REGULAMENTO DELEGADO (UE) 2018/389 DA COMISSÃO

de 27 de novembro de 2017

que complementa a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta a Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE ([1]), nomeadamente o artigo 98.º, n.º 4, segundo parágrafo,

Considerando o seguinte:

(1) Os serviços de pagamento oferecidos por via eletrónica devem ser prestados de forma segura, adotando tecnologias suscetíveis de garantir a autenticação segura do utilizador e de reduzir, tanto quanto possível, o risco de fraude. O procedimento de autenticação deve incluir, de um modo geral, mecanismos de controlo das operações para detetar tentativas de utilização das credenciais de segurança personalizadas de um utilizador de um serviço pagamento que tenham sido perdidas, furtadas ou objeto de apropriação abusiva, e deve igualmente assegurar que o utilizador do serviço de pagamento é o utilizador legítimo, e, nessa qualidade, consente a transferência de fundos e o acesso à informação sobre a sua conta através de uma utilização normal das credenciais de segurança personalizadas. Além disso, é necessário especificar os requisitos da autenticação forte do cliente aplicáveis sempre que um ordenante acede em linha à sua conta de pagamento, inicia uma operação de pagamento eletrónico ou realiza uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou outros abusos, exigindo a geração de um código de autenticação que exclua o risco de falsificação em todos os seus elementos ou de divulgação de qualquer um dos elementos que serviu de base à sua geração.

(2) Dada a constante mutação dos métodos de fraude, os requisitos da autenticação forte do cliente devem abrir caminho à inovação nas soluções técnicas de resposta à emergência de novas ameaças para a segurança dos pagamentos eletrónicos. A fim de garantir a aplicação eficaz e contínua dos requisitos a estabelecer, importa também exigir que as medidas de segurança para a aplicação da autenticação forte do cliente e das suas isenções, as medidas de proteção da confidencialidade e da integridade das credenciais de segurança personalizadas e as medidas que estabelecem normas abertas de comunicação comuns e seguras sejam documentadas, periodicamente testadas, avaliadas e auditadas por auditores especializados em segurança informática e pagamentos eletrónicos e operacionalmente independentes. A fim de permitir que as autoridades competentes controlem a qualidade da avaliação destas medidas, tais avaliações devem, a seu pedido, ser-lhes disponibilizadas.

(3) Dado que as operações de pagamento eletrónico remotas estão sujeitas a um maior risco de fraude, é necessário introduzir requisitos adicionais para a autenticação forte do cliente de tais operações, assegurando que, no início da operação, os elementos a associem de forma dinâmica a um montante e a um beneficiário especificado pelo ordenante.

(4) A ligação dinâmica é possível através de uma geração de códigos de autenticação que esteja sujeita a um conjunto de requisitos estritos de segurança. A fim de manter a neutralidade tecnológica, não deve ser exigida uma tecnologia específica para a implementação dos códigos de autenticação. Assim, os códigos de autenticação devem basear-se em soluções como a geração e validação de senhas de utilização única, assinaturas digitais ou outras asserções de validade de base criptográfica que utilizem chaves ou material criptográfico armazenado nos elementos de autenticação, desde que sejam cumpridos os requisitos de segurança.

([1]) JO L 337 de 23.12.2015, p. 35.

(5) É necessário estabelecer requisitos específicos para o caso de o montante final não ser conhecido no momento em que o ordenante inicia uma operação de pagamento eletrónico remota, de modo a assegurar que a autenticação forte do cliente corresponde ao montante máximo consentido pelo ordenante nos termos da Diretiva (UE) 2015/2366.

(6) A fim de assegurar a implementação da autenticação forte do cliente, é também necessário impor características de segurança adequadas para os elementos da autenticação forte do cliente pertencentes à categoria do conhecimento (algo que só o utilizador conhece), como a extensão ou a complexidade, para os elementos pertencentes à categoria da posse (algo que só o utilizador possui), como especificações algorítmicas, o comprimento da chave e a entropia informacional, e para os dispositivos e *software* que leiam elementos pertencentes à categoria da inerência (algo que o utilizador é), como especificações algorítmicas, características de proteção baseada em sensores biométricos e modelos, nomeadamente para reduzir o risco de estes elementos serem descobertos, divulgados junto de partes não autorizadas e por elas utilizados. É ainda necessário estabelecer requisitos que assegurem a independência destes elementos, de modo que a violação de um deles não comprometa a fiabilidade dos restantes, em especial quando um destes elementos seja utilizado através de um dispositivo multifuncional, como um tablete ou um telemóvel, suscetível de ser utilizado tanto para dar a instrução de realização do pagamento como no processo de autenticação.

(7) Os requisitos da autenticação forte do cliente aplicam-se aos pagamentos iniciados pelo ordenante, independentemente de este ser uma pessoa singular ou uma pessoa coletiva.

(8) Pela sua própria natureza, os pagamentos efetuados através de instrumentos de pagamento anónimos não estão sujeitos à obrigação de autenticação forte do cliente. Caso o anonimato de tais instrumentos seja levantado por motivos contratuais ou legislativos, os pagamentos ficam sujeitos aos requisitos de segurança que decorrem da Diretiva (UE) 2015/2366 e das presentes normas técnicas de regulamentação.

(9) Em conformidade com a Diretiva (UE) 2015/2366, as isenções do princípio da autenticação forte do cliente foram definidas com base no nível de risco, no montante, na recorrência e no canal de pagamento utilizado para a execução da operação de pagamento.

(10) As ações que implicam o acesso ao saldo e às operações recentes de uma conta de pagamento sem a divulgação de dados de pagamento sensíveis, de pagamentos recorrentes aos mesmos beneficiários previamente criados ou confirmados pelo ordenante com a utilização da autenticação forte do cliente e de pagamentos para e por uma mesma pessoa singular ou coletiva que tenha contas com o mesmo prestador de serviços de pagamento apresentam um baixo nível de risco, permitindo assim que os prestadores de serviços de pagamento não apliquem a autenticação forte do cliente. Tal não obsta a que, nos termos dos artigos 65.º, 66.º e 67.º da Diretiva (UE) 2015/2366, os prestadores de serviços de iniciação de pagamentos, os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões e os prestadores de serviços de informação sobre contas apenas devam solicitar e obter informações essenciais junto do prestador de serviços de pagamento gestor de contas para prestarem um determinado serviço de pagamento com o consentimento do utilizador de serviços de pagamento. Esse consentimento pode ser dado individualmente, para cada pedido de informações ou para cada pagamento a iniciar, ou, quando é dado aos prestadores de serviços de informação sobre contas, a título de autorização aplicável a contas de pagamento designadas e às operações de pagamento associadas, tal como estabelecido no contrato com o utilizador de serviços de pagamento.

(11) As isenções relativas aos pagamentos sem contacto de baixo valor em pontos de venda, tendo igualmente em conta um número máximo de operações consecutivas ou um determinado valor máximo fixo de operações consecutivas sem aplicação da autenticação forte do cliente, permitem o desenvolvimento de serviços de pagamento de fácil utilização e de baixo risco, devendo, por isso, ser contempladas. Convém também estabelecer uma isenção para as operações de pagamento eletrónico iniciadas em terminais não assistidos, nas quais a autenticação forte do cliente pode nem sempre ser fácil de aplicar por razões operacionais (por exemplo, para evitar filas de espera e potenciais acidentes em guichets de portagem ou outros riscos de segurança).

(12) De forma análoga à isenção aplicável aos pagamentos sem contacto de baixo valor nos pontos de venda, é necessário obter um equilíbrio adequado entre o interesse do reforço da segurança dos pagamentos remotos e as necessidades de acessibilidade e facilidade dos pagamentos no domínio do comércio eletrónico. Em sintonia com estes princípios, os limiares abaixo dos quais não é necessário aplicar a autenticação forte do cliente devem ser fixados com prudência, de modo a cobrir apenas compras em linha de baixo valor. Os limiares aplicáveis às compras em linha devem ser fixados de forma mais prudente, porquanto o facto de a pessoa não estar fisicamente presente quando efetua a compra aumenta ligeiramente o risco de segurança.

(13) Os requisitos da autenticação forte do cliente aplicam-se aos pagamentos iniciados pelo ordenante, independentemente de este ser uma pessoa singular ou uma pessoa coletiva. Muitos dos pagamentos efetuados por empresas são iniciados através de processos ou protocolos dedicados que garantem os elevados níveis de segurança dos pagamentos que a Diretiva (UE) 2015/2366 visa alcançar mediante a autenticação forte do cliente. Caso as autoridades competentes considerem que os processos e protocolos de pagamento disponibilizados apenas a ordenantes que não sejam consumidores alcançam os objetivos da Diretiva (UE) 2015/2366 em termos de segurança, os prestadores de serviços de pagamento podem, relativamente a tais processos ou protocolos, ficar isentos dos requisitos da autenticação forte do cliente.

