EBA/GL/2014/12

19 de dezembro de 2014

Orientações definitivas

sobre a segurança dos pagamentos efetuados através da internet

Índice

Orientações sobre a segurança dos pagamentos efetuados através da internet

Natureza das presentes orientações

O presente documento contém orientações emitidas nos termos do artigo 16.º do 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 – "EBA"), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão («Regulamento EBA»). Em conformidade com o disposto no artigo 16.º, n.º 3, do Regulamento EBA, as autoridades competentes e as instituições financeiras desenvolvem todos os esforços para dar cumprimento às presentes orientações.

As orientações expressam o ponto de vista da EBA sobre o que constituem práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União Europeia deve ser aplicada num domínio específico. A EBA espera, por conseguinte, que todas as autoridades competentes e instituições financeiras às quais se dirigem as presentes orientações deem cumprimento às mesmas. As autoridades competentes a quem se aplicam as presentes orientações devem cumpri-las incorporando-as nas suas práticas de supervisão conforme for mais adequado (por exemplo, alterando o seu regime jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são dirigidas em primeiro lugar às instituições.

Requisitos de notificação

Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento EBA, as autoridades competentes confirmam à EBA se dão ou se tencionam dar cumprimento às presentes orientações. Caso contrário, indicam as razões da decisão de não cumprimento até 5 de maio de 2015. Na ausência de qualquer notificação dentro do referido prazo, a EBA considera que as autoridades competentes em causa não cumprem as presentes orientações. As notificações deverão ser efetuadas através do envio do modelo constante da Secção 5 para o endereço compliance@eba.europa.eu, com a referência «EBA/GL/2014/12». As notificações são efetuadas por pessoas devidamente autorizadas para o efeito pelas respetivas autoridades competentes.

As notificações são publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.º, n.º 3.

Título I - Âmbito de aplicação e definições

Âmbito de aplicação

1. As presentes Orientações estabelecem um conjunto de requisitos mínimos no campo da segurança dos pagamentos efetuados através da internet. As Orientações têm por base as regras da Diretiva 2007/64/CE[1] («Diretiva de Serviços de Pagamento», DSP) referentes aos requisitos de informação aplicáveis aos serviços de pagamento e às obrigações dos prestadores de serviços de pagamento (PSP) relativamente à prestação de serviços de pagamento. Além disso, o n.º 4 do artigo 10.º da Diretiva exige que as instituições de pagamento disponham de dispositivos sólidos de governação e de mecanismos de controlo interno adequados.

2. As Orientações aplicam-se à prestação de serviços de pagamento disponibilizados através da internet pelos PSP, na aceção do artigo 1.º da Diretiva.

3. As Orientações são dirigidas às instituições financeiras, na aceção do n.º 1 do artigo 4.º do Regulamento (UE) n.º 1093/2010, e às autoridades competentes, na aceção do n.º 2 do artigo 4.º do mesmo Regulamento. As autoridades competentes dos 28 Estados-Membros da União Europeia devem assegurar, sob a sua supervisão, a aplicação das presentes Orientações pelos PSP, na aceção do artigo 1.º da DSP.

4. Além disso, as autoridades competentes podem decidir exigir aos PSP que reportem à autoridade competente que dão cumprimento às Orientações.

5. As presentes Orientações não afetam a validade das «Recomendações relativas à segurança dos pagamentos efetuados através da internet» (o «Relatório»)[2] do Banco Central Europeu. Em particular, o Relatório continua a representar o documento com base no qual os bancos centrais, no âmbito da sua função de superintendência dos sistemas e dos instrumentos de pagamento, devem avaliar a conformidade relativamente à segurança dos pagamentos efetuados através da internet.

6. As Orientações preveem conteúdos mínimos, não afetando as responsabilidade dos PSP em matéria de controlo e de avaliação dos riscos envolvidos nas suas operações de pagamento, de desenvolvimento das suas próprias políticas de segurança detalhadas e de implementação de medidas adequadas de segurança, de contingência, de gestão de incidentes e de continuidade da atividade proporcionais aos riscos inerentes aos serviços de pagamento prestados.

[1] Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro de 2007, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e revoga a Diretiva 97/5/CE - JO L 319 de 5.12.2007

[2] http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1.en.html

7. O objetivo das presentes Orientações é definir requisitos mínimos comuns para os serviços de pagamento prestados através da internet indicados *infra*, independentemente do dispositivo de acesso utilizado:

   - [cartões] a realização de pagamentos com cartão através da internet, incluindo pagamentos com cartão virtual, assim como o registo de dados de pagamentos com cartão para utilização em "carteiras virtuais" ('*wallet solutions*'),

   - [transferências a crédito] a realização de transferências a crédito através da internet,

   - [autorização eletrónica de débito em conta] a emissão e a alteração de autorizações eletrónicas de débito diretos,

   - [moeda eletrónica] transferências de moeda eletrónica entre duas contas de moeda eletrónica através da internet.

8. Quando as Orientações indicam um resultado, este pode ser alcançado através de diferentes meios. As presentes Orientações, para além dos requisitos seguidamente enunciados, disponibilizam exemplos de boas práticas (no Anexo 1), que os PSP são encorajados a adotar, embora não sejam obrigados a fazê-lo.

9. Quando a prestação de serviços e a disponibilização de instrumentos de pagamento é oferecida através de um sistema de pagamento (por exemplo, sistemas de pagamento com cartão, sistemas de transferências a crédito, sistemas de débito direto, etc.), as autoridades competentes e o banco central relevante, que exerce a função de superintendência dos instrumentos de pagamento, devem cooperar, a fim de garantir uma aplicação coerente das Orientações por parte dos agentes responsáveis pelo funcionamento do sistema.

