dispositivos de criação de selo eletrónico qualificados.

2. O artigo 23.º aplica-se *mutatis mutandis* à certificação dos dispositivos de criação de selo eletrónico qualificados.

3. O artigo 24.º aplica-se *mutatis mutandis* à publicação da lista de dispositivos de criação de selo eletrónico qualificados certificados.

Artigo 31.º

Validação e preservação dos selos eletrónicos qualificados

Os artigos 25.º, 26.º e 27.º aplicam-se *mutatis mutandis* à validação e à preservação dos selos eletrónicos qualificados.

Secção 5

Carimbo eletrónico da hora

Artigo 32.º

Efeito legal dos carimbos eletrónicos da hora

1. A forma eletrónica de um carimbo da hora, por si só, não pode ser motivo para que lhe sejam negados efeitos legais e a admissibilidade enquanto prova em processos judiciais.

2. Um carimbo eletrónico da hora qualificado beneficia da presunção legal de garantir a hora que indica e a integridade dos dados aos quais está associado.

3. Um carimbo eletrónico da hora qualificado deve ser reconhecido e aceite em todos os Estados-Membros.

Artigo 33.º

Requisitos aplicáveis aos carimbos eletrónicos da hora qualificados

1. Um carimbo eletrónico da hora qualificado deve cumprir os seguintes requisitos:

(a) estar ligado com exatidão à Hora Universal Coordenada (UTC) de tal modo que torne impossível a alteração dos dados de forma não detetável;

(b) basear-se numa fonte horária precisa;

(c) ser emitido por um prestador de serviços de confiança qualificado;

(d) ser assinado utilizando uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador de serviços de confiança qualificado, ou por outro método equivalente.

2. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas à ligação exata da hora aos dados e a uma fonte horária precisa. Uma ligação exata da hora aos dados e uma fonte horária precisa que sejam conformes com essas normas beneficiam 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 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Secção 6

Documentos eletrónicos

Artigo 34.º

Efeitos legais e aceitação dos documentos eletrónicos

1. Um documento eletrónico deve ser considerado equivalente a um documento em papel e admissível como prova em processos judiciais, tendo em conta o seu nível de garantia de autenticidade e integridade.

2. Um documento que ostente uma assinatura eletrónica qualificada ou um selo eletrónico qualificado da pessoa competente para emitir o documento beneficia de presunção legal de autenticidade e integridade desde que não contenha características dinâmicas capazes de o alterar automaticamente.

3. Quando se exija um documento original ou uma cópia certificada para a prestação de um serviço em linha oferecido por um organismo público, serão aceites noutros Estados-Membros sem requisitos adicionais pelo menos os documentos eletrónicos emitidos pelas pessoas competentes para emitir os documentos em causa e que são considerados originais ou cópias certificadas de acordo com a legislação nacional do Estado-Membro de origem.

4. A Comissão pode, através de atos de execução, definir formatos de assinaturas e selos eletrónicos que devem ser aceites sempre que um Estado-Membro exija, para a prestação de

um serviço em linha oferecido por um organismo do setor público, um documento assinado ou selado do tipo a que se refere o n.º 2. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2.

Secção 7

Serviço de entrega eletrónica qualificado

Artigo 35.º

Efeito legal de um serviço de entrega eletrónica

1. Os dados enviados ou recebidos com recurso a um serviço de entrega eletrónica são admissíveis como prova em processos judiciais no que respeita à integridade dos dados e à certeza da data e da hora em que foram enviados ou recebidos por um destinatário especificado.

2. Os dados enviados ou recebidos com recurso a um serviço de entrega eletrónica qualificado beneficiam de presunção legal de integridade dos dados e de exatidão da data e da hora de envio ou de receção dos dados indicadas pelo sistema de entrega eletrónica qualificado.

3. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para a especificação dos mecanismos de envio ou de receção dos dados com recurso a serviços de entrega eletrónica, que devem ser utilizados tendo em vista promover a interoperabilidade destes serviços.