(14) Caso a análise de risco das operações em tempo real classifique uma operação de pagamento como sendo de baixo risco, convém introduzir uma isenção para o prestador de serviços de pagamento que tencione não aplicar a autenticação forte do cliente, através da adoção de requisitos eficazes e baseados no risco que garantam a segurança dos fundos e dos dados pessoais do utilizador de serviços de pagamento. Esses requisitos baseados no risco devem combinar os resultados da análise de risco, confirmando a ausência de despesas ou padrões de comportamento anormais do ordenante e tendo em conta outros fatores de risco, nomeadamente as informações sobre a localização do ordenante e do beneficiário, com limiares monetários baseados nas taxas de fraude calculadas para os pagamentos remotos. Se, com base na análise de risco das operações em tempo real, não for possível classificar uma operação de pagamento como apresentando um baixo nível de risco, o prestador de serviços de pagamento deve voltar a aplicar a autenticação forte do cliente. O valor máximo da isenção baseada no risco deve ser fixado de modo a garantir uma taxa de fraude correspondente muito baixa, também em comparação com as taxas de fraude de todas as operações de pagamento do prestador de serviços de pagamento, incluindo as autenticadas por autenticação forte do cliente, dentro de um determinado prazo e de forma contínua.

(15) A fim de assegurar uma execução eficaz, os prestadores de serviços de pagamento que pretendam beneficiar das isenções da autenticação forte do cliente devem controlar e disponibilizar regularmente às autoridades competentes e à Autoridade Bancária Europeia (ABE), a seu pedido, e por cada tipo de operação de pagamento, o valor das operações de pagamento fraudulentas ou não autorizadas e as taxas de fraude observadas na totalidade das suas operações de pagamento, sejam elas autenticadas por autenticação forte do cliente ou executadas ao abrigo de uma isenção aplicável.

(16) A recolha destes novos dados históricos sobre as taxas de fraude nas operações de pagamento eletrónico contribuirá igualmente para uma revisão eficaz pela EBA dos limiares para a isenção da autenticação forte do cliente, com base numa análise de risco das operações em tempo real. A fim de reforçar a segurança dos pagamentos eletrónicos remotos, a EBA deve rever e apresentar à Comissão projetos de atualização das presentes normas técnicas de regulamentação, se for caso disso, mediante a apresentação de novos projetos de limiares e das correspondentes taxas de fraude, em conformidade com o artigo 98.º, n.º 5, da Diretiva (UE) 2015/2366 e o artigo 10.º do Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([1]).

(17) Os prestadores de serviços de pagamento que apliquem qualquer uma das isenções a prever devem poder, em qualquer momento, optar por aplicar a autenticação forte do cliente às ações e às operações de pagamento referidas nessas disposições.

(18) As medidas de proteção da confidencialidade e da integridade das credenciais de segurança personalizadas, bem como os dispositivos e *software* de autenticação, devem limitar os riscos de fraude associados à utilização fraudulenta ou não autorizada de instrumentos de pagamento e ao acesso não autorizado a contas de pagamento. Para este efeito, é necessário introduzir requisitos sobre a geração e o fornecimento seguros das credenciais de segurança personalizadas e a sua associação ao utilizador de serviços de pagamento, bem como criar condições para a renovação e desativação dessas credenciais.

(19) A fim de garantir a eficácia e a segurança da comunicação entre os intervenientes relevantes no contexto dos serviços de informação sobre contas, dos serviços de iniciação de pagamentos e da confirmação da disponibilidade de fundos, é necessário especificar os requisitos em matéria de normas abertas de comunicação comuns e seguras a cumprir por todos os prestadores de serviços de pagamento em causa. A Diretiva (UE) 2015/2366 prevê o acesso e a utilização das informações sobre contas de pagamento por parte dos prestadores de serviços de informação sobre contas. Por conseguinte, o presente regulamento não altera as regras de acesso a outras contas além das de pagamento.

([1]) Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331 de 15.12.2010, p. 12).

(20) Cada prestador de serviços de pagamento gestor de contas que tenha contas de pagamento acessíveis em linha deve oferecer pelo menos uma interface de acesso que permita uma comunicação segura com os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões. A interface deve permitir que os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões se identifiquem junto do prestador de serviços de pagamento gestor de contas. De igual modo, a interface deve permitir que os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos se baseiem nos procedimentos de autenticação facultados pelo prestador de serviços de pagamento gestor de contas ao utilizador de serviços de pagamento. A fim de assegurar a neutralidade tecnológica e do modelo de negócio, os prestadores de serviços de pagamento que gerem as contas devem ser livres de decidir se oferecem uma interface dedicada à comunicação com os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões, ou se permitem, para essa comunicação, a utilização da interface para efeitos de identificação e comunicação com os utilizadores de serviços de pagamento dos prestadores de serviços de pagamento gestores de contas.

(21) A fim de permitir que os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões desenvolvam as suas soluções técnicas, as especificações técnicas da interface devem ser devidamente documentadas e tornadas públicas. Além disso, o prestador de serviços de pagamento gestor de contas deve disponibilizar um mecanismo que permita aos prestadores de serviços de pagamento testarem as soluções técnicas pelo menos seis meses antes da data de aplicação das presentes normas de regulamentação ou, se o lançamento ocorrer após a referida data de aplicação, antes da data do lançamento da interface no mercado. A fim de assegurar a interoperabilidade das diferentes soluções tecnológicas de comunicação, a interface deve aplicar normas de comunicação formuladas por organizações de normalização internacionais ou europeias.

(22) A qualidade dos serviços prestados pelos prestadores de serviços de informação sobre contas e pelos prestadores de serviços de iniciação de pagamentos depende do bom funcionamento das interfaces criadas ou adaptadas pelos prestadores de serviços de pagamento gestor de contas. Deste modo, importa que, caso essas interfaces não cumpram as disposições incluídas nas presentes normas, sejam tomadas medidas para assegurar a continuidade das atividades em benefício dos utilizadores desses serviços. Cabe às autoridades nacionais competentes garantir que os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos não enfrentam bloqueios nem obstáculos na prestação dos seus serviços.

(23) Caso o acesso a contas de pagamento seja oferecido por intermédio de uma interface dedicada, a fim de garantir o direito dos utilizadores de serviços de pagamento de recorrerem a prestadores de serviços de iniciação de pagamentos e a serviços que permitam o acesso a informação sobre contas, conforme previsto na Diretiva (UE) 2015/2366, é necessário exigir que as interfaces dedicadas tenham o mesmo nível de disponibilidade e desempenho da interface disponibilizada ao utilizador de serviços de pagamento. Os prestadores de serviços de pagamento gestores de contas devem também definir indicadores de desempenho fundamentais e objetivos de nível de serviço transparentes no que toca à disponibilidade e ao desempenho das interfaces dedicadas, devendo tais indicadores e objetivos ser pelo menos tão exigentes como os da interface disponibilizada aos utilizadores de serviços de pagamento desses prestadores. Essas interfaces devem ser testadas pelos prestadores de serviços de pagamento que as utilizam, bem como submetidas a testes de esforço e controladas pelas autoridades competentes.

(24) A fim de garantir que os prestadores de serviços de pagamento que dependem da interface dedicada possam continuar a prestar os seus serviços em caso de problemas de disponibilidade ou de desempenho inadequado, é necessário criar, sob condições estritas, um mecanismo de recurso que permita a esses prestadores utilizarem a interface que o prestador de serviços de pagamento gestor de contas mantém para identificar e comunicar com os seus próprios utilizadores de serviços de pagamento. Caso as respetivas autoridades competentes determinem que as interfaces dedicadas cumprem condições específicas que garantem uma concorrência sem entraves, certos prestadores de serviços de pagamento gestores de contas ficarão isentos da obrigação de criar esse mecanismo de recurso através das suas interfaces de interação com os clientes. Caso as interfaces dedicadas que são objeto de isenção não cumpram as condições exigidas, as autoridades competentes revogam as isenções concedidas.

(25) A fim de permitir que as autoridades competentes supervisionem e controlem com eficácia a implementação e a gestão das interfaces de comunicação, os prestadores de serviços de pagamento gestores de contas devem apresentar um resumo da documentação pertinente no respetivo sítio Web e fornecer às autoridades competentes, a seu pedido, a documentação das soluções para os casos de emergência. Os prestadores de serviços de pagamento gestores de contas devem igualmente publicar as estatísticas sobre a disponibilidade e o desempenho dessas interfaces.

(26) A fim de salvaguardar a confidencialidade e a integridade dos dados, é necessário garantir a segurança das sessões de comunicação entre os prestadores de serviços de pagamento gestores de contas, os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de

pagamento que emitem instrumentos de pagamento baseados em cartões. Designadamente, é necessário exigir que, durante aos intercâmbios de dados, exista uma encriptação segura entre os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos, os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões e os prestadores de serviços de pagamento gestores de contas.