10. Os integradores de pagamento[3] que disponibilizam serviços de iniciação de pagamento são considerados adquirentes de serviços de pagamento através da internet (e, portanto, como PSP) ou prestadores de serviços técnicos externos dos sistemas relevantes ou dos PSP. Neste último caso, os integradores de pagamento devem ser contratualmente obrigados a cumprir as presentes Orientações.

11. Estão excluídos do âmbito de aplicação das presentes Orientações:

   - outros serviços de internet prestados por um PSP através do seu sítio web de pagamento (por exemplo, corretagem eletrónica, contratos celebrados através da internet),

[3] Os integradores de pagamento oferecem ao beneficiário (por exemplo, a entidade de comércio eletrónico) uma interface normalizada para os serviços de iniciação de pagamento fornecidos pelos PSP.

- pagamentos em que a instrução é comunicada através de correio, por telefone, correio de voz ou utilizando tecnologia baseada em SMS (*short message service* ou, por tradução, "serviço de mensagens curtas"),

- pagamentos móveis, exceto pagamentos baseados em navegadores (*browsers*),

- transferências a crédito em que terceiros têm acesso à conta de pagamento do cliente,

- operações de pagamento efetuadas por uma empresa através de redes dedicadas,

- pagamentos com cartão, utilizando cartões pré-pagos físicos ou virtuais anónimos e não recarregáveis em que não existe uma relação contínua entre o emitente e o titular do cartão,

- compensação e liquidação de operações de pagamento.

Definições

12. Para efeitos das presentes Orientações e sem prejuízo das definições fornecidas na DSP, aplicam-se as seguintes definições:

Autenticação é o procedimento que permite ao PSP verificar a identidade de um cliente.

Autenticação forte do cliente é, para efeitos das presentes Orientações, o procedimento baseado na utilização de dois ou mais dos seguintes elementos – categorizados como conhecimento, propriedade e inerência: i) algo que apenas o utilizador conhece, por exemplo uma palavra-passe estática, um código, um número de identificação pessoal; ii) algo que apenas o utilizador possui, por exemplo um dispositivo de autenticação (*token*), um cartão inteligente, um telemóvel; iii) alguma característica inerente ao utilizador, por exemplo, uma característica biométrica, designadamente uma impressão digital. Além disso, os elementos escolhidos devem ser mutuamente independentes, isto é, a violação de um desses elementos não compromete o(s) outro(s). Pelo menos um destes elementos deve ser não reutilizável e não reproduzível (com exceção da inerência) e insuscetível de ser sub-repticiamente furtado através da internet. O procedimento de autenticação forte deve ser concebido de forma a proteger a confidencialidade dos dados de autenticação.

Autorização é um procedimento que verifica se um cliente ou um PSP tem o direito de executar uma determinada ação, por exemplo o direito de transferir fundos ou de ter acesso a dados sensíveis.

Credenciais são as informações, geralmente confidenciais, fornecidas por um cliente ou por um PSP, para efeitos de autenticação. As credenciais podem também dizer respeito à posse de um instrumento físico que contém informações (por exemplo, um gerador de palavras-passe de uso único, um cartão inteligente) ou alguma coisa que o utilizador memoriza ou representa (tais como características biométricas).

Incidente de segurança dos pagamentos de carácter severo é um incidente que tem ou poderá ter um impacto material sobre a segurança, a integridade ou a continuidade dos sistemas relacionados com pagamentos do PSP e/ou a segurança de dados de pagamento sensíveis ou de fundos. A avaliação da materialidade deve incluir o número de potenciais clientes afetados, o montante/valor em risco e o impacto sobre outros PSP ou sobre outras infraestruturas de pagamento.

Análise de risco da operação é a avaliação do risco associado a uma operação específica, tendo em conta critérios como, por exemplo, os padrões de pagamento do cliente (comportamento), o valor da operação relacionada, o tipo de produto e o perfil do beneficiário.

Cartão virtual é uma solução de pagamento baseada num cartão, em que é criado um número de cartão temporário e alternativo, com um período de validade reduzido, uma utilização limitada e um limite de despesa predefinido, que pode ser utilizado para efetuar compras através da internet.

Carteira virtual é a solução que permite a um cliente registar dados relacionados com um ou mais instrumentos de pagamento, a fim de realizar pagamentos com várias entidades de comércio eletrónico.

Título II - Orientações sobre a segurança dos pagamentos efetuados através da internet

Ambiente geral de controlo e de segurança

Governo

1. Os PSP devem implementar e rever regularmente uma política de segurança formal para os serviços de pagamento através da internet.

   1.1 A política de segurança deve ser devidamente documentada, revista regularmente (em conformidade com a Orientação 2.4) e aprovada pela direção de topo. Esta política deve definir os objetivos de segurança e a apetência pelo risco.

   1.2 A política de segurança deve definir funções e responsabilidades, incluindo a função de gestão de riscos com uma linha de reporte direta ao órgão de administração e linhas de reporte para os serviços de pagamento prestados através da internet, incluindo a gestão de dados de pagamento sensíveis relativos à avaliação, ao controlo e à mitigação de riscos.

Avaliação de riscos

2. Os PSP devem realizar e documentar, de forma exaustiva, avaliações de risco relativas à segurança de pagamentos efetuados através da internet e de serviços relacionados, antes da criação do(s) serviço(s) e, de forma regular, após a sua criação .

   2.1 Os PSP, através da sua função de gestão de riscos, devem realizar e documentar avaliações de risco detalhadas para os pagamentos efetuados através da internet e os serviços relacionados. Os PSP devem considerar os resultados do acompanhamento permanente de ameaças de segurança relacionadas com serviços de pagamento através da internet que prestam ou pretendam prestar, tendo em conta: i) as soluções de tecnologia que utilizam, ii) os serviços subcontratados a prestadores externos e iii) o ambiente tecnológico dos clientes. Os PSP devem considerar os riscos associados às plataformas de tecnologia escolhidas, à arquitetura da aplicação, às técnicas e às rotinas de programação, que provenham tanto da sua parte[4] como da parte dos seus clientes[5], assim como os resultados do processo de acompanhamento de incidentes de segurança (ver Orientação 3).

