Diretrizes 06/2020 sobre a interação entre a Segunda Diretiva Serviços de Pagamento e o RGPD

Versão 2.0

Adotadas em 15 de dezembro de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Histórico das versões

Versão 2.0	15.12.2020	Adoção das Diretrizes após consulta pública
Versão 1.0	17.7.2020	Adoção das Diretrizes para consulta pública

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n.º 1, alínea e), do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (a seguir designado por «RGPD»),

Tendo em conta o Acordo EEE, nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta o artigo 12.º e o artigo 22.º do seu regulamento interno,

Considerando o seguinte:

(1) O Regulamento Geral sobre a Proteção de Dados estabelece um conjunto coerente de regras para o tratamento de dados pessoais em toda a UE.

(2) A segunda Diretiva Serviços de Pagamento [(Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, publicada em 23 de dezembro de 2015, a seguir designada por «DSP2»)] revoga a Diretiva 2007/64/CE e estabelece novas regras para garantir segurança jurídica aos consumidores, aos comerciantes e às empresas na cadeia de pagamentos e modernizar o quadro jurídico para o mercado dos serviços de pagamento[2]. Os Estados-Membros tinham de transpor a DSP2 para o direito nacional até 13 de janeiro de 2018.

(3) Um elemento importante da DSP2 é a introdução de um quadro jurídico para novos serviços de iniciação de pagamentos e serviços de informação sobre contas. A DSP2 permite que estes novos prestadores de serviços de pagamento obtenham acesso às contas de pagamento dos titulares dos dados para efeitos de prestação dos referidos serviços.

(4) No que diz respeito à proteção de dados, o artigo 94.º, n.º 1, da DSP2 estabelece que qualquer tratamento de dados pessoais, incluindo a prestação de informação sobre esse tratamento, para efeitos da DSP2 é efetuado em conformidade com o RGPD[3] e com o Regulamento (UE) 2018/1725.

(5) O considerando 89 da DSP2 afirma que, caso os dados pessoais sejam tratados para efeitos da mesma diretiva, deve ser especificado o objetivo exato do tratamento, deve ser indicada a base jurídica aplicável, devem ser cumpridos os requisitos de segurança aplicáveis estabelecidos no RGPD e devem ser respeitados os princípios da necessidade, da proporcionalidade, da limitação da finalidade e do período proporcionado de conservação de dados. De igual modo, a proteção de dados desde a conceção e a proteção de dados por defeito deverão estar incorporadas em todos os sistemas de tratamento de dados desenvolvidos e utilizados no quadro da DSP2[4].

(6) O considerando 93 da DSP2 afirma que os prestadores de serviços de iniciação de pagamentos e os prestadores de serviços de informação sobre contas, por um lado, e o prestador do serviço de

---

1 As referências a «Estados-Membros» efetuadas ao longo do presente documento devem ser entendidas como referências a «Estados do EEE».

2 Considerando 6 da DSP2.

3 A DSP2 é anterior ao RGPD e, por conseguinte, ainda remete para a Diretiva 95/46/CE. O artigo 94.º do RGPD refere que as remissões para a Diretiva 95/46/CE revogada são consideradas remissões para o RGPD.

4 Considerando 89 da DSP2.

pagamento que gere a conta, por outro, devem observar os requisitos necessários em matéria de proteção e segurança dos dados estabelecidos ou referidos na mesma diretiva ou incluídos em normas técnicas de regulamentação.

ADOTOU AS SEGUINTES DIRETRIZES

1. INTRODUÇÃO

1. A segunda Diretiva Serviços de Pagamento (a seguir designada por «DSP2») introduziu um conjunto de novidades no domínio dos serviços de pagamento. Embora a DSP2 crie novas oportunidades para os consumidores e reforce a transparência neste domínio, a sua aplicação suscita algumas dúvidas e preocupações no que diz respeito à necessidade de manter o pleno controlo dos titulares dos dados sobre os seus dados pessoais. O Regulamento Geral sobre a Proteção de Dados (a seguir designado por «RGPD») é aplicável ao tratamento de dados pessoais, incluindo atividades de tratamento realizadas no contexto dos serviços de pagamento na aceção da DSP2[5]. Por conseguinte, os responsáveis pelo tratamento que atuam no domínio abrangido pela DSP2 devem sempre assegurar o cumprimento dos requisitos do RGPD, incluindo os princípios da proteção de dados estabelecidos no artigo 5.º do RGPD, bem como as disposições aplicáveis da Diretiva Privacidade Eletrónica[6]. Embora a DSP2[7] e as normas técnicas de regulamentação relativas à autenticação forte do cliente e às normas abertas de comunicação comuns e seguras (a seguir designadas por «NTR»[8]) contenham algumas disposições relativas à proteção e à segurança dos dados, surgiu incerteza quanto à interpretação destas disposições, bem como à interação entre o quadro geral da proteção de dados e a DSP2.

2. Em 5 de julho de 2018, o CEPD publicou uma carta relativa à DSP2 na qual clarificou algumas questões relacionadas com a proteção de dados pessoais no âmbito da mesma diretiva e, em especial, com o tratamento de dados pessoais de partes não contratantes (os chamados «dados de parte silenciosa») por prestadores de serviços de informação sobre contas (PSIC) e prestadores do serviço de iniciação do pagamento (PSIP), com os procedimentos de comunicação e de retirada do consentimento, com as NTR e com a cooperação entre os prestadores de serviços de pagamento que gerem as contas (PSPGC) no âmbito das medidas de segurança. Entretanto, o trabalho de preparação das presentes diretrizes incluiu a recolha de contributos de partes interessadas, por escrito e num evento específico, a fim de identificar os desafios mais prementes.

3. As presentes diretrizes visam fornecer mais orientações sobre os aspetos da proteção de dados no contexto da DSP2, e em especial sobre a relação entre as disposições aplicáveis do RGPD e da DSP2. As presentes diretrizes incidem principalmente no tratamento de dados pessoais pelos PSIC

5 Artigo 1.º, n.º 1, do RGPD.

6 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas); JO L 201 de 31.7.2002, p. 37.

7 Artigo 94.º da DSP, etc.

8 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); C/2017/7782; JO L 69 de 13.3.2018, p. 23; disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R0389&from=PT

e pelos PSIP. Por conseguinte, o presente documento aborda as condições para conceder acesso às informações sobre a conta de pagamento pelos PSPGC e o tratamento de dados pessoais pelos PSIP e pelos PSIC, incluindo os requisitos e salvaguardas relativos ao tratamento de dados pessoais pelos PSIP e pelos PSIC para além das finalidades iniciais para que os dados foram recolhidos, principalmente se tal recolha tiver ocorrido no contexto da prestação de um serviço de informação sobre contas[9]. O presente documento aborda também diferentes conceitos de consentimento explícito ao abrigo da DSP2 e do RGPD, o tratamento de «dados de parte silenciosa», o tratamento de categorias especiais de dados pessoais pelos PSIP e pelos PSIC e a aplicação dos principais princípios da proteção de dados estabelecidos no RGPD, incluindo a minimização dos dados, a transparência, a responsabilidade e as medidas de segurança. A DSP2 implica responsabilidades multidisciplinares nos domínios, nomeadamente, da proteção dos consumidores e do direito da concorrência. O âmbito de aplicação das presentes diretrizes não abrange considerações relativas a estes domínios do direito.

4. Para facilitar a leitura das diretrizes, apresentam-se em seguida as principais definições utilizadas no presente documento.