(27) Com o intuito de aumentar a confiança dos utilizadores e assegurar uma autenticação forte do cliente, deve ser tida em conta a utilização de meios de identificação eletrónica e serviços de confiança prevista no Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([1]), em especial no que se refere aos sistemas de identificação eletrónica notificados.

(28) A fim de assegurar o alinhamento das datas de aplicação, o presente regulamento deve ser aplicável a partir da mesma data em que os Estados-Membros têm de assegurar a aplicação das medidas de segurança a que se referem os artigos 65.º, 66.º, 67.º e 97.º da Diretiva (UE) 2015/2366.

(29) O presente regulamento tem por base os projetos de normas técnicas de regulamentação apresentados pela Autoridade Bancária Europeia (EBA) à Comissão.

(30) A EBA realizou consultas públicas abertas e transparentes sobre os projetos de normas técnicas de regulamentação em que se baseia o presente regulamento, analisou os potenciais custos e benefícios conexos e solicitou o parecer do Grupo das Partes Interessadas do Setor Bancário criado nos termos do artigo 37.º do Regulamento (UE) n.º 1093/2010,

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente regulamento estabelece os requisitos a cumprir pelos prestadores de serviços de pagamento a fim de implementarem medidas de segurança que lhes permitam efetuar o seguinte:

a) Aplicar o procedimento da autenticação forte do cliente nos termos do artigo 97.º da Diretiva (UE) 2015/2366;

b) Isentar da aplicação dos requisitos de segurança da autenticação forte do cliente, sob reserva de condições específicas e limitadas tendo por base o nível de risco, o montante e a recorrência da operação de pagamento e o canal de pagamento utilizado para a sua execução;

c) Proteger a confidencialidade e a integridade das credenciais de segurança personalizadas do utilizador de serviços de pagamento;

d) Estabelecer normas abertas comuns e seguras para as comunicações entre os prestadores de serviços de pagamento gestores de contas, os prestadores de serviços de iniciação de pagamentos, os prestadores de serviços de informação sobre contas, os ordenantes, os beneficiários e outros prestadores de serviços de pagamento, relativamente à prestação e utilização de serviços de pagamento em aplicação do título IV da Diretiva (UE) 2015/2366.

Artigo 2.º

Requisitos gerais de autenticação

1. Os prestadores de serviços de pagamento devem dispor de mecanismos de controlo das operações que lhes permitam detetar operações de pagamento fraudulentas ou não autorizadas para efeitos da aplicação das medidas de segurança a que se refere o artigo 1.º, alíneas a) e b).

([1]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 53).

Esses mecanismos devem basear-se na análise das operações de pagamento, tendo em conta os elementos específicos do utilizador de serviços de pagamento em circunstâncias de utilização normal das credenciais de segurança personalizadas.

2. Os prestadores de serviços de pagamento devem assegurar que os mecanismos de controlo das operações têm em conta, no mínimo, cada um dos seguintes fatores baseados no risco:

a) Listas de elementos de autenticação que foram objeto de utilização fraudulenta ou furto;

b) O montante de cada operação de pagamento;

c) Cenários de fraude conhecidos no contexto da prestação de serviços de pagamento;

d) Sinais de infeção por *software* maligno (*malware*) em sessões do procedimento de autenticação;

e) Caso o dispositivo ou *software* de acesso seja fornecido pelo prestador de serviços de pagamento, um registo da utilização do dispositivo ou *software* de acesso fornecido ao utilizador de serviços de pagamento e da utilização anormal desse dispositivo ou *software*.

Artigo 3.º

Revisão das medidas de segurança

1. A aplicação das medidas de segurança a que se refere o artigo 1.º deve ser documentada, periodicamente testada, avaliada e auditada, em conformidade com o quadro jurídico aplicável ao prestador de serviços de pagamento, por revisores oficiais de contas com conhecimentos especializados em segurança informática e pagamentos eletrónicos e que sejam operacionalmente independentes do prestador de serviços de pagamento.

2. O período entre as auditorias referidas no n.º 1 é determinado tendo em conta o quadro jurídico em matéria de contabilidade e revisão oficial de contas aplicável ao prestador de serviços de pagamento.

No entanto, os prestadores de serviços de pagamento que utilizarem a isenção referida no artigo 18.º devem ser objeto de uma auditoria à metodologia, ao modelo e às taxas de fraude comunicadas, no mínimo uma vez por ano. O revisor oficial de contas que efetuar esta auditoria deve ter conhecimentos especializados em segurança informática e pagamentos eletrónicos e ser operacionalmente independente do prestador de serviços de pagamento. Durante o primeiro ano de aplicação da isenção prevista no artigo 18.º e, posteriormente, pelo menos de três em três anos, ou, a pedido da autoridade competente, com maior frequência, a auditoria deve ser efetuada por um revisor oficial de contas externo independente e qualificado.

3. A auditoria deve apresentar uma avaliação e um relatório sobre a conformidade das medidas de segurança tomadas pelo prestador de serviços de pagamento com os requisitos previstos no presente regulamento.

O relatório deve ser disponibilizado na íntegra às autoridades competentes, a pedido destas.

CAPÍTULO II

MEDIDAS DE SEGURANÇA PARA A APLICAÇÃO DA AUTENTICAÇÃO FORTE DO CLIENTE

Artigo 4.º

Código de autenticação

1. Sempre que os prestadores de serviços de pagamento apliquem a autenticação forte do cliente nos termos do artigo 97.º, n.º 1, da Diretiva (UE) 2015/2366, a autenticação deve basear-se em dois ou mais elementos pertencentes às categorias de conhecimento, posse e inerência e resultar na geração de um código de autenticação.

O código de autenticação só deve ser aceite uma vez pelo prestador de serviços de pagamento quando o ordenante o utilizar para aceder em linha à sua conta de pagamento, iniciar uma operação de pagamento eletrónico ou realizar uma ação, através de um canal remoto, suscetível de envolver um risco de fraude no pagamento ou outros abusos.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem adotar medidas de segurança para garantir o cumprimento de cada um dos seguintes requisitos:

a) Não pode ser obtida qualquer informação sobre nenhum dos elementos a que se refere o n.º 1 com a divulgação do código de autenticação;

b) Não é possível gerar um novo código de autenticação baseado no conhecimento de qualquer outro código de autenticação gerado anteriormente;

c) O código de autenticação não pode ser falsificado.

3. Os prestadores de serviços de pagamento devem assegurar que a autenticação por meio da geração de um código de autenticação inclui cada uma das seguintes medidas:

a) Caso a autenticação para acesso remoto, pagamentos eletrónicos remotos e outras ações, através de um canal remoto, suscetíveis de envolver um risco de fraude no pagamento ou outros abusos, não permita gerar um código de autenticação para efeitos do disposto no n.º 1, não deve ser possível identificar qual dos elementos referidos nesse número estava incorreto;

b) Não devem ser possíveis mais de cinco tentativas de autenticação falhadas consecutivas num determinado período de tempo, após o que as ações referidas no artigo 97.º, n.º 1, da Diretiva (UE) 2015/2366 devem ser temporária ou permanentemente bloqueadas;

c) As sessões de comunicação devem ser protegidas contra a captura dos dados de autenticação transmitidos durante o processo de autenticação e contra a manipulação por partes não autorizadas, em conformidade com os requisitos estabelecidos no capítulo V;

d) O tempo máximo de inatividade após o ordenante ser autenticado para aceder em linha à sua conta de pagamento não deve exceder cinco minutos.

4. Caso o bloqueio a que se refere o n.º 3, alínea b), seja temporário, a duração desse bloqueio e o número de novas tentativas devem ser estabelecidos com base nas características do serviço prestado ao ordenante e em todos os riscos relevantes envolvidos, tendo em conta, no mínimo, os fatores referidos no artigo 2.º, n.º 2.

O ordenante deve ser avisado antes de o bloqueio se tornar permanente.

Caso o bloqueio passe a ser permanente, deve ser estabelecido um procedimento seguro que permita ao ordenante voltar a utilizar os instrumentos de pagamento eletrónico bloqueados.

Artigo 5.º

Ligação dinâmica

1. Caso apliquem a autenticação forte do cliente nos termos do artigo 97.º, n.º 2, da Diretiva (UE) 2015/2366, os prestadores de serviços de pagamento devem, para além dos requisitos enunciados no artigo 4.º do presente regulamento, adotar igualmente medidas de segurança que satisfaçam cada uma das condições seguintes:

a) O ordenante deve tomar conhecimento do montante da operação de pagamento e do beneficiário;

b) O código de autenticação gerado deve ser específico do montante da operação de pagamento e do beneficiário aceite pelo ordenante ao iniciar a operação;

c) O código de autenticação aceite pelo prestador de serviços de pagamento deve corresponder ao montante específico inicial da operação de pagamento e à identidade do beneficiário aceite pelo ordenante;

d) Qualquer alteração do montante ou do beneficiário resulta na invalidação do código de autenticação gerado.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem adotar medidas de segurança que assegurem a confidencialidade, a autenticidade e a integridade de cada um dos seguintes elementos:

a) O montante da operação e o beneficiário, em todas as fases da autenticação;

b) As informações mostradas ao ordenante em todas as fases da autenticação, nomeadamente a geração, a transmissão e a utilização do código de autenticação.