[4] Tais como, a suscetibilidade de o sistema para a sessão de pagamento ser sujeito a intrusão (*hijacking*), a injeção de *SQL (SQL injection)*, a execução de *scripts* maliciosos em vários sítios (*cross-site scripting*), capacidades da memória intermédia excedidas (*buffer overflows*), etc.

[5] Tais como, os riscos associados à utilização de aplicações multimédia, *plug-ins* do navegador (*browser*), *frames*, hiperligações externas, etc.

2.2 Nesta base, os PSP devem determinar se e em que medida podem ser necessárias alterações aos mecanismos de segurança existentes, às tecnologias utilizadas e aos procedimentos ou serviços prestados. Os PSP devem ter em consideração o tempo necessário para implementar as alterações (incluindo junto dos clientes) e devem tomar as medidas transitórias apropriadas para minimizar os incidentes de segurança e a fraude, assim como potenciais efeitos disruptivos.

2.3 A avaliação de riscos deve ter em conta a necessidade de proteção e de salvaguarda dos dados sensíveis de pagamento.

2.4 Os PSP devem realizar uma análise dos cenários de risco e dos mecanismos de segurança existentes, após incidentes graves que afetem os seus serviços, antes de uma alteração significativa na infraestrutura ou nos procedimentos, e quando são identificadas novas ameaças através de atividades de monitorização de riscos. Além disso, deve ser realizada uma revisão geral da avaliação de riscos, pelo menos, uma vez por ano. Os resultados das avaliações e das análises de risco devem ser submetidos à aprovação da direção de topo.

Monitorização e reporte de incidentes

3. Os PSP devem assegurar, de forma consistente e integrada, a monitorização, o tratamento e o acompanhamento de incidentes de segurança, incluindo as reclamações de clientes relacionadas com segurança. Os PSP devem estabelecer um procedimento de reporte desses incidentes aos órgãos de administração e fiscalização e, em caso de incidentes de segurança dos pagamentos de carácter severo, às autoridades competentes.

3.1 Os PSP devem implementar um processo para monitorizar, tratar e acompanhar os incidentes de segurança e as reclamações de clientes relacionadas com a segurança e devem reportar esses incidentes à direção.

3.2 Os PSP devem estabelecer um procedimento para informar imediatamente as autoridades competentes (*i.e.*, as autoridades de supervisão e de proteção de dados), sempre que existam incidentes de segurança dos pagamentos de carácter severo.

3.3 Os PSP devem possuir um procedimento de cooperação com as autoridades responsáveis pela aplicação da lei relevantes, em caso de incidentes de segurança dos pagamentos de carácter severo, incluindo violações de dados.

3.4 Os PSP adquirentes devem exigir contratualmente que as entidades de comércio eletrónico conservem, tratem e transmitam dados sensíveis de pagamento colaborem com os próprios PSP e com as autoridades responsáveis pela aplicação da lei relevantes, em caso de incidentes de segurança dos pagamentos de carácter severo, incluindo violações de dados. Se um PSP tomar conhecimento de que uma entidade de comércio eletrónico não coopera, como lhe é exigido contratualmente, deverá tomar medidas para fazer cumprir a obrigação contratual ou resolver o contrato.

Controlo e mitigação de riscos

4. Os PSP devem implementar medidas, em consonância com as respetivas políticas de segurança, para mitigação dos riscos identificados. Essas medidas devem incorporar várias camadas de segurança, de modo a que a falha de uma linha de defesa seja mitigada pela seguinte ('*defense in depth*' ou, por tradução, "defesa em profundidade").

   4.1 Na criação, no desenvolvimento e na manutenção de serviços de pagamento através da internet, os PSP devem prestar especial atenção à separação adequada de funções em ambientes de tecnologias da informação (TI) (por exemplo, em ambientes de desenvolvimento, de teste e de produção) e à implementação adequada do princípio do «privilégio mínimo» (*'least privilege*') como a base para uma gestão adequada de identidades e de acessos[6].

   4.2 Os PSP devem dispor de soluções de segurança apropriadas para proteger as redes, os sítios web, os servidores e as hiperligações de comunicação contra violações ou ataques. Os PSP devem desativar todas as funções desnecessárias dos servidores, de modo a protegê-los (fortalecê-los) e a eliminar ou a reduzir as vulnerabilidades de aplicações em risco. O acesso de várias aplicações aos dados e aos recursos exigidos deve ser limitado ao mínimo, segundo o princípio do «privilégio mínimo». De forma a limitar a utilização de sítios web «falsos» (que imitam sítios reais dos PSP), os sítios web de operações que oferecem serviços de pagamento através da internet devem ser identificados por certificados de validação digital criados em nome do PSP ou através de outros métodos de autenticação semelhantes.

   4.3 Os PSP devem implementar processos apropriados para monitorizar, detetar e limitar o acesso a: i) dados sensíveis de pagamento e ii) recursos lógicos e físicos críticos, tais como redes, sistemas, bases de dados, módulos de segurança, etc. Os PSP devem criar, conservar e analisar os registos e as pistas de auditoria adequadas.

   4.4 Durante a conceção[7], o desenvolvimento e a manutenção de serviços de pagamento através da internet, os PSP devem assegurar que o princípio da minimização de dados[8] é uma componente essencial da funcionalidade principal: a recolha, o encaminhamento, o processamento, o armazenamento e/ou o arquivamento e a visualização de dados de pagamento sensíveis devem ser mantidos num nível mínimo absoluto.