Artigo 36.º

Requisitos aplicáveis aos serviços de entrega eletrónica qualificados

1. Os serviços de entrega eletrónica qualificados devem satisfazer os seguintes requisitos:

(a) devem ser prestados por um ou mais prestadores de serviços de confiança qualificados;

(b) devem permitir a identificação inequívoca do remetente e, se adequado, do destinatário;

(c) o processo de envio ou de receção dos dados deve ser securizado por uma assinatura eletrónica avançada ou um selo eletrónico avançado do prestador de serviços de confiança qualificado, de modo a tornar impossível a alteração dos dados de forma não detetável;

(d) qualquer alteração dos dados necessária para o seu envio ou receção deve ser claramente indicada ao remetente e ao destinatário dos mesmos;

(e) a data do envio e da receção, assim como as eventuais alterações dos dados, devem ser indicadas através de um carimbo eletrónico da hora qualificado;

(f) caso os dados sejam transferidos entre dois ou mais prestadores de serviços de confiança qualificados, os requisitos das alíneas a) a e) aplicam-se a todos eles.

2. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos processos de envio e receção de dados. O processo de envio e receção de dados que esteja conforme com essas 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 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

Secção 8

Autenticação de sítios Web

Artigo 37.º

Requisitos aplicáveis aos certificados qualificados de autenticação de sítios Web

1. Os certificados qualificados de autenticação de sítios Web devem cumprir os requisitos estabelecidos no anexo IV.

2. Os certificados qualificados de autenticação de sítios Web devem ser reconhecidos e aceites em todos os Estados-Membros.

3. A Comissão tem poderes para adotar atos delegados, em conformidade com o artigo 38.º, para uma especificação mais detalhada dos requisitos estabelecidos no anexo IV.

4. A Comissão pode, através de atos de execução, estabelecer os números de referência das normas relativas aos certificados qualificados de autenticação de sítios Web. Um certificado qualificado de autenticação de sítio Web que esteja conforme com essas normas beneficia da presunção de conformidade com os requisitos estabelecidos no anexo IV. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 39.º, n.º 2. A Comissão publica esses atos no *Jornal Oficial da União Europeia*.

CAPÍTULO IV

ATOS DELEGADOS

Artigo 38.º

Exercício da delegação

1. É conferido à Comissão o poder para adotar atos delegados nas condições estabelecidas no presente artigo.

2. O poder para adotar atos delegados referido nos artigos 8.º, n.º 3, 13.º, n.º 5, 15.º, n.º 5, 16.º, n.º 5, 18.º, n.º 5, 20.º, n.º 6, 21.º, n.º 4, 23.º, n.º 3, 25.º, n.º 2, 27.º, n.º 2, 28.º, n.º 6, 29.º, n.º 4, 30.º, n.º 2, 31.º, 35.º, n.º 3, e 37.º, n.º 3, é conferido à Comissão por um período de tempo indeterminado a partir da data de entrada em vigor do presente regulamento.

3. A delegação de poder referida nos artigos 8.º, n.º 3, 13.º, n.º 5, 15.º, n.º 5, 16.º, n.º 5, 18.º, n.º 5, 20.º, n.º 6, 21.º, n.º 4, 23.º, n.º 3, 25.º, n.º 2, 27.º, n.º 2, 28.º, n.º 6, 29.º, n.º 4, 30.º, n.º 2, 31.º, 35.º, n.º 3, e 37.º, n.º 3, pode ser revogada em qualquer altura pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela

especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. Essa decisão em nada prejudica a validade de eventuais atos delegados já em vigor.