3. Para efeitos do disposto no n.º 1, alínea b), e caso os prestadores de serviços de pagamento apliquem a autenticação forte do cliente nos termos do artigo 97.º, n.º 2, da Diretiva (UE) 2015/2366, são aplicáveis os seguintes requisitos ao código de autenticação:

a) Relativamente a uma operação de pagamento baseada em cartão para a qual o ordenante tenha dado o seu consentimento quanto ao montante exato dos fundos a bloquear nos termos do artigo 75.º, n.º 1, da referida diretiva, o código de autenticação deve ser específico do montante cujo bloqueio e aceitação tenham sido consentidos pelo ordenante no início da operação;

b) Relativamente a operações de pagamento para as quais o ordenante tenha consentido a execução de um lote de operações de pagamento eletrónico remotas para um ou vários beneficiários, o código de autenticação deve ser específico do montante total do lote de operações de pagamento e dos beneficiários indicados.

Artigo 6.º

Requisitos dos elementos pertencentes à categoria do conhecimento

1. Os prestadores de serviços de pagamento devem adotar medidas para reduzir o risco de os elementos da autenticação forte do cliente pertencentes à categoria do conhecimento serem descobertos por partes não autorizadas ou divulgados junto delas.

2. A utilização destes elementos pelo ordenante deve ser objeto de medidas de atenuação de riscos que evitem a sua divulgação a partes não autorizadas.

Artigo 7.º

Requisitos dos elementos pertencentes à categoria da posse

1. Os prestadores de serviços de pagamento devem adotar medidas para reduzir o risco de os elementos da autenticação forte do cliente pertencentes à categoria da posse serem utilizados por partes não autorizadas.

2. A utilização pelo ordenante destes elementos deve ser objeto de medidas destinadas a evitar a sua replicação.

Artigo 8.º

Requisitos dos dispositivos e *software* associados aos elementos pertencentes à categoria da inerência

1. Os prestadores de serviços de pagamento devem adotar medidas para reduzir o risco de os elementos de autenticação pertencentes à categoria da inerência e lidos pelos dispositivos e *software* de acesso fornecidos ao ordenante serem descobertos por partes não autorizadas. No mínimo, os prestadores de serviços de pagamento devem assegurar que tais dispositivos e *software* de acesso implicam uma probabilidade muito reduzida de uma parte não autorizada ser autenticada como sendo o ordenante.

2. A utilização destes elementos pelo ordenante deve ser sujeita a medidas que assegurem que os dispositivos e o *software* impedem a utilização não autorizada dos elementos através do acesso aos dispositivos e ao *software*.

Artigo 9.º

Independência dos elementos

1. Os prestadores de serviços de pagamento devem assegurar que a utilização dos elementos da autenticação forte do cliente referidos nos artigos 6.º, 7.º e 8.º é sujeita a medidas que garantam que, em termos tecnológicos, algorítmicos e paramétricos, a violação de um dos elementos não compromete a fiabilidade dos restantes.

2. Os prestadores de serviços de pagamento devem adotar medidas de segurança sempre que um dos elementos da autenticação forte do cliente ou do próprio código de autenticação seja utilizado através de um dispositivo multifuncional, de modo a reduzir o risco decorrente de uma eventual utilização fraudulenta desse dispositivo.

3. Para efeitos do n.º 2, as medidas de atenuação de riscos devem incluir cada um dos seguintes elementos:

a) A utilização de ambientes de execução seguros e distintos através do *software* instalado no dispositivo multifuncional;

b) Mecanismos que assegurem que o *software* ou o dispositivo não foi alterado pelo ordenante ou por terceiros;

c) Caso tenham ocorrido alterações, mecanismos para atenuar as suas consequências.

CAPÍTULO III

ISENÇÕES DA AUTENTICAÇÃO FORTE DO CLIENTE

Artigo 10.º

Informações sobre contas de pagamento

1. Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos previstos no artigo 2.º e no n.º 2 do presente artigo, e, caso um utilizador de serviços de pagamento tenha o acesso limitado a um dos seguintes elementos em linha ou a ambos, sem a divulgação de dados de pagamento sensíveis:

a) O saldo de uma ou mais contas de pagamento designadas;

b) As operações de pagamento executadas nos últimos 90 dias através de uma ou mais contas de pagamento designadas.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento não ficam isentos da aplicação da autenticação forte do cliente sempre que uma das seguintes condições estiver preenchida:

a) O utilizador de serviços de pagamento está a aceder em linha pela primeira vez às informações especificadas no n.º 1;

b) Decorreram mais de 90 dias desde a última vez que o utilizador de serviços de pagamento acedeu em linha às informações especificadas no n.º 1, alínea b), e a autenticação forte do cliente foi aplicada.

Artigo 11.º

Pagamentos sem contacto no ponto de venda

Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos previstos no artigo 2.º, sempre que o ordenante inicie uma operação de pagamento eletrónico sem contacto, desde que estejam preenchidas as seguintes condições:

a) O montante da operação de pagamento eletrónico sem contacto não ultrapassa 50 EUR; e

b) O montante acumulado das anteriores operações de pagamento eletrónico sem contacto iniciadas por meio de um instrumento de pagamento com uma funcionalidade sem contacto desde a data da última aplicação da autenticação forte do cliente não ultrapassa 150 EUR; ou

c) Não ocorreram mais de cinco operações de pagamento eletrónico sem contacto sucessivas iniciadas por meio de um instrumento de pagamento com uma funcionalidade sem contacto desde a última aplicação da autenticação forte do cliente.

Artigo 12.º

Terminais automáticos para o pagamento de tarifas de transporte e de estacionamento

Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos previstos no artigo 2.º, sempre que o ordenante inicie uma operação de pagamento eletrónico num terminal automático de pagamento de uma tarifa de transporte ou de estacionamento.

Artigo 13.º

Beneficiários fiáveis

1. Os prestadores de serviços de pagamento devem aplicar a autenticação forte do cliente caso o ordenante crie ou altere uma lista de beneficiários fiáveis através do prestador de serviços de pagamento que gere a conta do ordenante.

2. Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos gerais de autenticação, sempre que o ordenante inicie uma operação de pagamento a favor de um beneficiário constante de uma lista de beneficiários de confiança previamente criada pelo primeiro.

Artigo 14.º

Operações recorrentes

1. Os prestadores de serviços de pagamento devem aplicar a autenticação forte do cliente caso o ordenante crie, altere ou inicie pela primeira vez uma série de operações recorrentes do mesmo montante e junto do mesmo beneficiário.

2. Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos gerais de autenticação, à iniciação de todas as operações de pagamento subsequentes incluídas na série de operações de pagamento a que se refere o n.º 1.

Artigo 15.º

Transferências a crédito entre contas detidas pela mesma pessoa singular ou coletiva

Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente, sob reserva do cumprimento dos requisitos previstos no artigo 2.º, sempre que o ordenante inicie uma transferência a crédito em circunstâncias nas quais o ordenante e o beneficiário sejam a mesma pessoa singular ou coletiva e as duas contas de pagamento sejam detidas pelo mesmo prestador de serviços de pagamento gestor de contas.

Artigo 16.º

Operações de pequeno valor

Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente sempre que o ordenante inicie uma operação de pagamento eletrónico remoto, desde que estejam preenchidas as seguintes condições:

a) O montante da operação de pagamento eletrónico remoto não ultrapassa 30 EUR; e

b) O montante acumulado das anteriores operações de pagamento eletrónico remoto iniciadas pelo ordenante desde a última aplicação da autenticação forte do cliente não ultrapassa 100 EUR; ou

c) Não ocorreram mais de cinco operações de pagamento eletrónico remoto sucessivas iniciadas pelo ordenante desde a última aplicação da autenticação forte do cliente.

Artigo 17.º

Processos e protocolos de pagamento seguros para empresas

Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente às pessoas coletivas que iniciem operações de pagamento eletrónico utilizando processos ou protocolos de pagamento específicos só disponibilizados a ordenantes que não sejam consumidores, caso as autoridades competentes considerem que tais processos ou protocolos garantem níveis de segurança pelo menos equivalentes aos previstos na Diretiva (UE) 2015/2366.

Artigo 18.º

Análise de risco das operações

1. Os prestadores de serviços de pagamento podem não aplicar a autenticação forte do cliente sempre que o ordenante inicie uma operação de pagamento eletrónico remoto identificada pelo prestador de serviços de pagamento como apresentando um baixo nível de risco de acordo com os mecanismos de controlo das operações referidos no artigo 2.º e no n.º 2, alínea c), do presente artigo.