1.1 Definições

«Prestador de serviços de informação sobre contas» (PSIC), prestador de um serviço em linha para prestação de informações consolidadas sobre uma ou mais contas de pagamento detidas pelo utilizador de serviços de pagamento junto de outro ou outros prestadores de serviços de pagamento;

«Prestador de serviços de pagamento que gere a conta» (PSPGC), um prestador de serviços de pagamento que disponibiliza e mantém contas de pagamento para um ordenante;

«Minimização dos dados», um princípio da proteção de dados segundo o qual os dados pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados;

«Ordenante», uma pessoa singular ou coletiva titular de uma conta de pagamento que autoriza uma ordem de pagamento a partir dessa conta, ou, na falta de conta de pagamento, a pessoa singular ou coletiva que emite uma ordem de pagamento;

«Beneficiário», uma pessoa singular ou coletiva que seja o destinatário previsto dos fundos que foram objeto de uma operação de pagamento;

«Conta de pagamento», uma conta detida em nome de um ou mais utilizadores de serviços de pagamento que é utilizada para a execução de operações de pagamento;

«Prestador do serviço de iniciação do pagamento» (PSIP), prestador de um serviço que inicia uma ordem de pagamento a pedido do utilizador do serviço de pagamento relativamente a uma conta de pagamento detida noutro prestador de serviços de pagamento;

«Prestador de serviços de pagamento», uma entidade a que se refere o artigo 1.º, n.º 1, da DSP2[10] ou uma pessoa singular ou coletiva que beneficie de uma isenção por força do artigo 32.º ou 33.º da DSP2;

---

9 Um serviço de informação sobre contas consiste num serviço em linha para prestação de informações consolidadas sobre uma ou mais contas de pagamento detidas pelo utilizador de serviços de pagamento junto de outro ou outros prestadores de serviços de pagamento.

10 Nos termos do seu artigo 1.º, n.º 1, a DSP2 estabelece as regras nos termos das quais os Estados-Membros distinguem as seguintes categorias de *prestadores de serviços de pagamento*:

«Utilizador de serviços de pagamento», uma pessoa singular ou coletiva que utiliza um serviço de pagamento a título de ordenante ou de beneficiário, ou a ambos os títulos;

«Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

«Proteção de dados desde a conceção», medidas técnicas ou organizativas incorporadas num produto ou serviço, concebidas para aplicar princípios da proteção de dados de forma eficaz e integrar as salvaguardas necessárias no tratamento de modo a cumprir os requisitos do RGPD e proteger os direitos dos titulares dos dados;

«Proteção de dados por defeito», medidas técnicas e organizativas adequadas aplicadas no produto ou serviço para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento;

«NTR», 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;

«Terceiros prestadores de serviços» *(TPS)* refere-se aos PSIP e aos PSIC.

1.2 Serviços ao abrigo da DSP2

5. A DSP2 introduz dois novos tipos de (prestadores de) serviços de pagamento: os PSIP e os PSIC. O anexo I da DSP2 contém os oito serviços de pagamento abrangidos pela mesma diretiva.

6. Os PSIP prestam serviços que iniciam ordens de pagamento a pedido do utilizador do serviço de pagamento relativamente a uma conta de pagamento de um utilizador detida noutro prestador de serviços de pagamento[11]. Um PSIP pode solicitar a um PSPGC (geralmente um banco) que inicie uma operação em nome do utilizador do serviço de pagamento. O utilizador (do serviço de pagamento) pode ser uma pessoa singular (titular dos dados) ou coletiva.

---

a) Instituições de crédito, na aceção do artigo 4.º, n.º 1, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, incluindo as suas sucursais, na aceção do ponto 17 do n.º 1 desse artigo, quer a sede dessas sucursais esteja situada na União, quer, nos termos do artigo 47.º da Diretiva 2013/36/UE e do direito nacional, fora da União;
b) Instituições de moeda eletrónica, na aceção do artigo 2.º, ponto 1, da Diretiva 2009/110/CE, incluindo, nos termos do artigo 8.º dessa diretiva e do direito nacional, as suas sucursais, caso essas sucursais estejam situadas na União e a sua sede esteja situada fora da União, na medida em que os serviços de pagamento prestados por essas sucursais estejam associados à emissão de moeda eletrónica;
c) Instituições de giro postal autorizadas pelo direito nacional a prestar serviços de pagamento;
d) Instituições de pagamento;
e) O BCE e os bancos centrais nacionais, quando não atuem na qualidade de autoridades monetárias ou de outras autoridades públicas;
f) Os Estados-Membros ou as respetivas autoridades regionais ou locais, quando não atuem na qualidade de autoridades públicas.

11 Artigo 4.º, ponto 15, da DSP2.

7. Os PSIC prestam serviços em linha para prestação de informações consolidadas sobre uma ou mais contas de pagamento detidas pelo utilizador de serviços de pagamento junto de outro ou outros prestadores de serviços de pagamento[12]. Segundo o considerando 28 da DSP2, o utilizador de serviços de pagamento pode ter imediatamente uma visão global da sua situação financeira num dado momento.

8. No que diz respeito aos serviços de informação sobre contas, podem ser oferecidos vários tipos diferentes de serviços, com ênfase em diferentes elementos e finalidades. Por exemplo, alguns prestadores de serviços podem oferecer aos utilizadores serviços como o planeamento orçamental ou o acompanhamento das despesas. O tratamento de dados pessoais no contexto destes serviços é abrangido pela DSP2. Os serviços que implicam verificações da solvabilidade do utilizador de serviços de pagamento ou serviços de auditoria prestados com base na recolha de informações através de um serviço de informação sobre contas não se inserem no âmbito de aplicação da DSP2 e, por conseguinte, regem-se pelo RGPD. Além disso, as contas que não são de contas de pagamento (por exemplo, poupanças, investimentos) também não são abrangidas pela DSP2. Em qualquer caso, o RGPD é o quadro jurídico aplicável ao tratamento de dados pessoais.

Exemplo 1:

A Bons Pagamentos é uma empresa que presta um serviço em linha assente na prestação de informações sobre uma ou mais contas de pagamento através de uma aplicação móvel a fim de proporcionar uma visão geral da situação financeira (um serviço de informação sobre contas). Com este serviço, o utilizador de serviços de pagamento pode ver ao mesmo tempo os saldos e as operações recentes em duas ou mais contas de pagamento em bancos diferentes. É também disponibilizada, se for essa a opção do utilizador de serviços de pagamento, uma categorização das despesas e das receitas de acordo com diferentes tipologias (salário, lazer, energia, crédito hipotecário, etc.), de forma a apoiar o planeamento financeiro do utilizador em causa. Nesta aplicação, a Bons Pagamentos também presta um serviço que inicia pagamentos diretamente a partir da(s) conta(s) de pagamento designada(s) dos utilizadores (um serviço de iniciação do pagamento).

9. Tendo em vista a prestação destes serviços, a DSP2 estabelece as condições legais em que os PSIP e os PSIC podem aceder às contas de pagamento para prestar um serviço ao utilizador de serviços de pagamento.

10. O artigo 66.º, n.º 1, e o artigo 67.º, n.º 1, da DSP2 determinam que o acesso e recurso aos serviços de pagamento e de informação sobre contas constituem direitos do utilizador de serviços de pagamento. Por conseguinte, o utilizador de serviços de pagamento deve manter total liberdade relativamente ao exercício deste direito e não pode ser obrigado a exercê-lo.