   4.5 Os mecanismos de segurança para serviços de pagamento através da internet devem ser testadas sob supervisão da função de gestão de riscos, a fim de garantir a sua

[6] «Todos os programas e todos os utilizadores privilegiados dos sistemas devem funcionar utilizando o nível de privilégio mínimo necessário para completar a tarefa.» Consultar Saltzer, J.H. (1974), *Protection and the Control of Information Sharing in Multics», Comunicatios of ACM, Volume 17*, n.º 7, pág. 388.

[7] Privacidade desde a conceção.

[8] A minimização de dados refere-se à política de recolha do mínimo de informação pessoal necessária para executar uma determinada função.

solidez e eficácia. Todas as alterações devem ser submetidas a um processo formal de gestão de alteração, assegurando que as alterações são devidamente planeadas, testadas, documentadas e autorizadas. Os testes devem ser repetidos regularmente e incluir cenários de ataques potenciais relevantes e conhecidos, com base nas alterações realizadas e nas ameaças à segurança observadas.

4.6 Os mecanismos de segurança dos PSP para serviços de pagamento através da internet devem ser periodicamente auditados a fim de assegurar a sua solidez e eficácia. A implementação e o funcionamento de serviços de pagamento através da internet também devem ser auditados. A frequência e o âmbito destas auditorias devem ter em conta os riscos de segurança envolvidos e devem ser proporcionais a estes riscos. As auditorias devem ser realizadas por especialistas acreditados e independentes (internos ou externos). Estes auditores não devem estar envolvidos, seja de que forma for, no desenvolvimento, na implementação ou na gestão operacional dos serviços de pagamento prestados através da internet.

4.7 Quando os PSP subcontratem funções relacionadas com a segurança de serviços de pagamento através da internet, o contrato deve incluir disposições que exijam o cumprimento dos princípios e das linhas de orientação estabelecidas nas presentes Orientações.

4.8 Os PSP que oferecem serviços de aceitação (*acquiring*) devem exigir contratualmente que as entidades de comércio eletrónico que processem (por exemplo, armazenem, tratem ou transmitam) dados de pagamento sensíveis implementem medidas de segurança na sua infraestrutura de TI, em conformidade com as Orientações 4.1 a 4.7, a fim de evitar o furto desses mesmos dados através dos seus sistemas. Se um PSP tomar conhecimento de que um comerciante eletrónico não implementou as medidas de segurança exigidas, deverá tomar medidas para fazer cumprir esta obrigação contratual ou resolver o contrato.

Rastreabilidade

5. Os PSP devem implementar processos que garantam que todas as operações, assim como o fluxo do processo da autorização eletrónica de débito em conta são rastreados adequadamente.

5.1 Os PSP devem assegurar que o seu serviço inclui mecanismos de segurança para o registo detalhado de dados da operação e da autorização eletrónica de débito em conta, incluindo o número sequencial da operação, os carimbos temporais para os dados da operação, as alterações de parametrização, assim como o acesso aos dados da operação e da autorização eletrónica de débito em conta.

5.2 Os PSP devem implementar ficheiros de registo que permitam rastrear qualquer adição, alteração ou exclusão de dados da operação e da autorização eletrónica de débito em conta.

5.3 Os PSP devem consultar e analisar os dados da operação e da autorização eletrónica de débito em conta e garantir que possuem instrumentos para avaliar os ficheiros de registo. As respetivas aplicações apenas devem estar acessíveis a pessoal autorizado.

Mecanismos de controlo específicos e medidas de segurança para pagamentos através da internet

Identificação inicial do cliente, informação

6. Os clientes devem ser devidamente identificados, em conformidade com a legislação europeia relativa à prevenção do branqueamento de capitais[9], e devem confirmar a sua vontade de realizar pagamentos através da internet, antes de lhes ser concedido o acesso a esses mesmos serviços. Os PSP devem, previamente, de forma regular ou se necessário *ad hoc*, fornecer informações adequadas ao cliente, sobre os requisitos necessários (por exemplo, equipamento, procedimentos) para realizar operações de pagamento seguras através da internet e sobre os riscos inerentes.

6.1 Os PSP devem assegurar que o cliente foi sujeito aos procedimentos de simplificados vigilância dos clientes e que forneceu os documentos de identificação adequados[10], assim como informações relacionadas, antes de lhe ser concedido o acesso aos serviços de pagamento através da internet[11].

6.2 Os PSP devem assegurar que a informação prévia[12], fornecida ao cliente, contém detalhes específicos relacionados com os serviços de pagamento através da internet. Estes detalhes devem incluir, sempre que se considere adequado:

- informações claras sobre quaisquer requisitos em termos de equipamento do cliente, *software* ou outros instrumentos necessários (por exemplo, *software* antivírus, *firewalls*),

- orientações para a utilização adequada e segura de credenciais de segurança personalizadas,

[9] Por exemplo, a Diretiva 2005/60/CE do Parlamento Europeu e do Conselho, de 26 de outubro de 2005, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais e de financiamento do terrorismo. JO L 309, 25.11.2005, p. 1-155. Ver também a Diretiva 2006/70/CE da Comissão, de 1 de agosto de 2006, que estabelece medidas de execução da Diretiva 2005/60/CE do Parlamento Europeu e do Conselho no que diz respeito à definição de «pessoa politicamente exposta» e aos critérios técnicos para os procedimentos simplificados de vigilância da clientela e para efeitos de isenção com base numa atividade financeira desenvolvida de forma ocasional ou muito limitada. JO L 214, 4.8.2006, p. 29-34.

[10] Por exemplo, passaporte, cartão de identificação nacional ou assinatura eletrónica avançada.