2. Considera-se que uma operação de pagamento eletrónico como a referida no n.º 1 apresenta um baixo nível de risco se estiverem preenchidas todas as seguintes condições:

a) A taxa de fraudes do tipo de operação em causa, comunicada pelo prestador de serviços de pagamento e calculada nos termos do artigo 19.º, é equivalente ou inferior às taxas de fraude de referência indicadas no quadro constante do anexo relativo aos «pagamentos eletrónicos remotos baseados em cartões» e às «transferências a crédito eletrónicas remotas», respetivamente;

b) O montante da operação não ultrapassa o valor-limiar de isenção («VLI») indicado no quadro que consta do anexo;

c) A análise de risco em tempo real efetuada pelos prestadores de serviços de pagamento não detetou nenhuma das seguintes situações:

   i) despesas ou padrões de comportamento anormais do ordenante,

   ii) informações invulgares sobre o acesso do ordenante com o dispositivo ou *software* por ele utilizado,

   iii) infeção por *software* maligno (*malware*) numa sessão do procedimento de autenticação,

   iv) cenário de fraude conhecido no contexto da prestação de serviços de pagamento,

   v) localização anormal do ordenante,

   vi) localização de alto risco do beneficiário.

3. Os prestadores de serviços de pagamento que tencionem isentar operações de pagamento eletrónico remoto da autenticação forte do cliente por essas operações apresentarem um baixo risco devem ter em conta, no mínimo, os seguintes fatores baseados no risco:

a) O perfil de despesas anterior do utilizador de serviços de pagamento em causa;

b) O histórico de operações de pagamento de cada um dos utilizadores de serviços de pagamento do prestador de serviços de pagamento;

c) A localização do ordenante e do beneficiário no momento da operação de pagamento, caso o dispositivo ou *software* de acesso seja fornecido pelo prestador de serviços de pagamento;

d) A identificação de padrões de pagamento anormais do utilizador de serviços de pagamento em relação ao seu histórico de operações de pagamento.

A avaliação efetuada por um prestador de serviços de pagamento deve combinar todos estes fatores baseados no risco e atribuir uma classificação de risco a cada operação para determinar se um pagamento específico deve ser autorizado sem autenticação forte do cliente.

Artigo 19.º

Cálculo das taxas de fraude

1. Por cada tipo de operação indicado no quadro constante do anexo, o prestador do serviço de pagamento deve certificar-se de que as taxas de fraude gerais tanto das operações de pagamento autenticadas através da autenticação forte do cliente como das executadas ao abrigo de uma das isenções previstas nos artigos 13.º a 18.º são equivalentes ou inferiores à taxa de fraude de referência do mesmo tipo de operação de pagamento indicado no quadro constante do anexo.

A taxa de fraude geral de cada tipo de operação deve ser calculada como sendo o valor total das operações remotas não autorizadas ou fraudulentas, com ou sem recuperação dos fundos, dividido pelo valor total de todas as operações remotas do mesmo tipo de operação, tenham sido elas autenticadas com a aplicação da autenticação forte do cliente ou executadas ao abrigo de uma das isenções previstas nos artigos 13.º a 18.º, num período trimestral contínuo (90 dias).

2. O cálculo das taxas de fraude e os valores resultantes devem ser avaliados pela análise auditoria referida no artigo 3.º, n.º 2, a qual deve garantir a sua exaustividade e exatidão.

3. A metodologia e o(s) modelo(s) utilizados pelo prestador de serviços de pagamento para calcular as taxas de fraude, bem como as próprias taxas de fraude, devem ser adequadamente documentados e integralmente disponibilizados às autoridades competentes e à EBA, com notificação prévia às autoridades competentes, a pedido das mesmas.

Artigo 20.º

Cessação das isenções com base na análise de risco das operações

1. Os prestadores de serviços de pagamento que apliquem as isenções referidas no artigo 18.º devem comunicar de imediato às autoridades competentes qualquer situação em que uma das respetivas taxas de fraude controladas, de um dos tipos de operações de pagamento indicados no quadro constante do anexo, seja superior à taxa de fraude de referência aplicável, e devem apresentar às autoridades competentes uma descrição das medidas que pretendem adotar para restabelecer a conformidade da taxa de fraude controlada com as taxas de fraude de referência aplicáveis.

2. Os prestadores de serviços de pagamento devem cessar de imediato a aplicação da isenção referida no artigo 18.º a qualquer um dos tipos de operações de pagamento indicados no quadro constante do anexo se, com base no respetivo intervalo de valores-limiar de isenção, a sua taxa de fraude controlada for superior, durante dois trimestres consecutivos, à taxa de fraude de referência aplicável a esse instrumento de pagamento ou tipo de operação de pagamento, de acordo com esse intervalo.

3. Na sequência da cessação da isenção referida no artigo 18.º em conformidade com o n.º 2 do presente artigo, os prestadores de serviços de pagamento não podem voltar a aplicar essa isenção até que a respetiva taxa de fraude calculada seja igual ou inferior às taxas de fraude de referência aplicáveis a esse tipo de operação de pagamento, de acordo com o intervalo de valores-limiar de isenção, durante um trimestre.

4. Caso pretendam voltar a aplicar a isenção referida no artigo 18.º, os prestadores de serviços de pagamento devem notificar as autoridades competentes dentro de um prazo razoável e, antes de voltarem a aplicar a isenção, apresentar provas do restabelecimento da conformidade da respetiva taxa de fraude controlada com a taxa de fraude de referência aplicável do intervalo de valores-limiar de isenção, em conformidade com o n.º 3 do presente artigo.

Artigo 21.º

Controlo

1. A fim de aplicar as isenções previstas nos artigos 10.º a 18.º, os prestadores de serviços de pagamento devem registar e controlar os seguintes dados relativamente a cada tipo de operações de pagamento, distinguindo entre operações de pagamento remoto e não remoto, pelo menos com uma periodicidade trimestral:

a) O valor total das operações de pagamento não autorizadas ou fraudulentas nos termos do artigo 64.º, n.º 2, da Diretiva (UE) 2015/2366, o valor total de todas as operações de pagamento e a taxa de fraude resultante, discriminando as operações de pagamento iniciadas através da autenticação forte do cliente e ao abrigo de cada uma das isenções;

b) O valor médio por operação, discriminando as operações de pagamento iniciadas através da autenticação forte do cliente e ao abrigo de cada uma das isenções;

c) O número de operações de pagamento em que foi aplicada cada uma das isenções e a sua percentagem em relação ao número total de operações de pagamento.

2. Os prestadores de serviços de pagamento devem disponibilizar os resultados do controlo às autoridades competentes e à EBA em conformidade com o n.º 1, com notificação prévia à(s) autoridade(s) competente(s), a pedido da(s) mesma(s).

CAPÍTULO IV

CONFIDENCIALIDADE E INTEGRIDADE DAS CREDENCIAIS DE SEGURANÇA PERSONALIZADAS DOS UTILIZADORES DE SERVIÇOS DE PAGAMENTO

Artigo 22.º

Requisitos gerais

1. Os prestadores de serviços de pagamento devem garantir a confidencialidade e a integridade das credenciais de segurança personalizadas do utilizador do serviço de pagamento, incluindo códigos de autenticação, em todas as fases da autenticação.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem assegurar o cumprimento de cada um dos seguintes requisitos:

a) As credenciais de segurança personalizadas devem ser dissimuladas ao serem visualizadas e não devem ser legíveis na totalidade aquando da sua introdução pelo utilizador de serviços de pagamento durante a autenticação;

b) As credenciais de segurança personalizadas em formato de dados, assim como os elementos criptográficos relacionados com a encriptação das credenciais de segurança personalizadas, não devem ser armazenadas em texto simples;

c) Os elementos criptográficos secretos devem ser protegidos da divulgação não autorizada.

3. Os prestadores de serviços de pagamento devem documentar devidamente o processo relacionado com a gestão dos elementos criptográficos utilizados para encriptar as credenciais de segurança personalizadas ou torná-las de outro modo ilegíveis.

4. Os prestadores de serviços de pagamento devem assegurar que o tratamento e o encaminhamento das credenciais de segurança personalizadas e dos códigos de autenticação gerados nos termos do disposto no capítulo II são efetuados em ambientes seguros, em conformidade com normas sólidas e amplamente reconhecidas no setor.

Artigo 23.º

Geração e transmissão de credenciais

Os prestadores de serviços de pagamento devem garantir que a geração das credenciais de segurança personalizadas é efetuada num ambiente seguro.

De igual modo, devem reduzir os riscos de utilização não autorizada das credenciais de segurança personalizadas e dos dispositivos e *software* de autenticação que tenham sido perdidos, furtados ou copiados antes de serem fornecidos ao ordenante.