11. O acesso às contas de pagamento e a utilização de informações sobre as contas de pagamento são parcialmente regulamentados pelos artigos 66.º e 67.º da DSP2, que contêm salvaguardas relativas à proteção de dados (pessoais). O artigo 66.º, n.º 3, alínea f), da DSP2 estabelece que um PSIP não pode exigir ao utilizador de serviços de pagamento quaisquer outros dados além dos necessários para prestar o serviço de iniciação do pagamento, e o artigo 66.º, n.º 3, alínea g), da DSP2 estabelece que um PSIP não pode utilizar nem armazenar dados nem aceder aos mesmos para outros fins que não sejam a prestação do serviço de iniciação do pagamento expressamente solicitado pelo utilizador de serviços de pagamento. Além disso, o artigo 67.º, n.º 2, alínea d), da DSP2 limita o acesso dos PSIC às informações das contas de pagamento designadas e das

[12] Artigo 4.º, ponto 16, da DSP2.

operações de pagamento associadas, enquanto o artigo 67.º, n.º 2, alínea f), da DSP2 estabelece que os PSIC não podem utilizar nem armazenar dados nem aceder aos mesmos para outros fins que não sejam a prestação do serviço de informação sobre contas expressamente solicitado pelo utilizador de serviços de pagamento, de acordo com as regras em matéria de proteção de dados. Estas regras salientam que, no contexto dos serviços de informação sobre contas, os dados pessoais apenas podem ser recolhidos para finalidades determinadas, explícitas e legítimas. Por conseguinte, um PSIC deve explicitar no contrato as finalidades específicas para que serão tratados dados pessoais no âmbito da informação sobre contas, no contexto dos serviços de informação sobre contas por ele prestados. O contrato deve ser lícito, leal e transparente, nos termos do artigo 5.° do RGPD, bem como cumprir outras leis relativas à proteção dos consumidores.

12. Consoante as circunstâncias específicas, os prestadores de serviços de pagamento podem ser responsáveis pelo tratamento ou subcontratantes nos termos do RGPD. Nas presentes diretrizes, os «responsáveis pelo tratamento» são os prestadores de serviços de pagamento que, individualmente ou em conjunto com outras partes, determina as finalidades e os meios de tratamento de dados pessoais. As Diretrizes 07/2020 do CEPD, relativas aos conceitos de responsável pelo tratamento e subcontratante no RGPD, contêm mais orientações sobre esta questão.

2 RAZÕES LEGÍTIMAS E TRATAMENTO POSTERIOR AO ABRIGO DA DSP2

2.1 Razões legítimas para o tratamento

13. Nos termos do RGPD, os responsáveis pelo tratamento devem ter um fundamento jurídico para tratar dados pessoais. O artigo 6.º, n.º 1, do RGPD constitui uma lista exaustiva e restritiva de seis fundamentos jurídicos para o tratamento de dados pessoais ao abrigo do RGPD[13]. Cabe ao responsável pelo tratamento definir o fundamento jurídico adequado e assegurar que todas as condições associadas ao mesmo se encontram preenchidas. A determinação do fundamento válido e mais adequado numa determinada situação depende das circunstâncias em que o tratamento ocorre, incluindo a finalidade do tratamento e a relação entre o responsável pelo tratamento e o titular dos dados.

2.2 Artigo 6.º, n.º 1, alínea b), do RGPD (o tratamento é necessário para a execução de um contrato)

14. Os serviços de pagamento são prestados numa base contratual entre o utilizador e o prestador do serviço de pagamento. Conforme referido no considerando 87 da DSP2, esta diretiva «*deverá dizer exclusivamente respeito às obrigações e responsabilidades contratuais entre o utilizador do serviço de pagamento e o prestador do serviço de pagamento*». No que diz respeito ao RGPD, o principal fundamento jurídico para o tratamento de dados pessoais para a prestação de serviços de pagamento é o artigo 6.º, n.º 1, alínea b), do RGPD, ou seja, a necessidade do tratamento para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados.

15. Os serviços de pagamento ao abrigo da DSP2 são definidos no anexo I da mesma diretiva. A prestação destes serviços, na aceção da DSP2, é um requisito da celebração de um contrato em que as partes têm acesso aos dados da conta de pagamento do utilizador do serviço de pagamento. Estes prestadores de serviços de pagamento têm de ser também operadores licenciados. No que se refere aos serviços de iniciação de pagamentos e aos serviços de informação sobre contas ao

---

[13] Nos termos do artigo 6.º, o tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:

(a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

(b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;

(c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;

(d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;

(e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;

(f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

abrigo da DSP2, os contratos podem conter cláusulas que também imponham condições sobre serviços adicionais não regulados pela DSP2. As *Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados* do CEPD esclarecem que os responsáveis pelo tratamento devem avaliar que tratamento de dados pessoais é objetivamente necessário para a execução do contrato. As referidas diretrizes salientam que a justificação da necessidade depende da natureza do serviço, das perspetivas e expectativas mútuas das partes do contrato, da lógica do contrato e dos elementos essenciais do contrato.

16. As Diretrizes 2/2019 do CEPD também clarificam que, à luz do artigo 7.º, n.º 4, do RGPD, existe uma distinção entre as atividades de tratamento necessárias para a execução de um contrato e as cláusulas que tornam o serviço subordinado a determinadas atividades de tratamento que não são, de facto, necessárias para a execução do contrato. A expressão «necessário para a execução» exige claramente algo mais do que uma cláusula contratual[14]. O responsável pelo tratamento deve poder demonstrar de que modo o objeto principal do contrato específico com o titular dos dados não pode, na realidade, ser executado se o tratamento específico dos dados pessoais em questão não ocorrer. A simples referência ou menção do tratamento de dados num contrato não é suficiente para inserir o tratamento em causa no âmbito de aplicação do artigo 6.º, n.º 1, alínea b), do RGPD.

17. O artigo 5.º, n.º 1, alínea b), do RGPD estabelece o princípio da limitação das finalidades, segundo o qual os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Ao avaliar se o artigo 6.º, n.º 1, alínea b), constitui um fundamento jurídico adequado para um serviço (de pagamento) em linha, deve ter-se em conta o fim, a finalidade ou o objetivo específicos do serviço[15]. As finalidades do tratamento devem ser claramente especificadas e comunicadas ao titular dos dados, em conformidade com as obrigações de limitação das finalidades e de transparência do responsável pelo tratamento. A avaliação do que é «necessário» implica uma avaliação combinada, baseada em factos, do tratamento «para o objetivo prosseguido e da sua menor intrusão em comparação com outras opções para atingir o mesmo objetivo». O artigo 6.º, n.º 1, alínea b), não abrange o tratamento útil mas não objetivamente necessário para a execução do serviço contratual ou para diligências pré-contratuais relevantes a pedido do titular dos dados, mesmo que tal seja necessário para outros fins comerciais do responsável pelo tratamento[16].

18. As Diretrizes 2/2019 do CEPD esclarecem que os contratos não podem expandir artificialmente as categorias de dados pessoais ou os tipos de operações de tratamento que o responsável pelo tratamento tem de efetuar para a execução do contrato, na aceção do artigo 6.º, n.º 1, alínea b)[17]. As referidas diretrizes também referem casos em que podem ser criadas situações de «pegar ou largar» para os titulares dos dados que apenas possam estar interessados num dos serviços. Tal pode acontecer quando o responsável pelo tratamento pretende agregar vários serviços distintos ou elementos de um serviço com diferentes finalidades, características ou lógica fundamentais num único contrato. Sempre que o contrato consista em vários serviços ou elementos de um

---

14 Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, CEPD, página 9.

15 *Idem*.

16 *Idem*, página 9.