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

5. Um ato delegado adotado nos termos dos artigos 8.º, n.º 3, 13.º, n.º 5, 15.º, n.º 5, 16.º, n.º 5, 18.º, n.º 5, 20.º, n.º 6, 21.º, n.º 4, 23.º, n.º 3, 25.º, n.º 2, 27.º, n.º 2, 28.º, n.º 6, 29.º, n.º 4, 30.º, n.º 2, 31.º, 35.º, n.º 3, e 37.º, n.º 3, só pode entrar em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de dois meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse período, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não formularão objeções. O referido prazo é prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

CAPÍTULO V

ATOS DE EXECUÇÃO

Artigo 39.º

Procedimento de comité

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

2. Sempre que se faça referência ao presente número, é aplicável o artigo 5.º do Regulamento (UE) n.º 182/2011.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Artigo 40.º

Relatório

A Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a aplicação do presente regulamento. O primeiro relatório é apresentado o mais tardar quatro anos após a entrada em vigor do presente regulamento. Os relatórios subsequentes são apresentados com uma periodicidade de quatro anos.

Artigo 41.º

Revogação

1. A Diretiva 1999/93/CE é revogada.

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

3. Os dispositivos de criação de assinaturas seguros, cuja conformidade tenha sido determinada nos termos do artigo 3.º, n.º 4, da Diretiva 1999/93/CE, são considerados dispositivos de criação de assinaturas qualificados por força do presente regulamento.

4. Os certificados qualificados emitidos em conformidade com a Diretiva 1999/93/CE são considerados certificados qualificados para assinaturas eletrónicas por força do presente regulamento até caducarem, mas durante não mais do que cinco anos a contar da data de entrada em vigor do presente regulamento.

Artigo 42.º

Entrada em vigor

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

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

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

ANEXO I

Requisitos aplicáveis aos certificados qualificados de assinaturas eletrónicas

Os certificados qualificados de assinaturas eletrónicas devem conter:

(a) uma indicação, pelo menos numa forma adequada ao tratamento automático, de que o certificado foi emitido como certificado qualificado de assinatura eletrónica;

(b) um conjunto de dados que representem inequivocamente o prestador de serviços de confiança qualificado que emitiu os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontra estabelecido e

- para uma pessoa coletiva: o nome e o número de registo conforme constam dos registos oficiais;
- para uma pessoa singular: o nome da pessoa;

(c) um conjunto de dados que representem inequivocamente o signatário para o qual o certificado é emitido, incluindo, pelo menos, o nome do signatário ou um pseudónimo, que deve ser identificado como tal;

(d) os dados necessários para a validação da assinatura eletrónica que correspondam aos dados necessários para a criação da assinatura eletrónica;

(e) informações sobre o início e o termo do prazo de validade do certificado;

(f) o código de identidade do certificado, que deve ser único para o prestador de serviços de confiança qualificado;

(g) a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador de serviços de confiança qualificado emitente;

(h) o local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado referidos na alínea g);

(i) a localização dos serviços que conferem o estatuto de válido ao certificado e que podem ser utilizados para inquirir do estado de validade do certificado qualificado;

(j) se os dados para criação da assinatura eletrónica relacionados com os dados para validação da assinatura eletrónica estiverem localizados num dispositivo de criação de assinatura eletrónica qualificado, uma indicação adequada desse facto, pelo menos numa forma adequada para tratamento automático.

ANEXO II

Requisitos aplicáveis aos dispositivos de criação de assinaturas qualificados

1. Os dispositivos de criação de assinaturas eletrónicas qualificados devem assegurar, através de meios técnicos e procedimentais adequados, que pelo menos:

(a) a confidencialidade dos dados necessários para a criação de uma assinatura eletrónica utilizados para criar uma assinatura eletrónica está assegurada;

(b) os dados necessários para a criação de uma assinatura eletrónica utilizados para gerar uma assinatura eletrónica apenas possam ocorrer uma vez;

(c) os dados necessários para a criação de uma assinatura eletrónica utilizados para a geração de uma assinatura eletrónica não possam, com uma segurança razoável, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através de tecnologias atualmente disponíveis;

(d) os dados necessários para a criação de uma assinatura eletrónica utilizados para a geração de uma assinatura eletrónica possam ser eficazmente protegidos pelo signatário legítimo contra a utilização por terceiros.

2. Os dispositivos de criação de assinaturas eletrónicas qualificados não podem alterar os dados a assinar nem impedir que esses dados sejam apresentados ao signatário antes da assinatura.