[11] O processo de identificação do cliente não prejudica quaisquer exceções previstas na legislação vigente de prevenção do branqueamento de capitais. Os PSP não necessitam de realizar um processo separado de identificação do cliente para os serviços de pagamento através da internet, desde que essa identificação já tenha sido realizada, por exemplo, por outros serviços relacionados com o pagamento ou para a abertura de uma conta.

[12] A presente informação complementa o artigo 42.º da DSP, que especifica a informação que os PSP devem fornecer ao utilizador dos serviços de pagamento antes da celebração de um contrato para a prestação de serviços de pagamento.

- uma descrição passo-a-passo do procedimento a observar pelo cliente para a apresentação e a autorização de uma operação de pagamento e/ou a obtenção de informações, incluindo as consequências de cada ação,

- orientações para a utilização adequada e segura de todo o *hardware* e *software* fornecidos ao cliente,

- os procedimentos a observar em caso de perda ou de furto das credenciais de segurança personalizadas ou do *hardware* ou do *software* do cliente para início de sessão ou para execução das operações,

- os procedimentos a observar em caso de suspeita ou de deteção de uma utilização abusiva ,

- uma descrição das responsabilidades e das obrigações do PSP e do cliente, respetivamente, no que respeita à utilização do serviço de pagamento através da internet.

6.3 Os PSP devem assegurar que o contrato-quadro celebrado com o cliente especifica que o PSP pode bloquear uma determinada operação ou o instrumento de pagamento[13] por motivos de segurança. O PSP deve estabelecer o método e os termos da notificação do cliente e a forma como o cliente pode contactar o PSP para que a operação ou o serviço de pagamento através da internet seja "desbloqueado", em conformidade com a DSP.

Autenticação forte do cliente

7. A iniciação de pagamentos através da internet, assim como o acesso a dados de pagamento sensíveis, devem ser protegidos por uma autenticação forte do cliente. Os PSP devem ter implementado um procedimento de autenticação forte do cliente, de acordo com a definição estabelecida nas presentes Orientações.

7.1 [Operações baseadas em cartão/autorização eletrónica de débito em conta/moeda eletrónica] Os PSP devem realizar uma autenticação forte do cliente para a autorização de operações de pagamento através da internet (incluindo operações agrupadas, baseadas em cartão) e para a emissão ou a alteração de autorizações eletrónicas de débito direto. No entanto, os PSP podem adotar medidas alternativas de autenticação do cliente para:

- pagamentos efetuados a beneficiários de confiança incluídos em listas positivas estabelecidas anteriormente para esse cliente,

- operações entre duas contas do mesmo cliente detidas junto do mesmo PSP,

[13] Ver artigo 55.º da DSP sobre os limites de utilização do instrumento de pagamento.

- transferências dentro do mesmo PSP justificadas por uma análise de risco da operação,

- pagamentos de baixo valor, tal como definido na DSP[14].

7.2 A obtenção de acesso ou a alteração de dados sensíveis de pagamento (incluindo a criação e a alteração de listas positivas) requerem uma autenticação forte do cliente. Quando um PSP presta serviços meramente consultivos, sem a apresentação de informação sensível do cliente ou do pagamento, tais como dados do cartão de pagamento, que podem facilmente ser usados de forma inadequada para praticar fraudes, o PSP pode adaptar os seus requisitos de autenticação com base na sua avaliação de riscos.

7.3 [cartões] No caso de operações com cartão, todos os PSP emitentes de cartões devem apoiar a autenticação forte do titular do cartão. Todos os cartões emitidos devem estar tecnicamente preparados (registados) para ser utilizados com a autenticação forte.

7.4 [cartões] Os PSP que oferecem serviços de aceitação (*acquiring*) devem apoiar tecnologias que permitam que o emitente proceda à autenticação forte do titular do cartão para os sistemas de pagamento com cartão nos quais o adquirente participa.

7.5 [cartões] Os PSP que oferecem serviços de aceitação (*acquiring*) devem exigir que a sua entidade de comércio eletrónico promova soluções que permitam ao emitente realizar uma autenticação forte do titular do cartão para operações com cartão através da internet. Podem ser utilizados métodos de autenticação alternativos para categorias pré-definidas de operações de baixo risco, por exemplo, com base na análise de risco da operação ou no caso de pagamentos de baixo valor, nos termos previstos na DSP.

7.6 [cartões] Para os sistemas de pagamento com cartão aceites pelo serviço, os fornecedores de carteiras virtuais devem exigir uma autenticação forte por parte do emitente, no momento em que o legítimo titular regista os dados do cartão pela primeira vez.

7.7 Os fornecedores de carteiras virtuais devem suportar a autenticação forte do cliente, quando estes clientes iniciam a sessão nos serviços de pagamento com carteiras ou realizam operações com cartão através da internet. Podem ser utilizados métodos de autenticação alternativos para categorias pré-definidas de operações de baixo risco, por exemplo, com base na análise de risco da operação ou em casos de pagamentos de baixo valor, nos termos previstos na DSP.

[14] Ver a definição de instrumentos de pagamento de baixo valor no n.º 1 do artigo 34.º e no n.º 1 do artigo 53.º da DSP.

7.8 [cartões] No caso de cartões virtuais, o registo inicial deve ser realizado em ambiente seguro e de confiança[15]. Se o cartão for emitido através da internet, deve ser exigida a autenticação forte do cliente para o processo de criação de dados do cartão virtual.

7.9 Os PSP devem assegurar a autenticação bilateral adequada durante a comunicação com entidades de comércio eletrónico para efeitos de iniciação de pagamentos através da internet e de acesso a dados de pagamento sensíveis.