17 *Idem*, página 10.

serviço distintos que, de facto, podem ser razoavelmente prestados independentemente uns dos outros, a aplicabilidade do artigo 6.º, n.º 1, alínea b), deve ser avaliada no contexto de cada um desses serviços, isoladamente, verificando-se o que é objetivamente necessário para prestar cada um dos serviços individuais que o titular dos dados tenha ativamente solicitado ou aceite[18].

19. Em conformidade com as diretrizes supramencionadas, os responsáveis pelo tratamento têm de avaliar o que é objetivamente necessário para a execução do contrato. Quando os responsáveis pelo tratamento não podem demonstrar que o tratamento dos dados pessoais da conta de pagamento é objetivamente necessário para a prestação de cada um dos serviços isoladamente, o artigo 6.º, n.º 1, alínea b), do RGPD não é um fundamento jurídico válido para o tratamento. Nestes casos, o responsável pelo tratamento deverá considerar outro fundamento jurídico para o tratamento.

2.3 Prevenção da fraude

20. Nos termos do artigo 94.º, n.º 1, da DSP2, os Estados-Membros devem permitir o tratamento de dados pessoais pelos sistemas de pagamento e pelos prestadores de serviços de pagamento quando tal for necessário para salvaguardar a prevenção, a investigação e a deteção de fraudes em matéria de pagamentos. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção da fraude pode constituir um interesse legítimo do prestador de serviços de pagamento em causa, desde que a esse interesse não se sobreponham os interesses ou os direitos e liberdades fundamentais do titular dos dados[19]. As atividades de tratamento para efeitos de prevenção da fraude devem basear-se numa avaliação cuidada, caso a caso, realizada pelo responsável pelo tratamento, em conformidade com o princípio da responsabilidade. Além disso, para prevenir a fraude, os responsáveis pelo tratamento poderão também ser sujeitos a obrigações legais específicas subjacentes ao tratamento de dados pessoais.

2.4 Tratamento posterior (PSIC e PSIP)

21. O artigo 6.º, n.º 4, do RGPD determina as condições do tratamento de dados pessoais para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos. Mais concretamente, este tratamento posterior pode ocorrer se se basear em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, se o titular dos dados o tiver consentido ou se o tratamento para outros fins for compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos.

22. O artigo 66.º, n.º 3, alínea g), e o artigo 67.º, n.º 2, alínea f), da DSP2 devem ser devidamente tidos em consideração. Conforme referido acima, o artigo 66.º, n.º 3, alínea g), da DSP2 estabelece que os PSIP não podem utilizar nem armazenar dados nem aceder aos mesmos para outros fins que não sejam a prestação do serviço de iniciação do pagamento expressamente solicitado pelo ordenante. O artigo 67.º, n.º 2, alínea f), da DSP2 estabelece que os PSIC não podem utilizar nem armazenar dados nem aceder aos mesmos para outros fins que não sejam a prestação do serviço de informação sobre contas expressamente solicitado pelo utilizador de serviços de pagamento, de acordo com as regras em matéria de proteção de dados.

23. Consequentemente, o artigo 66.º, n.º 3, alínea g), e o artigo 67.º, n.º 2, alínea f), da DSP2 limitam consideravelmente as possibilidades de tratamento para outras finalidades, na medida em que este tratamento apenas é permitido se o titular dos dados o tiver consentido nos termos do

18 *Idem*, página 12.
19 Considerando 47 do RGPD.

artigo 6.º, n.º 1, alínea a), do RGPD ou se tal tratamento for definido pelo direito da União ou pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito, nos termos do artigo 6.º, n.º 4, do RGPD. Nos casos em que o tratamento para fins que não aqueles para os quais os dados pessoais foram recolhidos não é realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros, as restrições estabelecidas no artigo 66.º, n.º 3, alínea g), e no artigo 67.º, n.º 2, alínea f), da DSP2 esclarecem que nenhum outro fim é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos. O teste de compatibilidade do artigo 6.º, n.º 4, do RGPD não pode resultar num fundamento jurídico para o tratamento.

24. O artigo 6.º, n.º 4, do RGPD permite o tratamento posterior com base em disposições do direito da União ou dos Estados-Membros. Por exemplo, todos os PSIP e PSIC são entidades obrigadas nos termos do artigo 3.º, ponto 2, alínea a), da Diretiva (UE) 2015/849 do Parlamento Europeu e do Conselho, de 20 de maio de 2015, relativa à prevenção da utilização do sistema financeiro para efeitos de branqueamento de capitais ou de financiamento do terrorismo, ou Diretiva Antibranqueamento de Capitais. Estas entidades obrigadas têm de aplicar medidas de diligência quanto à clientela conforme especificado na diretiva. Por conseguinte, os dados pessoais tratados no âmbito de um serviço previsto na DSP2 são objeto de tratamento posterior com base em pelo menos uma obrigação jurídica do prestador de serviços[20].

25. Conforme mencionado no ponto 20, o artigo 6.º, n.º 4, do RGPD indica que o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos se pode basear no consentimento do titular dos dados, se estiverem preenchidas todas as condições aplicáveis ao consentimento nos termos do RGPD. Como descrito acima, o responsável pelo tratamento tem de demonstrar que é possível recusar ou retirar o consentimento sem ser prejudicado (considerando 42 do RGPD).

2.5 Razão legítima para conceder acesso à conta (PSPGC)

26. Conforme mencionado no ponto 10, os utilizadores de serviços de pagamento podem exercer o direito de utilizar serviços de iniciação de pagamentos e de informação sobre contas. As obrigações impostas aos Estados-Membros pelo artigo 66.º, n.º 1, e pelo artigo 67.º, n.º 1, da DSP2 devem ser transpostas para o direito nacional para garantir a aplicação efetiva do direito do utilizador do serviço de pagamento a beneficiar dos serviços de pagamento supramencionados. A aplicação efetiva destes direitos não seria possível sem uma obrigação correspondente do PSPGC, geralmente um banco, de conceder ao prestador do serviço de pagamento acesso à conta desde que este cumpra todos os requisitos para ter acesso à conta do utilizador do serviço de pagamento. Além disso, o artigo 66.º, n.º 5, e o artigo 67.º, n.º 4, da DSP2 estabelecem claramente que a prestação dos serviços de iniciação de pagamentos e dos serviços de informação sobre contas não está subordinada à existência de uma relação contratual entre o PSIP/PSIC e o PSPGC.

27. O tratamento de dados pessoais pelo PSPGC assente na concessão do acesso aos dados pessoais solicitado pelo PSIP e pelo PSIC para executar o seu serviço de pagamento ao utilizador baseia-se numa obrigação jurídica. A fim de alcançar os objetivos da DSP2, os PSPGC têm de fornecer os dados pessoais para os serviços dos PSIP e dos PSIC, enquanto condição necessária para que estes prestem os seus serviços e, consequentemente, garantam os direitos previstos no artigo 66.º,

[20] Note-se que está fora do âmbito do presente documento examinar de forma aprofundada se a Diretiva Antibranqueamento de Capitais cumpre a norma prevista no artigo 6.º, n.º 4, do RGPD.

n.º 1, e no artigo 67.º, n.º 1, da DSP2. Por conseguinte, o fundamento jurídico aplicável neste caso é o artigo 6.º, n.º 1, alínea c), do RGPD.

28. Uma vez que o RGPD especificou que o tratamento baseado numa obrigação jurídica deve ser claramente definido pelo direito da União ou de um Estado-Membro (ver artigo 6.º, n.º 3, do RGPD), a obrigação do PSPGC de conceder acesso deve decorrer da legislação nacional que transpõe a DSP2.