3. A geração ou a gestão, em nome do signatário, dos dados necessários para a criação de uma assinatura eletrónica devem ser efetuadas por um prestador de serviços de confiança qualificado.

4. Os prestadores de serviços de confiança qualificados que gerem os dados necessários para a criação de uma assinatura eletrónica em nome do signatário podem duplicar esses dados para fins de cópia de segurança, desde que sejam cumpridos os seguintes requisitos:

(a) a segurança dos conjuntos de dados duplicados deve estar ao mesmo nível da dos conjuntos de dados originais;

(b) o número de conjuntos de dados duplicados não pode exceder o mínimo necessário para garantir a continuidade do serviço.

ANEXO III

Requisitos aplicáveis aos certificados qualificados de selos eletrónicos

Os certificados qualificados de selos eletrónicos devem conter:

(a) uma indicação, pelo menos numa forma adequada para tratamento automático, de que o certificado foi emitido como certificado qualificado de selo eletrónico;

(b) um conjunto de dados que representem inequivocamente o prestador de serviços de confiança qualificado que emitiu os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontra estabelecido e

- para uma pessoa coletiva: o nome e o número de registo conforme constam dos registos oficiais;
- para uma pessoa singular: o nome da pessoa;

(c) um conjunto de dados que representem inequivocamente a pessoa coletiva para a qual o certificado é emitido, incluindo, pelo menos, o nome e o número de registo conforme constam dos registos oficiais;

(d) os dados necessários para a validação do selo eletrónico que correspondam aos dados necessários para a criação do selo eletrónico;

(e) informações sobre o início e o termo do prazo de validade do certificado;

(f) o código de identidade do certificado, que deve ser único para o prestador de serviços de confiança qualificado;

(g) a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador de serviços de confiança qualificado emitente;

(h) o local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado referidos na alínea g);

(i) a localização dos serviços que conferem o estatuto de válido ao certificado e que podem ser utilizados para inquirir do estado de validade do certificado qualificado;

(j) se os dados para criação do selo eletrónico relacionados com os dados para validação do selo eletrónico estiverem localizados num dispositivo de criação de selo eletrónico qualificado, uma indicação adequada desse facto, pelo menos numa forma adequada ao tratamento automático.

ANEXO IV

Requisitos aplicáveis aos certificados qualificados de autenticação de sítios Web

Os certificados qualificados de autenticação de sítios Web devem conter:

(a) uma indicação, pelo menos numa forma adequada ao tratamento automático, de que o certificado foi emitido como certificado qualificado de autenticação de sítio Web;

(b) um conjunto de dados que representem inequivocamente o prestador de serviços de confiança qualificado que emitiu os certificados qualificados, incluindo, pelo menos, o Estado-Membro em que esse prestador se encontra estabelecido e

- para uma pessoa coletiva: o nome e o número de registo conforme constam dos registos oficiais;
- para uma pessoa singular: o nome da pessoa;

(c) um conjunto de dados que representem inequivocamente a pessoa coletiva para a qual o certificado é emitido, incluindo, pelo menos, o nome e o número de registo conforme constam dos registos oficiais;

(d) elementos do endereço, incluindo, pelo menos, a cidade e o Estado-Membro, da pessoa coletiva para a qual o certificado é emitido, conforme constam dos registos oficiais;

(e) o nome ou os nomes de domínio explorados pela pessoa coletiva para a qual o certificado é emitido;

(f) informações sobre o início e o termo do prazo de validade do certificado;

(g) o código de identidade do certificado, que deve ser único para o prestador de serviços de confiança qualificado;

(h) a assinatura eletrónica avançada ou o selo eletrónico avançado do prestador de serviços de confiança qualificado emitente;

(i) o local em que está disponível, a título gratuito, o certificado que sustenta a assinatura eletrónica avançada ou o selo eletrónico avançado referidos na alínea h);

(j) a localização dos serviços que conferem o estatuto de válido ao certificado e que podem ser utilizados para inquirir do estado de validade do certificado qualificado.