Artigo 24.º

Associação ao utilizador de serviços de pagamento

1. Os prestadores de serviços de pagamento devem assegurar que apenas o utilizador de serviços de pagamento é associado, de forma segura, às credenciais de segurança personalizadas e aos dispositivos e *software* de autenticação.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem assegurar o cumprimento de cada um dos seguintes requisitos:

a) A associação da identidade do utilizador de serviços de pagamento a credenciais de segurança personalizadas, dispositivos e *software* de autenticação deve ser efetuada em ambientes seguros sob a responsabilidade do prestador de serviços de pagamento, incluindo, pelo menos, as instalações do prestador de serviços de pagamento, o ambiente de Internet disponibilizado pelo prestador de serviços de pagamento ou outros sítios Web seguros semelhantes por ele utilizados e os seus serviços de caixas automáticos, tendo em conta os riscos associados aos dispositivos e componentes subjacentes utilizados durante o processo de associação que não estejam sob a responsabilidade do prestador de serviços de pagamento;

b) A associação, através de um canal remoto, da identidade do utilizador de serviços de pagamento às credenciais de segurança personalizadas, aos dispositivos ou *software* de autenticação deve ser efetuada aplicando a autenticação forte do cliente.

Artigo 25.º

Fornecimento de credenciais, dispositivos e *software* de autenticação

1. Os prestadores de serviços de pagamento devem assegurar que o fornecimento de credenciais de segurança personalizadas, dispositivos e *software* de autenticação ao utilizador de serviços de pagamento se processa de uma forma segura e concebida para enfrentar os riscos relacionados com a sua utilização não autorizada em caso de perda, furto ou cópia.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem aplicar, pelo menos, cada uma das seguintes medidas:

a) Mecanismos eficazes e seguros que garantam o fornecimento das credenciais de segurança personalizadas e dos dispositivos e *software* de autenticação ao utilizador de serviços de pagamento legítimo;

b) Mecanismos que permitam ao prestador de serviços de pagamento verificar a autenticidade do *software* de autenticação fornecido ao utilizador de serviços de pagamento através da Internet;

c) Medidas que garantam que, caso o fornecimento das credenciais de segurança personalizadas seja executado fora das instalações do prestador de serviços de pagamento ou através de um canal remoto:

   i) nenhuma parte não autorizada possa obter mais do que um elemento das credenciais de segurança personalizadas e dos dispositivos ou *software* de autenticação quando forem fornecidos através do mesmo canal,

   ii) as credenciais de segurança personalizadas e os dispositivos ou *software* de autenticação tenham de ser ativados antes da sua utilização;

d) Medidas que garantam que, nos casos em que as credenciais de segurança personalizadas e os dispositivos ou *software* de autenticação tenham de ser ativados antes da sua primeira utilização, a ativação seja efetuada num ambiente seguro, em conformidade com os procedimentos de associação referidos no artigo 24.º.

Artigo 26.º

Renovação de credenciais de segurança personalizadas

Os prestadores de serviços de pagamento devem assegurar que a renovação ou reativação das credenciais de segurança personalizadas respeita os procedimentos de geração, associação e fornecimento das credenciais e dos dispositivos de autenticação, nos termos dos artigos 23.º, 24.º e 25.º.

Artigo 27.º

Destruição, desativação e revogação

Os prestadores de serviços de pagamento devem assegurar a existência de processos eficazes para aplicar cada uma das medidas de segurança seguintes:

a) A destruição, desativação ou revogação segura das credenciais de segurança personalizadas e dos dispositivos e *software* de autenticação;

b) Caso distribua dispositivos e *software* de autenticação reutilizáveis, o prestador de serviços de pagamento deve determinar, documentar e aplicar a reutilização segura de um dispositivo ou *software* antes de o disponibilizar a outro utilizador de serviços de pagamento;

c) A desativação ou revogação de informações relacionadas com as credenciais de segurança personalizadas armazenadas nos sistemas e bases de dados do prestador de serviços de pagamento e, se for esse o caso, em repositórios públicos.

CAPÍTULO V

NORMAS ABERTAS DE COMUNICAÇÃO COMUNS E SEGURAS

Secção 1

Requisitos gerais de comunicação

Artigo 28.º

Requisitos de identificação

1. Os prestadores de serviços de pagamento devem garantir uma identificação segura nas comunicações entre o dispositivo do ordenante e os dispositivos de aceitação de pagamentos eletrónicos do beneficiário, incluindo, entre outros, os terminais de pagamento.

2. Os prestadores de serviços de pagamento devem assegurar de forma eficaz a redução dos riscos de direcionamento indevido de comunicações para partes não autorizadas nas aplicações móveis e noutras interfaces de utilizadores de serviços de pagamento que ofereçam serviços de pagamento eletrónico.

Artigo 29.º

Rastreabilidade

1. Os prestadores de serviços de pagamento devem dispor de processos que assegurem a rastreabilidade de todas as operações de pagamento e de outras interações com o utilizador de serviços de pagamento, com outros prestadores de serviços de pagamento e com outras entidades, incluindo comerciantes, no contexto da prestação de serviços de pagamento, garantindo o conhecimento *ex post* de todos os eventos relevantes para a operação eletrónica em todas as fases.

2. Para efeitos do disposto no n.º 1, os prestadores de serviços de pagamento devem assegurar que qualquer sessão de comunicação estabelecida com o utilizador de serviços de pagamento, com outros prestadores de serviços de pagamento e com outras entidades, incluindo comerciantes, tem por base cada um dos seguintes elementos:

a) Um identificador único da sessão;

b) Mecanismos de segurança para o registo pormenorizado da operação, nomeadamente o número, marcas temporais e todos os dados relevantes da mesma;

c) Marcas temporais baseadas num sistema horário de referência uniforme e sincronizados de acordo com um sinal horário oficial.

Secção 2

Requisitos específicos das normas abertas de comunicação comuns e seguras

Artigo 30.º

Obrigações gerais para as interfaces de acesso

1. Os prestadores de serviços de pagamento gestores de contas que ofereçam a um ordenante uma conta de pagamento acessível em linha devem dispor de pelo menos uma interface que satisfaça cada um dos seguintes requisitos:

a) Os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões devem poder identificar-se junto do prestador de serviços de pagamento gestor de contas;

b) Os prestadores de serviços de informação sobre contas devem poder comunicar de forma segura para pedir e receber informações sobre uma ou mais contas de pagamento designadas e as operações de pagamento associadas;

c) Os prestadores de serviços de iniciação de pagamentos devem poder comunicar de forma segura para iniciar uma ordem de pagamento a partir da conta de pagamento do ordenante e receber todas as informações sobre a iniciação da operação de pagamento e todas as informações acessíveis aos prestadores de serviços de pagamento gestores de contas sobre a execução da operação de pagamento.

2. Para efeitos de autenticação do utilizador de serviços de pagamento, a interface a que se refere o n.º 1 deve permitir que os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos se baseiem em todos os procedimentos de autenticação facultados pelo prestador de serviços de pagamento gestor de contas ao utilizador de serviços de pagamento.

A interface deve satisfazer pelo menos todos os seguintes requisitos:

a) Um prestador de serviços de iniciação de pagamentos ou um prestador de serviços de informação sobre contas deve poder instruir o prestador de serviços de pagamento gestor de contas no sentido de iniciar a autenticação com base no consentimento do utilizador de serviços de pagamento;

b) As sessões de comunicação entre o prestador de serviços de pagamento gestor de contas, o prestador de serviços de informação sobre contas, o prestador de serviços de iniciação de pagamentos e o utilizador de serviços de pagamento em causa devem ser estabelecidas e mantidas ao longo do processo de autenticação;

c) É necessário assegurar a integridade e a confidencialidade das credenciais de segurança personalizadas e dos códigos de autenticação transmitidos pelo ou através do prestador de serviços de iniciação de pagamentos ou do prestador de serviços de informação sobre contas.

3. Os prestadores de serviços de pagamento gestores de contas devem assegurar que as respetivas interfaces seguem as normas de comunicação emitidas por organizações de normalização internacionais ou europeias.

Os prestadores de serviços de pagamento gestores de contas devem igualmente assegurar que as especificações técnicas de qualquer uma das interfaces são documentadas especificando um conjunto de rotinas, protocolos e ferramentas necessários para permitir a interoperabilidade do *software* e das aplicações dos prestadores de serviços de iniciação de pagamentos, dos prestadores de serviços de informação sobre contas e dos prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões com os sistemas dos prestadores de serviços de pagamento que gerem as contas.

Os prestadores de serviços de pagamento gestores de contas devem, no mínimo, e pelo menos seis meses antes da data de aplicação indicada no artigo 38.º, n.º 2, ou antes da data fixada para o lançamento no mercado da interface de acesso, caso este lançamento tenha lugar após a data indicada no artigo 38.º, n.º 2, apresentar a documentação disponível, a título gratuito, a pedido dos prestadores de serviços de iniciação de pagamentos, prestadores de serviços de informação sobre contas e prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões autorizados, ou de prestadores de serviços de pagamento que tenham pedido junto das respetivas autoridades competentes a autorização em causa, e disponibilizar publicamente um resumo da documentação no seu sítio Web.