3 CONSENTIMENTO EXPLÍCITO

3.1 Consentimento ao abrigo do RGPD

29. Nos termos do RGPD, o consentimento é um dos seis fundamentos jurídicos para a licitude do tratamento de dados pessoais. O artigo 4.º, ponto 11, do RGPD define consentimento como «uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento». Estas quatro condições — livre, específica, informada e explícita — são essenciais para a validade do consentimento. Segundo as Diretrizes 05/2020 do CEPD relativas ao consentimento na aceção do Regulamento 2016/679, o consentimento só pode constituir fundamento jurídico adequado se, ao titular dos dados, for oferecido controlo e uma verdadeira opção de aceitar ou recusar os termos propostos ou recusá-los sem ser prejudicado. Ao solicitar o consentimento, os responsáveis pelo tratamento têm o dever de avaliar se irão cumprir todos os requisitos para obter um consentimento válido. Caso seja obtido em conformidade com o RGPD, o consentimento é um instrumento que permite aos titulares dos dados controlarem se os dados pessoais que lhes dizem respeito vão ou não ser tratados. Caso não o seja, o controlo do titular dos dados torna-se ilusório e o consentimento será um fundamento jurídico inválido para o tratamento, tornando essa atividade de tratamento ilícita[21].

30. O RGPD contém ainda salvaguardas adicionais no artigo 7.º, segundo o qual o responsável pelo tratamento deve poder demonstrar que houve um consentimento válido aquando do tratamento. Além disso, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente dos outros assuntos, de modo inteligível e de fácil acesso, e numa linguagem clara e simples. Por outro lado, o titular dos dados deve ser informado do direito de retirar o consentimento a qualquer momento, de forma tão simples como a utilizada para dar consentimento.

31. Nos termos do artigo 9.º do RGPD, o consentimento é uma das exceções à proibição geral de tratamento de categorias especiais de dados pessoais. Contudo, neste caso, o consentimento do titular dos dados tem de ser «explícito»[22].

32. Segundo as Diretrizes 05/2020 do CEPD relativas ao consentimento na aceção do Regulamento 2016/679, o consentimento explícito na aceção do RGPD refere-se à forma como o consentimento é manifestado pelo titular dos dados. Tal significa que o titular dos dados deve manifestar expressamente o consentimento para a(s) finalidade(s) específica(s) do tratamento. Uma maneira óbvia de garantir que o consentimento é explícito seria confirmar expressamente o consentimento numa declaração escrita. Quando adequado, o responsável pelo tratamento pode certificar-se de que a declaração escrita é assinada pelo titular dos dados, por forma a eliminar todas as dúvidas possíveis e uma potencial falta de provas no futuro.

33. O consentimento não pode, em nenhuma circunstância, ser inferido de declarações ou ações potencialmente ambíguas. O responsável pelo tratamento também deve ter cuidado com o facto de o consentimento não poder ser obtido através da mesma ação de concordar com o contrato ou aceitar as condições gerais do serviço.

---

21 Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, CEPD, n.º 3.

22 Ver também o Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 6-8, e/ou o Parecer 06/2014 sobre o conceito de interesses legítimos do responsável pelo tratamento dos dados na aceção do artigo 7.º da Diretiva 95/46/CE (WP 217), p. 9, 10, 13 e 14.

3.2 Consentimento ao abrigo da DSP2

34. O CEPD salienta que o quadro jurídico relativo ao consentimento explícito é complexo, já que este conceito está incluído na DSP2 e no RGPD. Importa perceber, pois, se o «consentimento expresso» a que se refere o artigo 94.º, n.º 2, da DSP2 deve ser interpretado da mesma forma que o consentimento explícito ao abrigo do RGPD.

3.2.1 Consentimento expresso ao abrigo do artigo 94.º, n.º 2, da DSP2

35. A DSP2 contém um conjunto de regras específicas relativas ao tratamento de dados pessoais, em especial no artigo 94.º, n.º 1, que determina que o tratamento de dados pessoais para efeitos da mesma diretiva tem de cumprir a legislação da UE em matéria de proteção de dados. Além disso, o artigo 94.º, n.º 2, da DSP2 estabelece que os prestadores de serviços de pagamento só acedem aos dados pessoais necessários para a prestação dos seus serviços de pagamento, e só os tratam e conservam, com o consentimento expresso do utilizador de serviços de pagamento. Nos termos do artigo 33.º, n.º 2, da DSP2, este requisito do consentimento expresso do utilizador de serviços de pagamento não se aplica aos PSIC. Contudo, o artigo 67.º, n.º 2, alínea a), da DSP2 prevê o consentimento expresso aos PSIC para a prestação do serviço.

36. Conforme referido acima, a lista de fundamentos jurídicos para o tratamento ao abrigo do RGPD é exaustiva. Como indicado no ponto 14, o fundamento jurídico para o tratamento de dados pessoais para a prestação de serviços de pagamento é, em princípio, o artigo 6.º, n.º 1, alínea b), do RGPD, ou seja, a necessidade do tratamento para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados. Daqui resulta que o artigo 94.º, n.º 2, da DSP2 não pode ser encarado como um fundamento jurídico adicional para o tratamento de dados pessoais. O CEPD considera que, face ao exposto, este número deve ser interpretado, por um lado, de forma coerente com o quadro jurídico aplicável em matéria de proteção de dados e, por outro, de forma a preservar o seu efeito útil. O consentimento expresso ao abrigo do artigo 94.º, n.º 2, da DSP2 deve, portanto, ser encarado como um requisito adicional de natureza contratual[23] no que respeita ao acesso e ao posterior tratamento e armazenamento de dados pessoais para efeitos de prestação de serviços de pagamento e não é, por conseguinte, equivalente ao consentimento (explícito) ao abrigo do RGPD.

37. O «consentimento expresso» a que se refere o artigo 94.º, n.º 2, da DSP2 é um consentimento contratual. Por conseguinte, deve interpretar-se este número como dispondo que os titulares dos dados, quando celebram um contrato com um prestador de serviços de pagamento ao abrigo da DSP2, devem estar plenamente cientes das categorias específicas de dados pessoais que serão tratados. Além disso, os titulares dos dados devem ser informados da finalidade específica (serviço de pagamento) para que os seus dados pessoais serão tratados e concordar expressamente com estas cláusulas. As cláusulas em questão devem ser apresentadas de uma forma que as distinga claramente dos outros assuntos tratados no contrato e têm de ser expressamente aceites pelo titular dos dados.

38. Um aspeto central do conceito de «consentimento expresso» ao abrigo do artigo 94.º, n.º 2, da DSP2 é a obtenção de acesso a dados pessoais para os tratar e armazenar posteriormente para efeitos de prestação de serviços de pagamento. Tal implica que o prestador do serviço de pagamento[24] ainda não trata os dados pessoais, mas precisa de aceder a dados pessoais que foram tratados sob a responsabilidade de qualquer outro responsável pelo tratamento. Se o utilizador do serviço de pagamento celebrar um contrato, por exemplo, com um prestador de serviços de

---

23 Carta do CEPD relativa à DSP2, 5 de julho de 2018, página 4.

24 Tal aplica-se aos serviços 1 a 7 do anexo I da DSP2.

iniciação de pagamentos, este prestador de serviços precisa de aceder aos dados pessoais do utilizador do serviço de pagamento que estão a ser tratados sob a responsabilidade do prestador de serviços de pagamento que gere a conta. O objeto do consentimento expresso ao abrigo do artigo 94.º, n.º 2, da DSP2 é a autorização para obter acesso aos dados pessoais em causa, a fim de poder tratar e armazenar os dados pessoais necessários para efeitos de prestação do serviço de pagamento. Caso o titular dos dados dê o seu consentimento expresso, o prestador de serviços de pagamento que gere a conta é obrigado a conceder acesso aos dados pessoais indicados.