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

A presente ficha financeira especifica as necessidades em termos de despesa administrativa para dar execução ao regulamento proposto relativo à *identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno*.

Após o processo legislativo e as discussões para a adoção pelo PE e pelo Conselho do regulamento proposto, a Comissão terá necessidade de doze equivalentes tempo inteiro (ETI) para conceber os atos delegados e de execução correspondentes, para garantir a disponibilidade de normas organizacionais e técnicas, para tratar as informações notificadas pelos Estados-Membros, e nomeadamente para manter atualizadas as informações ligadas às listas de confiança, para sensibilizar as partes interessadas – em particular os cidadãos e as PME – para as vantagens da utilização da identificação, da autenticação e das assinaturas eletrónicas e dos serviços de confiança conexos (*eIAS*) e para travar discussões com países terceiros tendo em vista assegurar a interoperabilidade dos *eIAS* a nível mundial.

1.1. Denominação da proposta/iniciativa

Proposta da Comissão de um regulamento relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno

1.2. Domínio(s) de intervenção envolvido(s) de acordo com a estrutura ABM/ABB[25]

09 SOCIEDADE DA INFORMAÇÃO

1.3. Natureza da proposta/iniciativa

☐ A proposta/iniciativa refere-se a **uma nova ação**

☐ A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**[26]

☐ A proposta/iniciativa refere-se à **prorrogação de uma ação existente**

☑ A proposta/iniciativa refere-se a **uma ação reorientada para uma nova ação**

1.4. Objetivos

1.4.1. Objetivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa

Os objetivos gerais da proposta são os das políticas gerais da UE nas quais a proposta se insere, tais como a Estratégia UE 2020. A estratégia UE 2020 visa transformar a

25 ABM: *Activity Based Management* (gestão por atividades) – ABB: *Activity Based Budgeting* (orçamentação por atividades).

26 Referidos no artigo 49.º, n.º 6, alíneas a) e b), do Regulamento Financeiro.

UE numa «economia inteligente, sustentável e inclusiva, que proporcione níveis elevados de emprego, de produtividade e de coesão social».

1.4.2. Objetivo(s) específico(s) e atividade(s) ABM/ABB em causa

Reforçar a confiança nas transações eletrónicas pan-europeias e garantir o reconhecimento legal transfronteiras da identificação, da autenticação e das assinaturas eletrónicas e dos serviços de confiança conexos, assim como um elevado nível de proteção dos dados e de autonomia dos utilizadores no mercado único (ver Agenda Digital para a Europa, ações-chave 3 e 16).

Atividade(s) ABM/ABB em causa

09 02 - Quadro regulamentar da Agenda Digital para a Europa

1.4.3. Resultados e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada

A proposta estabelecerá um ambiente regulamentar claro para os serviços eIAA que facilitará a tarefa para os utilizadores e promoverá a confiança no mundo digital.

1.4.4. Indicadores de resultados e de impacto

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.

1. Existência de fornecedores de *eIAS* que exercem atividades em vários Estados-Membros da UE;

2. Grau de interoperabilidade atingido pelos dispositivos (por exemplo, leitores de cartões) entre setores e países;

3. Utilização dos *eIAS* por todas as categorias de população;

4. O grau de utilização dos *eIAS* pelos utilizadores finais para transações nacionais e internacionais (entre Estados-Membros);

5. Grau de harmonização da legislação sobre os *eIAS* nos diversos Estados-Membros;

6. Sistemas de identificação eletrónica notificados à Comissão;

7. Serviços do setor público acessíveis através de meios de identificação eletrónica notificados (por exemplo, administração pública em linha, saúde em linha, justiça em linha, contratos públicos eletrónicos);

8. Serviços do setor privado acessíveis através de meios de identificação eletrónica notificados (por exemplo, serviços bancários em linha, comércio eletrónico, jogos de azar em linha, acesso a sítios Web, serviços de Internet mais segura).