Pedido e disponibilização de instrumentos de autenticação e/ou de *software* fornecido ao cliente

8. Os PSP devem assegurar que o primeiro pedido do cliente para disponibilização de instrumentos de autenticação necessários para utilizar o serviço de pagamento através da internet e/ou o fornecimento aos clientes de *software* relacionado com o pagamento são efetuados de forma segura.

8.1 O pedido e a disponibilização de instrumentos de autenticação e/ou *software* relacionado com o pagamento, fornecido ao cliente, devem cumprir os seguintes requisitos:

- Os procedimentos relacionados devem ser realizados num ambiente seguro e de confiança, tendo em conta os possíveis riscos que decorrentes de dispositivos que os PSP não controlam,

- Devem ser implementados procedimentos eficazes e seguros para o fornecimento de credenciais de segurança personalizadas, de *software* relacionado com pagamento e de todos os dispositivos personalizados relacionados com pagamentos através da internet. O *software* fornecido através da internet também deve ser assinado digitalmente pelo PSP, a fim de permitir que o cliente verifique a sua autenticidade e assegure que este não foi manipulado,

- [cartões] No caso de operações com cartão, o cliente deve ter a opção de registo para garantir a autenticação forte, independentemente da realização de uma compra específica através da internet. Sempre que, durante a realização de compras na internet, seja disponibilizada a ativação, este processo deve ser efetuado através do encaminhamento do cliente para um ambiente seguro e de confiança.

[15] Os ambientes sob responsabilidade do PSP, onde é assegurada a autenticação adequada do cliente e do PSP que oferece o serviço e a proteção de informação confidencial/sensível, incluem: i) as instalações do PSP; ii) a banca via internet ou outro sítio Web seguro, por exemplo, onde a entidade gestora do sistema de pagamentos oferece características de segurança comparáveis, nomeadamente, as definidas na Orientação 4; ou iii) os serviços de caixa automático (ATM). (No caso dos ATM, é necessária uma autenticação forte do cliente, normalmente fornecida através do chip e do código PIN ou do chip e dados biométricos).

8.2 [cartões] Os emitentes devem encorajar ativamente o titular do cartão a efetuar uma autenticação forte e não devem permitir que os titulares dos cartões ultrapassem essa autenticação senão em casos excecionais e limitados, justificados pelo risco associado a uma determinada operação com cartão.

Tentativas de início de sessão, tempo limite de sessão excedido, validade da autenticação

9. Os PSP devem limitar o número de tentativas de início de sessão ou de autenticação, definir regras para o «tempo limite» da sessão de serviços de pagamento através da internet e definir limites temporais para a validade da autenticação.

9.1 Aquando da utilização de uma palavra-passe de uso único (OTP), para fins de autenticação, os PSP devem assegurar que o período de validade dessas palavras-passe está limitado ao mínimo necessário.

9.2 Os PSP devem estabelecer o número máximo de tentativas falhadas de início de sessão ou de autenticação após o qual o acesso ao serviço de pagamento através da internet é (temporariamente ou permanentemente) bloqueado. Os PSP devem implementar um procedimento seguro para reativar os serviços de pagamento através da internet bloqueados.

9.3 Os PSP devem estabelecer o período máximo após o qual as sessões inativas dos serviços de pagamento através da internet são automaticamente terminadas.

Monitorização de operações

10. Os mecanismos de monitorização de operações concebidos para evitar, detetar e bloquear operações de pagamento fraudulentas devem ser executados antes da autorização final do PSP. As operações de risco elevado ou as suspeitas de tais operações devem ser sujeitas a um procedimento específico de filtragem e de avaliação. Também devem ser implementados mecanismos de monitorização de segurança e de autorização equivalentes para a emissão de autorizações eletrónicas de débito em conta.

10.1 Os PSP devem utilizar sistemas de deteção e de prevenção de fraude para identificar operações suspeitas antes da autorização das operações ou das autorizações eletrónicas de débito em conta. Esses sistemas devem ser baseados, por exemplo, em regras parametrizadas (tais como listas negras de dados de cartões comprometidos ou furtados) e devem monitorizar padrões de comportamento anormais do cliente ou do dispositivo de acesso do cliente (tais como uma alteração do endereço do Protocolo de internet (IP)[16] ou do alcance do IP durante a sessão de serviços de pagamento através da internet, por vezes identificada através de verificações de IP por geolocalização[17],

[16] Um endereço de IP é um código numérico exclusivo que identifica cada computador ligado à internet.

[17] Uma verificação de «Geo-IP» confirma se o país emitente corresponde ao endereço de IP a partir do qual o utilizador está a iniciar a operação.

categorias de entidades de comércio eletrónico atípicas para um determinado cliente ou dados de operações atípicas, etc.). Tais sistemas devem também conseguir detetar sinais de existência de *software* malicioso na sessão (por exemplo, através de validação por *script* contra validação humana) e de cenários de fraude conhecidos. O grau, a complexidade e a adaptabilidade das soluções de monitorização devem ser consentâneos com o resultado da avaliação de riscos e cumprir a legislação de proteção de dados relevante.

10.2 Os PSP adquirentes (*acquirers*) devem implementar sistemas de deteção e de prevenção de fraude para monitorizar as atividades das entidades de comércio eletrónico.

10.3 Os PSP devem realizar quaisquer procedimentos de filtragem e de avaliação de operações dentro de um prazo adequado, de modo a não atrasar indevidamente a iniciação e/ou a execução do serviço de pagamento em questão.

10.4 Sempre que o PSP, de acordo com a sua política de risco, decide bloquear uma operação de pagamento que foi identificada como potencialmente fraudulenta, o PSP deve manter o bloqueio durante o mínimo de tempo possível, até que sejam resolvidos os problemas de segurança.