39. Embora o consentimento previsto no artigo 94.º, n.º 2, da DSP2 não constitua um fundamento jurídico para o tratamento de dados pessoais, este consentimento está especificamente relacionado com os dados pessoais e a proteção de dados e assegura transparência e um certo nível de controlo ao utilizador do serviço de pagamento[25]. Embora a DSP2 não especifique as condições substantivas aplicáveis ao consentimento nos termos do seu artigo 94.º, n.º 2, esta diretiva deve, conforme referido acima, ser entendida de forma coerente com o quadro jurídico aplicável em matéria de proteção de dados e de forma a preservar o seu efeito útil.

40. No que diz respeito às informações a prestar pelos responsáveis pelo tratamento e ao requisito de transparência, as Orientações do Grupo de Trabalho do Artigo 29.º relativas à transparência especificam o seguinte: «*Uma consideração central em relação ao princípio da transparência realçada nas presentes disposições é que o titular dos dados deve poder determinar antecipadamente qual o âmbito do tratamento e quais as consequências decorrentes desse tratamento, não devendo mais tarde ser apanhado de surpresa acerca das formas como os seus dados pessoais estão a ser utilizados.*»[26].

41. Além disso, em conformidade com o princípio da limitação das finalidades, os dados pessoais devem ser recolhidos para finalidades determinadas, explícitas e legítimas (artigo 5.º, n.º 1, alínea b), do RGPD). Nos casos em que os dados são recolhidos para mais do que uma finalidade, os responsáveis pelo tratamento devem evitar identificar uma única finalidade global para justificar várias atividades de tratamento posterior que, na verdade, têm apenas uma relação remota com a finalidade inicial em si[27]. O CEPD salientou, mais recentemente, no contexto dos contratos de serviços em linha, que existe um risco de inclusão de cláusulas gerais de tratamento nos contratos e afirmou que a finalidade da recolha deve ser clara e especificamente identificada: deve ser suficientemente pormenorizada para determinar que tipo de tratamento está e não está incluído na finalidade especificada, e para permitir que o cumprimento da lei possa ser avaliado e que possam ser aplicadas salvaguardas em matéria de proteção de dados[28].

42. No contexto do requisito adicional de consentimento expresso nos termos do artigo 94.º, n.º 2, da DSP2, tal implica que os responsáveis pelo tratamento prestem aos titulares dos dados informações específicas e explícitas sobre as finalidades específicas, identificadas pelo responsável pelo tratamento, para as quais os seus dados são acedidos, tratados e conservados. Em

---

25 O artigo 94.º, n.º 2, da DSP2 faz parte do capítulo 4, «Proteção de dados».

26 Grupo de Trabalho do Artigo 29.º, Orientações relativas à transparência na aceção do Regulamento 2016/679, n.º 10 (adotadas em 11 de abril de 2018) — aprovadas pelo CEPD.

27 Parecer 03/2013 do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades (WP203), página 16.

28 Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, n.º 16 (versão de consulta pública), e Parecer 03/2013 do Grupo de Trabalho do Artigo 29.º sobre a limitação das finalidades (WP203), páginas 15 e 16.

conformidade com o artigo 94.º, n.º 2, da DSP2, os titulares dos dados têm de aceitar expressamente estas finalidades específicas.

43. Além disso, conforme referido no ponto 10 *supra*, o CEPD salienta que o utilizador do serviço de pagamento deve poder escolher se utiliza ou não o serviço e não pode ser obrigado a fazê-lo. Por conseguinte, o consentimento ao abrigo do artigo 94.º, n.º 2, da DSP2 tem de ser também um consentimento livre.

3.3 Conclusão

44. O consentimento expresso ao abrigo da DSP2 é diferente do consentimento (explícito) ao abrigo do RGPD. O consentimento expresso ao abrigo do artigo 94.º, n.º 2, da DSP2 é um requisito adicional de natureza contratual. Quando um prestador de serviços de pagamento precisa de aceder a dados pessoais para prestar um serviço de pagamento, necessita do consentimento expresso do utilizador deste serviço em conformidade com o artigo 94.º, n.º 2, da DSP2.

4 TRATAMENTO DE DADOS DE PARTE SILENCIOSA

4.1 Dados de parte silenciosa

45. O tratamento dos chamados «dados de parte silenciosa» é um aspeto da proteção de dados que merece uma análise atenta. No contexto do presente documento, os dados de parte silenciosa são dados pessoais relativos a um titular de dados que não é o utilizador de um determinado prestador de serviços de pagamento mas cujos dados pessoais são tratados por esse prestador de serviços para a execução de um contrato entre o prestador e o utilizador do serviço de pagamento. Tal acontece, por exemplo, quando um utilizador de serviços de pagamento, o titular de dados A, utiliza os serviços de um PSIC, e um titular de dados B efetuou uma série de operações de pagamento para a conta de pagamento do titular de dados A. Neste caso, o titular de dados B é considerando a «parte silenciosa» e os dados pessoais (como o número de conta do titular de dados B e o montante envolvido nessas operações) relativos ao titular de dados B são considerados «dados de parte silenciosa».

4.2 Interesses legítimos do responsável pelo tratamento

46. O artigo 5.º, n.º 1, alínea b), do RGPD estabelece que os dados pessoais apenas devem ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades. Além disso, o RGPD exige que qualquer tratamento de dados pessoais seja necessário e proporcionado e esteja em conformidade com os princípios de proteção de dados, nomeadamente a limitação das finalidades e a minimização dos dados.

47. O RGPD poderá permitir o tratamento de dados de parte silenciosa quando tal tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros (artigo 6.º, n.º 1, alínea f), do RGPD). Contudo, este tratamento apenas pode ocorrer quando aos interesses legítimos do responsável pelo tratamento não se sobrepõem «os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais».

48. Por conseguinte, o interesse legítimo de um responsável pelo tratamento ou de um terceiro em executar o contrato com o utilizador de serviços de pagamento pode constituir um fundamento jurídico para o tratamento de dados de parte silenciosa por PSIP e PSIC, no contexto da prestação de serviços de pagamento ao abrigo da DSP2. A necessidade de tratar dados pessoais da parte silenciosa é limitada e determinada pelas expectativas razoáveis destes titulares de dados. No contexto da prestação de serviços de pagamento abrangidos pela DSP2, é necessário estabelecer medidas eficazes e adequadas para impedir que o referido interesse legítimo se sobreponha aos interesses ou aos direitos e liberdades fundamentais das partes silenciosas e para assegurar o cumprimento das expectativas razoáveis destes titulares de dados no que respeita ao tratamento dos seus dados pessoais. Neste contexto, o responsável pelo tratamento (PSIC ou PSIP) deve estabelecer as garantias necessárias para o tratamento, a fim de proteger os direitos dos titulares dos dados, incluindo medidas técnicas para assegurar que os dados de parte silenciosa não sejam tratados para outra finalidade que não aquela para que os dados pessoais foram inicialmente recolhidos pelos PSIP ou PSIC. Se possível, também devem ser aplicadas a cifragem ou outras técnicas para alcançar um nível adequado de segurança e de minimização dos dados.