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo

As divergências na aplicação da diretiva relativa às assinaturas eletrónicas ao nível nacional devido às diferentes interpretações da mesma pelos Estados-Membros causam problemas de interoperabilidade transfronteiras, acabando por criar uma paisagem segmentada na UE e distorções no mercado interno. A essas divergências

há que juntar a falta de confiança nos sistemas eletrónicos, que impede os cidadãos europeus de beneficiarem, no mundo digital, do mesmo tipo de serviços que no mundo físico.

1.5.2. Valor acrescentado da participação da UE

Uma ação a nível da UE terá vantagens nítidas em relação às ações individuais dos Estados-Membros. A experiência mostra, na verdade, que as medidas nacionais não só são insuficientes para tornar as transações eletrónicas possíveis a nível transfronteiras, como criam, pelo contrário, barreiras à interoperabilidade das assinaturas eletrónicas em toda a UE, efeito esse que atualmente se faz sentir também a nível da identificação e da autenticação eletrónicas e dos serviços de confiança conexos.

1.5.3. Lições tiradas de experiências anteriores semelhantes

A presente proposta baseia-se na experiência adquirida com a Diretiva «Assinaturas Eletrónicas» e tem em conta os problemas suscitados pela transposição e a aplicação fragmentadas dessa diretiva, que impediram que os seus objetivos fossem atingidos.

1.5.4. Coerência e eventual sinergia com outros instrumentos relevantes

A Diretiva «Assinaturas Eletrónicas» é referenciada por várias outras iniciativas da UE cujo objetivo é eliminar os problemas de interoperabilidade e de reconhecimento e aceitação transfronteiras ligados a certos tipos de interações eletrónicas, nomeadamente a Diretiva «Serviços», as diretivas relativas aos contratos públicos, a Diretiva (na última versão revista) relativa ao IVA (faturas eletrónicas) ou o Regulamento relativo à Iniciativa Europeia de Cidadania.

Além disso, o regulamento proposto oferecerá um quadro legal propício à adoção generalizada dos projetos-piloto de grande escala que foram implantados a nível da UE para apoiar o desenvolvimento de meios de comunicação eletrónica interoperáveis e fiáveis (nomeadamente a iniciativa SPOCS, que apoia a implementação da Diretiva «Serviços», o projeto STORK, que apoia o desenvolvimento e a utilização de sistemas de identificação eletrónica interoperáveis, o projeto PEPPOL, que apoia o desenvolvimento e a utilização de soluções interoperáveis em matéria de contratos públicos eletrónicos, o projeto epSOS, que apoia o desenvolvimento e a utilização de soluções interoperáveis em matéria de saúde em linha, e o projeto eCodex, que apoia o desenvolvimento e a utilização de soluções interoperáveis em matéria de justiça em linha).

1.6. Duração da ação e do seu impacto financeiro

☐ Proposta/iniciativa de **duração limitada**

– ☐ Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA

☑ Proposta/iniciativa de **duração ilimitada**

1.7. Modalidade(s) de gestão prevista(s)[27]

☑ **Gestão centralizada direta** por parte da Comissão

☐ **Gestão centralizada indireta** por delegação de funções de execução em:

– ☐ agências de execução

– ☐ organismos criados pelas Comunidades[28]

– ☐ organismos públicos nacionais/organismos com missão de serviço público

– ☐ pessoas encarregadas da execução de ações específicas por força do Título V do Tratado da União Europeia, identificadas no ato de base pertinente na aceção do artigo 49.º do Regulamento Financeiro

☐ **Gestão partilhada** com os Estados-Membros

☐ **Gestão descentralizada** com países terceiros

☐ **Gestão conjunta** com organizações internacionais ***(a especificar)***

Se for indicada mais de uma modalidade de gestão, especificar na secção «Observações».

Observações:

[//]

[27] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[28] Referidos no artigo 185.º do Regulamento Financeiro.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições.