Proteção de dados sensíveis de pagamento

11. Os dados sensíveis de pagamento devem ser protegidos durante o seu armazenamento, tratamento ou transmissão.

11.1 Todos os dados utilizados para identificar e autenticar os clientes (por exemplo, no início de sessão, ao iniciar pagamentos através da internet e durante a emissão, a alteração ou o cancelamento de autorizações eletrónicas de débito em conta), e a interface do cliente (sítio web do PSP ou da entidade de comércio eletrónico), devem ser protegidos de forma adequada contra roubo e acesso ou alteração não autorizada.

11.2 Os PSP devem assegurar que, durante as transferências de dados de pagamento sensíveis através da internet, é utilizada uma encriptação segura ponto-a-ponto (‘*secure end-to-end encryption*’)[18] entre as partes que comunicam através da respetiva sessão de comunicação, de forma a salvaguardar a confidencialidade e a integridade dos dados, a qual deve usar técnicas de encriptação fortes e amplamente reconhecidas.

11.3 Os PSP que oferecem serviços de aceitação (*acquiring*) devem encorajar as entidades de comércio eletrónico por si apoiadas a não armazenar quaisquer dados de pagamento sensíveis. Caso as entidades de comércio eletrónico processem (ou seja,

[18] A encriptação ponto a ponto refere-se à encriptação na origem da comunicação, enquanto a desencriptação correspondente ocorre apenas no recetor final da comunicação. ETSI EN 302 109 V1.1.1. (2003-06).

armazenem, tratem ou transmitam) dados sensíveis de pagamento, esses PSP devem exigir contratualmente que as entidades de comércio eletrónico implementem as medidas necessárias para proteger esses dados. Os PSP devem realizar verificações regulares e, caso um PSP tome conhecimento de que uma entidade de comércio eletrónico que trata de dados sensíveis de pagamento não implementou as medidas de segurança exigidas, deverá tomar medidas para fazer cumprir esta obrigação contratual ou resolver o contrato.

Sensibilização e educação do cliente e comunicação com o cliente

Educação do cliente e comunicação com o cliente

12. Os PSP devem assistir e orientar os clientes, sempre que necessário, no que se refere à utilização segura dos serviços de pagamento através da internet. Os PSP devem comunicar com os seus clientes de modo a tranquilizá-los sobre a autenticidade das mensagens recebidas.

12.1 Os PSP devem fornecer, pelo menos, um canal seguro[19] para a comunicação permanente com os clientes relativamente à utilização correta e segura do serviço de pagamento através da internet. Os PSP devem informar os clientes sobre a existência deste canal e explicar que qualquer mensagem em nome do PSP enviada através de quaisquer outros meios, tais como e-mails, respeitante à utilização correta e segura do serviço de pagamento através da internet, não é fiável. O PSP deve explicar:

- o procedimento para que os clientes reportem ao PSP suspeitas de pagamentos fraudulentos, incidentes suspeitos ou anomalias durante a utilização de serviços de pagamento através da internet e/ou possíveis tentativas de engenharia social[20],
- os passos seguintes, ou seja, como é que o PSP responderá ao cliente,
- como é que o PSP notificará o cliente sobre (potenciais) operações fraudulentas ou sobre a sua não iniciação, ou como avisará o cliente sobre a ocorrência de ataques (por exemplo, *e-mails* de *phishing*).

12.2 Através do canal seguro, os PSP devem manter os clientes informados sobre atualizações de procedimentos de segurança relativos a serviços de pagamento através da internet. Quaisquer alertas sobre riscos emergentes significativos (como avisos sobre engenharia social) também devem ser disponibilizados através do canal seguro.

[19] Tal como uma caixa de correio eletrónico dedicada no sítio *Web* do PSP ou um sítio web seguro.

[20] Neste contexto, engenharia social refere-se a técnicas de manipulação de pessoas de forma a obter informações (por exemplo através de *e-mail* ou de chamadas telefónicas) ou a recolher informações de redes sociais, para fins de fraude ou de obtenção de acesso não autorizado a um computador ou a uma rede.

12.3 A assistência ao cliente deve ser disponibilizada pelos PSP para todas as questões, reclamações, pedidos de apoio e notificações de anomalias ou incidentes relativos a pagamentos através da internet e a serviços relacionados e os clientes devem ser informados sobre a forma como podem obter essa assistência.

12.4 Os PSP devem iniciar programas de educação e de sensibilização dos clientes concebidos de forma a assegurar que os clientes compreendem, no mínimo, a necessidade de:

- protegerem as suas palavras-passe, *tokens* de segurança, informações pessoais e outros dados confidenciais,
- gerirem adequadamente a segurança do seu dispositivo pessoal (como o computador), através da instalação e da atualização de componentes de segurança (antivírus, firewalls, atualizações de segurança),
- considerarem as ameaças e os riscos significativos relacionados com a transferência de *software* através da internet, no caso de o cliente não estar razoavelmente seguro de que o *software* é genuíno e não foi manipulado,
- utilizarem o sítio web genuíno de pagamento através da internet do PSP.

12.5 Os PSP adquirentes devem exigir que as entidades de comércio eletrónico separem claramente os processos relacionados com pagamentos da loja *online*, de modo a que os clientes identifiquem mais facilmente quando estão a comunicar com o PSP e não com o beneficiário (por exemplo, redirecionando o cliente e abrindo uma janela separada de forma a que o processo de pagamento não seja apresentado numa *frame* da entidade de comércio eletrónico).

Notificações, definição de limites

13. Os PSP devem definir limites para os serviços de pagamento através da internet e podem oferecer aos seus clientes opções para a limitação adicional de riscos dentro destes limites. Os PSP podem também fornecer serviços de alerta e de gestão do perfil do cliente.