4.3 Tratamento posterior de dados pessoais da parte silenciosa

49. Conforme referido no ponto 29, os dados pessoais tratados no âmbito de um serviço de pagamento regulado pela DSP2 podem ser objeto de tratamento posterior com base em

obrigações jurídicas do prestador de serviços. Estas obrigações jurídicas poderão dizer respeito aos dados pessoais da parte silenciosa.

50. No que diz respeito ao tratamento posterior de dados de parte silenciosa com base em interesses legítimos, o CEPD considera que estes dados não podem ser utilizados para outra finalidade que não aquela para que os dados pessoais foram recolhidos, com base no direito da UE ou de um Estado-Membro. O consentimento da parte silenciosa não é juridicamente viável, uma vez que, para obter o consentimento, seria necessário recolher ou tratar dados pessoais da parte silenciosa, sem que exista, para o efeito, fundamento jurídico no artigo 6.º do RGPS. O teste de compatibilidade previsto no artigo 6.º, n.º 4, do RGPD também não pode proporcionar um fundamento para o tratamento para outras finalidades (por exemplo, atividades de *marketing* direto). Os direitos e liberdades dos titulares destes dados de parte silenciosa não serão respeitados se o novo responsável pelo tratamento utilizar os dados pessoais para outras finalidades, tendo em conta o contexto em que os dados pessoais foram recolhidos, em especial a ausência de uma relação com os titulares de dados que são partes silenciosas[29]; a ausência de uma ligação entre qualquer outra finalidade e a finalidade para que os dados pessoais foram inicialmente recolhidos (ou seja, o facto de os prestadores de serviços de pagamento precisarem apenas dos dados de parte silenciosa para executar um contrato com a outra parte contratante); a natureza dos dados pessoais em causa[30], a circunstância de os titulares dos dados não poderem ter uma expectativa razoável em relação a qualquer tratamento posterior ou sequer saberem qual o responsável pelo tratamento que poderá tratar os seus dados pessoais e as restrições legais ao tratamento estabelecidas no artigo 66.º, n.º 3, alínea g), e no artigo 67.º, n.º 2, alínea f), da DSP2.

29 O considerando 87 da DSP2 dispõe que esta diretiva diz exclusivamente respeito «às obrigações e responsabilidades contratuais entre o utilizador do serviço de pagamento e o prestador do serviço de pagamento». Como tal, os dados de parte silenciosa não se inserem no âmbito de aplicação da DSP2.

30 Importa ter especial cuidado no tratamento de dados pessoais de natureza financeira, uma vez que este tratamento pode ser considerado suscetível de aumentar os possíveis riscos para os direitos e as liberdades dos indivíduos, de acordo com as Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD).

5 O TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS PESSOAIS AO ABRIGO DA DSP2

5.1 Categorias especiais de dados pessoais

51. O artigo 9.º, n.º 1, do RGPD proíbe «o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa».

52. É importante salientar que, em alguns Estados-Membros, os pagamentos eletrónicos já são omnipresentes e são privilegiados por muitas pessoas em detrimento do dinheiro nas suas operações diárias. Simultaneamente, as operações financeiras podem revelar informações sensíveis sobre um titular de dados individual, incluindo informações relacionadas com categorias especiais de dados pessoais. Por exemplo, consoante a operação concreta, é possível que donativos efetuados a partidos ou organizações políticas, igrejas ou paróquias revelem as opiniões políticas e as convicções religiosas do doador. A dedução de uma quota anual da conta bancária de uma pessoa também pode revelar a filiação num sindicato. É possível obter dados pessoais relativos à saúde analisando as contas médicas pagas por um titular de dados a um profissional de medicina (por exemplo, um psiquiatra). Por último, as informações sobre determinadas aquisições podem revelar informações sobre a vida sexual ou a orientação sexual de uma pessoa. Como mostram estes exemplos, até operações simples podem conter categorias especiais de dados pessoais. Além disso, os serviços de informação sobre contas podem basear-se na definição de perfis, na aceção do artigo 4.º, ponto 4, do RGPD. Conforme afirmado anteriormente nas Orientações do Grupo de Trabalho do Artigo 29.º sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, aprovadas pelo CEPD, a «definição de perfis pode criar dados de categorias especiais por inferência a partir de dados que não sejam dados de categorias especiais *per se*, mas que passem a sê-lo quando combinados com outros dados»[31]. Isto significa que o conjunto das operações financeiras pode revelar diferentes tipos de padrões comportamentais, que podem incluir categorias especiais de dados pessoais. Por conseguinte, é muito provável que um prestador de serviços que trata informações sobre operações financeiras de titulares de dados trate também categorias especiais de dados pessoais.

53. No que diz respeito ao termo «dados de pagamento sensíveis», o CEPD observa o seguinte: a definição de dados de pagamento sensíveis na DSP2 diverge consideravelmente da forma como o termo «dados pessoais sensíveis» é geralmente utilizado no contexto do RGPD e da proteção de dados (e respetiva legislação). Enquanto a DSP2 define «dados de pagamento sensíveis» como «dados, incluindo credenciais de segurança personalizadas, que podem ser utilizados para cometer fraudes», o RGPD salienta a necessidade de proteção específica de categorias especiais de dados pessoais que, nos termos do artigo 9.° do mesmo regulamento, são, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, como as categorias especiais de dados pessoais[32]. Neste contexto, é aconselhável, pelo menos, identificar e categorizar de forma precisa os tipos de dados pessoais que serão tratados. É provável que seja

[31] Grupo de Trabalho do Artigo 29.º para a Proteção de Dados, Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, WP251rev.01, página 16.

[32] Por exemplo, no considerando 10 do RGPD, as categorias especiais de dados pessoais são referidas como «dados sensíveis».

necessária uma avaliação de impacto sobre a proteção de dados (AIPD), em conformidade com o artigo 35.º do RGPD, que contribua para este exercício de identificação. Estão disponíveis mais orientações sobre as AIPD nas Orientações do Grupo de Trabalho do Artigo 29.º relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, aprovadas pelo CEPD.

5.2 Possíveis derrogações

54. A proibição estabelecida no artigo 9.º do RGPD não é absoluta. Em especial, enquanto as derrogações das alíneas b) a f) e h) a j) do artigo 9.º, n.º 2, do RGPD não são, manifestamente, aplicáveis ao tratamento de dados pessoais no contexto da DSP2, as seguintes duas derrogações do artigo 9.º, n.º 2, podem ser pertinentes:

a) A proibição não é aplicável se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas (artigo 9.º, n.º 2, alínea a), do RGPD).

b) A proibição não é aplicável se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados (artigo 9.º, n.º 2, alínea g), do RGPD).

55. Importa assinalar que a lista de derrogações do artigo 9.º, n.º 2, do RGPD é exaustiva. O prestador de serviços tem de reconhecer a possibilidade de existirem categorias especiais de dados pessoais nos dados pessoais tratados para a prestação de qualquer um dos serviços abrangidos pela DSP2. Uma vez que a proibição estabelecida no artigo 9.º, n.º 1, do RGPD é aplicável a estes prestadores de serviços, cabe-lhes assegurar que uma das exceções previstas no artigo 9.º, n.º 2, do RGPD lhes é aplicável. Importa salientar que, quando o prestador de serviços não consegue demonstrar que cumpre os requisitos de uma das derrogações, a proibição do artigo 9.º, n.º 1 é aplicável.