A primeira avaliação terá lugar quatro anos após a entrada em vigor do regulamento. O regulamento inclui um artigo específico intitulado "Relatório", que obriga a Comissão a apresentar ao Parlamento Europeu e ao Conselho um relatório sobre a sua aplicação. Os relatórios subsequentes devem ser apresentados com uma periodicidade de quatro anos. A Comissão aplicará os seus métodos de avaliação. Estas avaliações devem ser efetuadas com a ajuda de estudos específicos relativos à execução dos instrumentos legais, questionários às autoridades nacionais, debates com especialistas, sessões de trabalho, inquéritos Eurobarómetro, entre outros.

2.2. Sistema de gestão e de controlo

2.2.1. Risco(s) identificado(s)

A proposta de regulamento é acompanhada de uma avaliação de impacto. O novo instrumento legal assegurará o reconhecimento e a aceitação mútuos da identificação eletrónica a nível transfronteiras, melhorará o atual quadro das assinaturas eletrónicas, reforçando a supervisão nacional dos prestadores de serviços de confiança, e conferirá efeitos legais e reconhecimento legal aos serviços de confiança conexos. Além disso, prevê o recurso a atos delegados e de execução como mecanismo para garantir flexibilidade perante a evolução tecnológica.

2.2.2. Meios de controlo previstos

Os meios de controlo existentes aplicados pela Comissão cobrirão as dotações adicionais.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas.

Os meios de prevenção da fraude existentes aplicados pela Comissão cobrirão as dotações adicionais.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)

- Atuais rubricas orçamentais de despesas

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Natureza das despesas	Participação			
	Número [Designação…...….]	DD/DND (29)	dos países da EFTA 30	de países candidatos 31	de países terceiros	na aceção do artigo 18.º, n.º 1, alínea a-a), do Regulamento Financeiro
5	09. 01 01 01 Despesas com pessoal no ativo na DG «Sociedade da Informação e *Media*»	DND	NÃO	NÃO	NÃO	NÃO
5	09. 01 02 01 Pessoal externo	DND	NÃO	NÃO	NÃO	NÃO

29 DD = dotações diferenciadas/DND = dotações não diferenciadas.

30 EFTA: Associação Europeia de Comércio Livre.

31 Países candidatos e, se for o caso, potenciais países candidatos dos Balcãs Ocidentais.

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

Rubrica do quadro financeiro plurianual:	**Número**	[Rubrica 1. - **Crescimento inteligente e inclusivo** ……..……]

DG: INFSO			Ano **2014**	Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Ano **2019**	Ano **2020**	**TOTAL**
• Dotações operacionais										
Número da rubrica orçamental – N.A.	Autorizações	(1)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Pagamentos	(2)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
Número da rubrica orçamental – N.A.	Autorizações	(1a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Pagamentos	(2a)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
Dotações de natureza administrativa financiadas a partir da dotação para programas específicos[32]			0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0,000**
Número da rubrica orçamental		(3)	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
TOTAL das dotações para a DG INFSO	Autorizações	=1+1a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**
	Pagamentos	=2+2a +3	0,000	0,000	0,000	0,000	0,000	0,000	**0,000**	**0.000**

[32] Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

Rubrica do quadro financeiro plurianual:	**5**	«Despesas administrativas»

Em milhões de euros (3 casas decimais)

		Ano **2014**	Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Ano **2019**	Ano **2020**	**TOTAL**
		DG: INFSO							
• Recursos humanos		1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
• Outras despesas de natureza administrativa									
TOTAL DG INFSO	Dotações	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

TOTAL das dotações no âmbito da RUBRICA 5 do quadro financeiro plurianual	(Total das autorizações = Total dos pagamentos)	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Em milhões de euros (3 casas decimais)

		Ano **2014**	Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Ano **2019**	Ano **2020**	**TOTAL**
TOTAL das dotações no âmbito das RUBRICAS 1 a 5 do quadro financeiro plurianual	Autorizações	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
	Pagamentos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