13.1 Antes da disponibilização ao cliente dos serviços de pagamento através da internet, os PSP devem definir limites[21] aplicáveis a esses serviços, (por exemplo, um montante máximo para cada pagamento individual ou um montante cumulativo durante um determinado período de tempo) e devem informar os seus clientes em conformidade. Os PSP devem permitir que os clientes desativem a funcionalidade de pagamento através da internet.

[21] Esses limites podem ser aplicados globalmente (por exemplo, a todos os instrumentos de pagamento que permitem pagamentos através da internet) ou individualmente.

Acesso do cliente a informação sobre o estado da iniciação e da execução do pagamento

14. Os PSP devem confirmar aos seus clientes a iniciação do pagamento e devem fornecer, de forma atempada, a informação necessária para a verificação de que a operação de pagamento foi iniciada e/ou executada corretamente.

    14.1 [Operações baseadas em cartão/autorização eletrónica de débito em conta] Os PSP devem fornecer aos clientes, num ambiente seguro e de confiança, um sistema, quase em tempo real, de verificação do estado de execução das operações, assim como, a qualquer momento[22], os saldos das contas.

    14.2 Quaisquer demonstrações eletrónicas detalhadas devem ser disponibilizadas num ambiente seguro e de confiança. Sempre que os PSP informem os clientes sobre a disponibilidade de demonstrações eletrónicas (por exemplo, de forma regular, após a emissão de uma demonstração eletrónica periódica, ou numa base *ad hoc*, após a execução de uma operação) através de um canal alternativo, tal como através de SMS, de *e-mail* ou de carta, os dados de pagamento sensíveis não devem ser incluídos nessas comunicações ou, caso sejam incluídos, devem ser ocultados.

[22] Exceto durante a indisponibilidade excecional do sistema devida a motivos de manutenção técnica ou a incidentes graves.

Anexo 1: Exemplos de boas práticas

Complementarmente aos requisitos *supra* estabelecidos, as presentes Orientações descrevem algumas boas práticas a que os PSP e os intervenientes relevantes no mercado são encorajados, mas não obrigados, a adotar. De forma a facilitar a referência, os Capítulos aos quais as presentes boas práticas se aplicam são indicados explicitamente.

Ambiente geral de controlo e de segurança

Governo

BP 1: A política de segurança pode ser estabelecida num documento dedicado.

Controlo e mitigação de riscos

BP 2: Os PSP podem fornecer ferramentas de segurança (por exemplo, dispositivos e/ou navegadores personalizados, devidamente protegidos) para proteger a *interface* do cliente contra a utilização ilegal ou contra ataques (por exemplo, ataques de "*Man in the Browser*" (MITB)).

Rastreabilidade

BP 3: Os PSP que oferecem serviços de aceitação (*acquiring*) podem exigir contratualmente às entidades de comércio eletrónico que armazenam informações de pagamento que implementem processos adequados para apoiar a rastreabilidade.

Mecanismos de controlo específicos e medidas de segurança específicas para pagamentos através da internet

Identificação inicial do cliente, informação

BP 4: O cliente pode assinar um contrato de prestação de serviço dedicado para a execução de operações de pagamento através da internet, em substituição da inclusão de condições num contrato de prestação de serviço geral mais abrangente assinado com o PSP.

BP 5: Os PSP também podem assegurar que os clientes recebem, numa base permanente ou, se aplicável, numa base *ad hoc* e através dos meios apropriados (por exemplo, folhetos, sítios web), instruções claras e simples que explicam as suas responsabilidades relativamente à utilização segura do serviço.

Autenticação forte do cliente

BP 6: [cartões] Nas operações baseadas em cartão através da internet, as entidades de comércio eletrónico podem apoiar a autenticação forte do titular do cartão pelo emitente.

BP 7: Por conveniência do cliente, os PSP podem considerar a utilização de um único instrumento de autenticação forte do cliente para todos os serviços de pagamento através da internet. Isto pode aumentar a aceitação da solução entre os clientes e facilitar a sua utilização adequada.

BP 8: A autenticação forte do cliente pode incluir elementos que liguem a autenticação a um determinado montante e beneficiário. Isto pode proporcionar aos clientes uma maior certeza durante a autorização de pagamentos. A solução de tecnologia que permite a ligação entre a autenticação forte dos dados e os dados da operação deve estar protegida contra a manipulação.

Proteção de dados sensíveis de pagamento

BP 9: É recomendável que as entidades de comércio eletrónico que tratem dados sensíveis de pagamento deem formação adequada aos seus colaboradores de gestão de fraudes e atualizem a sua formação regularmente, a fim de assegurar que o conteúdo permanece relevante para um ambiente de segurança dinâmico.

Educação do cliente e comunicação com o cliente

BP 10: É recomendável que os PSP que ofereçam serviços de aceitação (*acquiring*) desenvolvam programas sobre a prevenção de fraude para as entidades de comércio eletrónico por si apoiadas.

Notificações, definição de limites

BP 11: Dentro dos limites estabelecidos, os PSP podem fornecer aos seus clientes um sistema para gerir os limites de serviços de pagamento através da internet num ambiente seguro e de confiança.

BP 12: Os PSP podem implementar alertas para os clientes, tais como chamadas telefónicas ou mensagens *SMS*, para operações de pagamento consideradas suspeitas ou de risco elevado, de acordo com as suas políticas de gestão de riscos.

BP 13: Os PSP podem permitir que os clientes definam regras personalizadas gerais como parâmetros para o seu comportamento com vista aos pagamentos através da internet e serviços relacionados, por exemplo, regras que estabeleçam que os clientes apenas iniciarão pagamentos a partir de determinados países e que os pagamentos iniciados a partir de qualquer outro local devem ser bloqueados, ou uma regra que estabeleça que os clientes podem incluir determinados beneficiários em listas positivas ou negativas.