4. Além do disposto no n.º 3, os prestadores de serviços de pagamento gestores de contas devem assegurar que, exceto em situações de emergência, qualquer alteração das especificações técnicas da respetiva interface é comunicada aos prestadores de serviços de iniciação de pagamentos, prestadores de serviços de informação sobre contas e prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões autorizados, ou aos prestadores de serviços de pagamento que tenham pedido junto das autoridades competentes a autorização em causa, antecipadamente, assim que possível e pelo menos três meses antes de a alteração ser aplicada.

Os prestadores de serviços de pagamento devem documentar as situações de emergência em que sejam aplicadas alterações e disponibilizar a documentação às autoridades competentes, a pedido destas.

5. Os prestadores de serviços de pagamento gestores de contas devem disponibilizar um dispositivo de teste, com apoio, para efetuar testes de ligação e funcionais, para que os prestadores de serviços de iniciação de pagamentos, prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões e prestadores de serviços de informação sobre contas autorizados, ou os prestadores de serviços de pagamento que tenham pedido a autorização em causa, possam testar o seu *software* e as aplicações que utilizam para oferecer um serviço de pagamento aos utilizadores. Este dispositivo de teste deve estar disponível o mais tardar seis meses antes da data de aplicação indicada no artigo 38.º, n.º 2, ou antes da data fixada para o lançamento no mercado da interface de acesso, caso este lançamento tenha lugar após a data indicada no artigo 38.º, n.º 2.

No entanto, não podem ser partilhadas informações sensíveis através do dispositivo de teste.

6. As autoridades competentes devem assegurar que os prestadores de serviços de pagamento gestores de contas cumprem sempre as obrigações previstas nestas normas em relação à(s) interface(s) por eles criadas. Caso um prestador de serviços de pagamento que gere contas não cumpra os requisitos aplicáveis às interfaces estabelecidos nestas normas, as autoridades competentes devem assegurar que a prestação de serviços de iniciação de pagamentos e de serviços de informação sobre contas não é impedida ou perturbada, desde que os prestadores desses serviços observem as condições definidas no artigo 33.º, n.º 5.

Artigo 31.º

Opções de interface de acesso

Os prestadores de serviços de pagamento gestores de contas devem criar a(s) interface(s) a que se refere o artigo 30.º através de uma interface dedicada ou permitindo aos prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, que utilizem as interfaces destinadas à autenticação e comunicação com os utilizadores de serviços de pagamento do prestador de serviços de pagamento gestor de contas.

Artigo 32.º

Obrigações para uma interface dedicada

1. Sob reserva do cumprimento do disposto nos artigos 30.º e 31.º, os prestadores de serviços de pagamento gestores de contas que tenham criado uma interface dedicada devem assegurar que esta proporciona sempre o mesmo nível de disponibilidade e desempenho, incluindo o apoio, que as interfaces disponibilizadas ao utilizador de serviços de pagamento para que este aceda diretamente em linha à sua conta de pagamento.

2. Os prestadores de serviços de pagamento gestores de contas que tenham criado uma interface dedicada devem definir indicadores de desempenho fundamentais e objetivos de nível de serviço transparentes, pelo menos tão exigentes como os definidos para a interface utilizada pelos seus utilizadores de serviços de pagamento em termos de disponibilidade e de fornecimento de dados em conformidade com o artigo 36.º. Essas interfaces, indicadores e objetivos devem ser controlados pelas autoridades competentes e submetidos a testes de esforço.

3. Os prestadores de serviços de pagamento gestores de contas que tenham criado uma interface dedicada devem assegurar que esta interface não cria obstáculos à prestação de serviços de iniciação de pagamentos e de serviços de informação sobre contas. Tais obstáculos podem consistir, designadamente, em impedir a utilização pelos prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, das credenciais emitidas pelos prestadores de serviços de pagamento gestores de contas aos seus clientes, impor o redirecionamento da autenticação ou de outras funções para o prestador de serviços de pagamento gestor de contas, exigir autorizações e registos adicionais para além dos previstos nos artigos 11.º, 14.º e 15.º da Diretiva (UE) 2015/2366 ou exigir verificações adicionais do consentimento dado pelos utilizadores de serviços de pagamento aos prestadores de serviços de iniciação de pagamentos e de serviços de informação sobre contas.

4. Para efeitos dos n.ºs 1 e 2, os prestadores de serviços de pagamento gestores de contas devem controlar a disponibilidade e o desempenho da interface dedicada. Os prestadores de serviços de pagamento gestores de contas devem publicar no respetivo sítio Web estatísticas trimestrais sobre a disponibilidade e o desempenho da interface dedicada e da interface utilizada pelos seus utilizadores de serviços de pagamento.

Artigo 33.º

Medidas de contingência para uma interface dedicada

1. Os prestadores de serviços de pagamento gestores de contas devem incluir, na configuração da interface dedicada, uma estratégia e planos de medidas de contingência caso se verifique um desempenho da interface não conforme com o artigo 32.º, uma indisponibilidade imprevista da interface ou uma avaria nos sistemas. Pode presumir-se a ocorrência de uma indisponibilidade imprevista ou de uma avaria nos sistemas quando cinco pedidos consecutivos de acesso a informação para a prestação de serviços de iniciação de pagamentos ou de serviços de informação sobre contas não tenham resposta em 30 segundos.

2. As medidas de contingência devem incluir planos de comunicação para informar os prestadores de serviços de pagamento que utilizam a interface dedicada das medidas tomadas para restaurar o sistema, bem como uma descrição das opções alternativas imediatamente disponíveis durante este período.

3. Tanto o prestador de serviços de pagamento gestor de contas como os prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, devem comunicar, sem demora, os problemas com interfaces dedicadas descritos no n.º 1 às respetivas autoridades nacionais competentes.

4. No âmbito de um mecanismo de contingência, os prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, devem poder utilizar as interfaces disponibilizadas aos utilizadores de serviços de pagamento para a autenticação e a comunicação com o seu prestador de serviços de pagamento gestor de contas, até que a interface dedicada recupere o nível de disponibilidade e desempenho previsto no artigo 32.º.

5. Para este efeito, os prestadores de serviços de pagamento gestores de contas devem assegurar que os prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, podem ser identificados e basear-se nos procedimentos de autenticação facultados pelo prestador de serviços de pagamento gestor de contas ao utilizador de serviços de pagamento. Sempre que utilizem a interface a que se refere o n.º 4, os prestadores de serviços de pagamento referidos no artigo 30.º, n.º 1, devem:

a) Tomar as medidas necessárias para assegurar que não tenham acesso, armazenem ou tratem dados para outros fins que não a prestação do serviço solicitado pelo utilizador de serviços de pagamento;

b) Continuar a cumprir as obrigações decorrentes do artigo 66.º, n.º 3, e do artigo 67.º, n.º 2, da Diretiva (UE) 2015/2366, respetivamente;

c) Registar os dados acedidos através da interface operada pelo prestador de serviços de pagamento gestor de contas para prestar serviços aos seus utilizadores de serviços de pagamento e fornecer, a pedido e sem demora injustificada, os ficheiros de registo à respetiva autoridade nacional competente;

d) Justificar devidamente junto da respetiva autoridade nacional competente, a pedido e sem demora injustificada, a utilização da interface disponibilizada aos utilizadores de serviços de pagamento para estes acederem diretamente em linha à sua conta de pagamento;

e) Informar o prestador de serviços de pagamento gestor de contas em conformidade.

6. As autoridades competentes, depois de consultarem a EBA para garantir uma aplicação coerente das seguintes condições, devem isentar os prestadores de serviços de pagamento gestores de contas que tenham optado por uma interface dedicada da obrigação de criar o mecanismo de contingência descrito no n.º 4, caso a interface dedicada satisfaça todas as seguintes condições:

a) Cumpre todas as obrigações relativas a interfaces dedicadas estabelecidas no artigo 32.º;

b) Foi concebida e testada em conformidade com o artigo 30.º, n.º 5, a contento dos prestadores de serviços de pagamento nele referidos;

c) Foi amplamente utilizada, durante pelo menos três meses, pelos prestadores de serviços de pagamento para oferecer serviços de informação sobre contas e serviços de iniciação de pagamentos e confirmar a disponibilidade de fundos para pagamentos baseados em cartões;

d) Os problemas relacionados com a interface dedicada foram resolvidos sem demoras injustificadas.