3.2.2. Impacto estimado nas dotações operacionais

– ☑ A proposta/iniciativa não acarreta a utilização de dotações operacionais

– ☐ A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

3.2.3. Impacto estimado nas dotações de natureza administrativa

3.2.3.1. Síntese

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– ☑ A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de euros (3 casas decimais)

	Ano **N 2014**	Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Ano **2019**	Ano **2020**	**TOTAL**
RUBRICA 5 do quadro financeiro plurianual								
Recursos humanos	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**
Outras despesas de natureza administrativa								
Subtotal RUBRICA 5 do quadro financeiro plurianual	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

Com exclusão da RUBRICA 5[33] do quadro financeiro plurianual								
Recursos humanos								
Outras despesas de natureza administrativa								
Subtotal com exclusão da RUBRICA 5 do quadro financeiro plurianual								

TOTAL	1,344	1,344	1,344	1,344	1,344	1,344	1,344	**9,408**

[33] Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

3.2.3.2. Necessidades estimadas de recursos humanos

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos

– ☑ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em números inteiros (ou, no máximo, com uma casa decimal)

	Ano **2014**	Ano **2015**	Ano **2016**	Ano **2017**	Ano **2018**	Ano **2019**	Ano **2020**
• Lugares do quadro do pessoal (postos de funcionários e de agentes temporários)							
09 01 01 01 (na sede e nos gabinetes de representação da Comissão)	9	9	9	9	9	9	9
XX 01 01 02 (nas delegações)							
XX 01 05 01 (investigação indireta)							
10 01 05 01 (Investigação direta)							
• Pessoal externo (em equivalente a tempo inteiro: ETI)[34]							
09 01 02 01 (AC, TT, PND da dotação global)	3	3	3	3	3	3	3
XX 01 02 02 (AC, TT, JPD, AL e PND nas delegações)							
XX 01 04 *yy*[35] - na sede[36]							
XX 01 04 *yy* - nas delegações							
XX 01 05 02 (AC, TT, PND - Investigação indireta)							
10 01 05 02 (AC, TT, PND - Investigação direta)							
Outra rubrica orçamental (especificar)							
TOTAL	**12**	**12**	**12**	**12**	**12**	**12**	**12**

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	Gerir os processos legislativos para a adoção pelo PE e pelo Conselho do regulamento previsto e dos atos delegados/de execução com ele relacionados. Domínios prioritários: 1. Estabelecimento de um novo quadro legislativo para os serviços eletrónicos de confiança

34 AC = Agente Contratual; TT = trabalhador temporário; JPD= jovem perito nas delegações; AL= Agente Local; PND = perito nacional destacado.

35 Dentro do limite para o pessoal externo previsto nas dotações operacionais (antigas rubricas «BA»).

36 Essencialmente os fundos estruturais, o Fundo Europeu Agrícola de Desenvolvimento Rural (FEADER) e o Fundo Europeu das Pescas (FEP).

	2. Promoção da aceitação dos serviços eletrónicos de confiança através da sensibilização das PME e dos cidadãos para o seu potencial 3. Acompanhamento da Diretiva 1999/93/CE, incluindo os aspetos internacionais 4. Potenciar os projetos-piloto de grande escala a fim de acelerar a realização concreta do objetivo do novo quadro legislativo.
Pessoal externo	Idem (como acima)

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

– ☑ A proposta/iniciativa é compatível com o atual quadro financeiro plurianual

– ☐ A proposta/iniciativa requer uma reprogramação da rubrica pertinente do quadro financeiro plurianual

Explicitar a reprogramação necessária, especificando as rubricas orçamentais em causa e as quantias correspondentes.

– ☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual[37].

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes.

3.2.5. Participação de terceiros no financiamento

– ☑ A proposta/iniciativa não prevê o cofinanciamento por terceiros

– ☐ A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

3.3. Impacto estimado nas receitas

– ☑ A proposta/iniciativa não tem impacto financeiro nas receitas

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

- ☐ nos recursos próprios
- ☐ nas receitas diversas

[37] Ver pontos 19 e 24 do Acordo Interinstitucional.