7. Caso os prestadores de serviços de pagamento gestores de contas não satisfaçam as condições previstas nas alíneas a) e d) durante mais de duas semanas de calendário consecutivas, as autoridades competentes devem revogar a isenção a que se refere o n.º 6. As autoridades competentes devem informar a EBA desta revogação e assegurar que os prestadores de serviços de pagamento gestores de contas criam, com a maior brevidade possível e o mais tardar no prazo de dois meses, o mecanismo de contingência referido no n.º 4.

Artigo 34.º

Certificados

1. Para efeitos de identificação nos termos do artigo 30.º, n.º 1, alínea a), os prestadores de serviços de pagamento devem basear-se nos certificados qualificados de selos eletrónicos referidos no artigo 3.º, n.º 30, do Regulamento (UE) n.º 910/2014, ou nos certificados qualificados de autenticação de sítios Web referidos no artigo 3.º, n.º 39, do mesmo regulamento.

2. Para efeitos do presente regulamento, o número de registo constante dos registos oficiais, nos termos do anexo III, alínea c), ou do anexo IV, alínea c), do Regulamento (UE) n.º 910/2014, é o número de autorização dos prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões, dos prestadores de serviços de informação sobre contas e dos prestadores de serviços de iniciação de pagamentos, incluindo os prestadores de serviços de pagamento gestores de contas que prestem esses serviços, disponível no registo público do Estado-Membro de origem nos termos do artigo 14.º da Diretiva (UE) 2015/2366 ou resultante das notificações de todas as autorizações concedidas ao abrigo do artigo 8.º da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho ([1]), nos termos do artigo 20.º da referida diretiva.

3. Para efeitos do presente regulamento, os certificados qualificados de selos eletrónicos ou de autenticação de sítios Web a que se refere o n.º 1 devem incluir, numa língua de uso corrente no setor financeiro internacional, atributos específicos adicionais em relação a cada um dos seguintes elementos:

a) O papel do prestador de serviços de pagamento, que pode consistir num ou mais dos seguintes serviços:

   i) gestão de contas,

   ii) iniciação de pagamentos,

   iii) informação sobre contas,

   iv) emissão de instrumentos de pagamento baseados em cartões;

b) O nome das autoridades competentes em que o prestador de serviços de pagamento se encontra registado.

4. Os atributos referidos no n.º 3 não devem afetar a interoperabilidade e o reconhecimento dos certificados qualificados de selos eletrónicos ou de autenticação de sítios Web.

([1]) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

Artigo 35.º

Segurança da sessão de comunicação

1. Os prestadores de serviços de pagamento gestores de contas, os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões, os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos devem assegurar, ao procederem ao intercâmbio de dados através da Internet, uma encriptação segura entre as partes comunicantes durante a respetiva sessão de comunicação, a fim de salvaguardar a confidencialidade e a integridade dos dados, utilizando técnicas de encriptação sólidas e amplamente reconhecidas.

2. Os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões, os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos devem manter as sessões de acesso oferecidas pelos prestadores de serviços de pagamento gestores de contas tão breves quanto possível e cessar ativamente a sessão em causa assim que a ação solicitada esteja concluída.

3. Sempre que mantiverem sessões de rede paralelas com o prestador de serviços de pagamento gestor de contas, os prestadores de serviços de informação sobre contas e os prestadores de serviços de iniciação de pagamentos devem assegurar que tais sessões são ligadas de forma segura às sessões correspondentes estabelecidas com o(s) utilizador(es) de serviços de pagamento, de modo a impossibilitar o encaminhamento errado de qualquer mensagem ou informação comunicada entre eles.

4. Os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões com o prestador de serviços de pagamento gestor de contas devem incluir referências inequívocas a cada um dos seguintes elementos:

a) O(s) utilizador(es) de serviços de pagamento e a sessão de comunicação correspondente, de modo a distinguir os vários pedidos do(s) mesmo(s) utilizador(es) de serviços de pagamento;

b) Relativamente aos serviços de iniciação de pagamentos, a identificação única da operação de pagamento iniciada;

c) Relativamente à confirmação da disponibilidade de fundos, a identificação única do pedido relativo ao montante necessário para a execução da operação de pagamento baseada em cartão.

5. Os prestadores de serviços de pagamento gestores de contas, os prestadores de serviços de informação sobre contas, os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de pagamento que emitem instrumentos de pagamento baseados em cartões devem assegurar que, ao comunicarem credenciais de segurança personalizadas e códigos de autenticação, estes nunca são legíveis, direta ou indiretamente, por qualquer membro do seu pessoal.

Em caso de perda de confidencialidade de credenciais de segurança personalizadas sob a sua responsabilidade, esses prestadores devem informar, sem demora injustificada, o utilizador de serviços de pagamento associado às credenciais de segurança personalizadas e o emitente das mesmas.

Artigo 36.º

Intercâmbio de dados

1. Os prestadores de serviços de pagamento gestores de contas devem cumprir cada um dos seguintes requisitos:

a) Fornecer aos prestadores de serviços de informação sobre contas as mesmas informações sobre contas de pagamento designadas e operações de pagamento associadas disponibilizadas ao utilizador de serviços de pagamento quando for diretamente pedido o acesso à informação sobre contas, desde que esta não inclua dados de pagamento sensíveis;

b) Logo após a receção da ordem de pagamento, fornecer aos prestadores de serviços de iniciação de pagamentos as mesmas informações sobre a iniciação e execução da operação de pagamento fornecidas ou disponibilizadas ao utilizador de serviços de pagamento, quando a operação for iniciada diretamente por este último;

c) A pedido, fornecer imediatamente aos prestadores de serviços de pagamento a confirmação, sob a forma de um simples «sim» ou «não», da disponibilidade ou não na conta de pagamento do ordenante do montante necessário para a execução de uma operação de pagamento.

2. Caso ocorra um evento ou erro imprevisto durante o processo de identificação ou autenticação, ou durante o intercâmbio de dados, o prestador de serviços de pagamento gestor de contas deve enviar uma mensagem de notificação ao prestador de serviços de iniciação de pagamentos ou ao prestador de serviços de informação sobre contas e ao prestador de serviços de pagamento que emite instrumentos de pagamento baseados em cartões, explicando o motivo desse evento ou erro imprevisto.

Caso o prestador de serviços de pagamento gestor de contas disponibilize uma interface dedicada nos termos do artigo 32.º, a interface deve assegurar que o prestador de serviços de pagamento que deteta o evento ou erro em causa comunica as mensagens de notificação de eventos ou erros imprevistos aos outros prestadores de serviços de pagamento participantes na sessão de comunicação.

3. Os prestadores de serviços de informação sobre contas devem dispor de mecanismos adequados e eficazes que impeçam o acesso a outras informações que não as relativas a contas de pagamento designadas e operações de pagamento associadas, com o consentimento expresso do utilizador.

4. Os prestadores de serviços de iniciação de pagamento devem fornecer aos prestadores de serviços de pagamento gestores de contas as mesmas informações solicitadas ao utilizador de serviços de pagamento quando este inicia diretamente uma operação de pagamento.

5. Para efeitos da prestação do serviço de informação sobre contas, os prestadores de serviços de informação sobre contas devem poder aceder às informações de contas de pagamento designadas e operações de pagamento associadas detidas pelos prestadores de serviços de pagamento gestores de contas em qualquer uma das seguintes circunstâncias:

a) Sempre que o utilizador de serviços de pagamento solicitar ativamente tais informações;

b) Caso o utilizador de serviços de pagamento não solicite ativamente tais informações, não mais de quatro vezes num período de 24 horas, salvo se for acordada uma frequência mais elevada entre o prestador de serviços de informação sobre contas e o prestador de serviços de pagamento gestor de contas, com o consentimento do utilizador de serviços de pagamento.

CAPÍTULO VI

DISPOSIÇÕES FINAIS

Artigo 37.º

Revisão

Sem prejuízo do disposto no artigo 98.º, n.º 5, da Diretiva (UE) 2015/2366, a EBA revê até 14 de março de 2021 as taxas de fraude referidas no anexo ao presente regulamento, bem como as isenções concedidas ao abrigo do artigo 33.º, n.º 6, em relação às interfaces dedicadas, e, se necessário, apresenta à Comissão projetos de atualização das mesmas nos termos do artigo 10.º do Regulamento (UE) n.º 1093/2010.

Artigo 38.º

Entrada em vigor

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

2. O presente regulamento é aplicável a partir de 14 de setembro de 2019.

3. Todavia, o artigo 30.º, n.ºs 3 e 5, é aplicável a partir de 14 de março de 2019.

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

Feito em Bruxelas, em 27 de novembro de 2017.

Pela Comissão

O Presidente

Jean-Claude JUNCKER

ANEXO

	Taxa de fraude de referência (%) para:	
VLI (valor limiar de isenção)	Pagamentos eletrónicos remotos baseados em cartões	Transferências a crédito eletrónicas remotas
500 EUR	0,01	0,005
250 EUR	0,06	0,01
100 EUR	0,13	0,015