5.3 Interesse público importante

56. Os serviços de pagamentos podem tratar categorias especiais de dados pessoais por motivos de interesse público importante, mas apenas se estiverem preenchidas todas as condições previstas no artigo 9.º, n.º 2, alínea g), do RGPD. Por conseguinte, o tratamento das categorias especiais de dados especiais tem de estar contemplado numa derrogação específica do artigo 9.º, n.º 1, do RGPD prevista no direito da União ou de um Estado-Membro. Esta disposição terá de abordar a proporcionalidade relativamente ao objetivo visado do tratamento e conter medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados. Além disso, esta disposição prevista no direito da União ou de um Estado-Membro terá de respeitar a essência do direito à proteção dos dados. Por último, deve também demonstrar-se que o tratamento das categorias especiais de dados é necessário por motivos de interesse público importante, incluindo interesses de importância sistémica. Todas estas condições têm de ser plenamente cumpridas para que esta derrogação possa ser aplicável aos tipos designados de serviços de pagamentos.

5.4 Consentimento explícito

57. Nos casos em que a derrogação do artigo 9.º, n.º 2, alínea g), do RGPD não é aplicável, a obtenção de consentimento explícito em conformidade com as condições para um consentimento válido

estabelecidas no RGPD parece ser a única derrogação lícita possível para o tratamento de categorias especiais de dados pessoais por TPS. As Diretrizes 05/2020 do CEPD relativas ao consentimento na aceção do Regulamento 2016/679 afirmam[33] o seguinte: «O artigo 9.º, n.º 2, não reconhece "necessário para a execução de um contrato" como uma exceção à proibição geral de tratamento de categorias especiais de dados. Por conseguinte, os responsáveis pelo tratamento e os Estados-Membros que se defrontam com esta situação devem recorrer às exceções previstas no artigo 9.º, n.º 2, alíneas b) a j).» Quando os prestadores de serviços se baseiam no artigo 9.º, n.º 2, alínea a), do RGPD, têm de assegurar que lhes foi dado consentimento explícito antes de iniciarem o tratamento. O consentimento explícito estabelecido no artigo 9.º, n.º 2, alínea a), do RGPD tem de cumprir todos os requisitos do RGPD.

5.5 Ausência de uma derrogação adequada

58. Conforme atrás referido, quando o prestador de serviços não consegue demonstrar que cumpre os requisitos de uma das derrogações, a proibição do artigo 9.º, n.º 1 é aplicável. Neste caso, podem ser aplicadas medidas técnicas para impedir o tratamento de categorias especiais de dados pessoais, por exemplo, impedindo o tratamento de certos pontos de dados. Neste sentido, os prestadores de serviços de pagamento podem avaliar as possibilidades técnicas que permitam excluir categorias especiais de dados pessoais e permitir um acesso selecionado que impeça o tratamento de categorias especiais de dados pessoais relacionados com partes silenciosas por TPS.

[33] Diretrizes 05/2020 relativas ao consentimento na aceção do Regulamento 2016/679, CEPD, n.º 99.

6 MINIMIZAÇÃO DOS DADOS, SEGURANÇA, TRANSPARÊNCIA, RESPONSABILIDADE E DEFINIÇÃO DE PERFIS

6.1 Minimização dos dados e proteção de dados desde a conceção e por defeito

59. O princípio da minimização dos dados está consagrado no artigo 5.º, n.º 1, alínea c), do RGPD: «Os dados pessoais são […] [a]dequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados». Essencialmente, ao abrigo do princípio da minimização dos dados, os responsáveis pelo tratamento não devem tratar mais dados pessoais do que os necessários para cumprir a finalidade específica em questão. Conforme salientado no capítulo 2, a quantidade e o tipo de dados pessoais necessários para prestar o serviço de pagamento são determinados pelo objeto contratual concreto e mutuamente compreendido[34]. A minimização dos dados é aplicável a todos os tratamentos (por exemplo, todas as recolhas de dados pessoais ou acessos e pedidos relativos a esses dados). As Diretrizes 4/2019 do CEPD sobre a proteção de dados desde a conceção e por defeito prevista no artigo 25.º do RGPD afirmam que os responsáveis pelo tratamento e os fornecedores de tecnologia são igualmente reconhecidos como facilitadores essenciais da proteção de dados desde a conceção e por defeito e devem estar cientes de que os responsáveis pelo tratamento são obrigados a tratar os dados pessoais com sistemas e tecnologias que têm a proteção de dados incorporada[35].

60. O artigo 25.º do RGPD contém as obrigações a aplicar à proteção de dados desde a conceção e por defeito. Estas obrigações são particularmente importantes para o princípio da minimização dos dados. O referido artigo determina que os responsáveis pelo tratamento devem aplicar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas destinadas a aplicar com eficácia os princípios da proteção de dados e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do RGPD e proteja os direitos dos titulares dos dados. O responsável pelo tratamento deve aplicar medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Estas medidas poderão incluir a cifragem, a pseudonimização e outras medidas técnicas.

61. Quando a obrigação prevista no artigo 25.º do RGPD é aplicada, os elementos a ter em conta são as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis. As referidas Diretrizes 4/2019 do CEPD sobre a proteção de dados desde a conceção e por defeito prevista no artigo 25.º do RGPD apresentam mais esclarecimentos sobre esta obrigação.

6.2 Medidas de minimização dos dados

62. Os TPS que acedem aos dados das contas de pagamento para prestar o serviço solicitado devem também ter em conta o princípio da minimização dos dados e apenas recolher os dados pessoais necessários para prestar os serviços de pagamento específicos solicitados pelo utilizador do serviço de pagamento. Em princípio, o acesso aos dados pessoais deve ser limitado ao necessário para

---

34 Diretrizes 2/2019 sobre o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea b), do RGPD no contexto da prestação de serviços em linha aos titulares dos dados, CEPD, n.º 32.

35 «Guidelines 4/2019 on Article 25 Data Protection by Design and by Default» [Diretrizes 4/2019 sobre a proteção de dados desde a conceção e por defeito prevista no artigo 25.º do RGPD], página 29.

prestar os serviços de pagamento. Conforme demonstrado no capítulo 2, a DSP2 exige que os PSPGC partilhem as informações do utilizador do serviço de pagamento a pedido deste, quando o mesmo pretende utilizar um serviço de iniciação do pagamento ou um serviço de informação sobre contas.

63. Se nem todos os dados da conta de pagamento forem necessários para a execução do contrato, o PSIC deve fazer uma seleção das categorias de dados pertinentes antes da recolha dos dados. As categorias de dados que poderão não ser necessárias incluirão, por exemplo, a identidade da parte silenciosa e as características da operação. Além disso, a menos que o direito da União ou de um Estado-Membro o exija, o IBAN da conta bancária da parte silenciosa poderá não ter de ser apresentado.

64. A este respeito, a possível aplicação de medidas técnicas para habilitar ou ajudar os TPS a cumprir a obrigação de aceder e recuperar apenas os dados necessários para a prestação dos seus serviços pode ser considerada como parte da aplicação de políticas adequadas em matéria de proteção de dados, em conformidade com o artigo 24.º, n.º 2, do RGPD. Neste sentido, o CEPD recomenda a utilização de ferramentas digitais destinadas a ajudar os PSIC a cumprir a obrigação de recolher apenas os dados pessoais necessários para as finalidades para que são tratados. Por exemplo quando um prestador de serviços não precisa das características da operação (no campo da descrição dos registos de operações) para prestar o seu serviço, poderá utilizar-se uma ferramenta de seleção digital como forma de excluir este campo das operações de tratamento gerais do TPS.

Exemplo 2:

A Bons Pagamentos, o prestador de serviços de informação sobre contas do exemplo 1, pretende assegurar que apenas trata os dados pessoais das contas de pagamento em que os seus utilizadores estão interessados. A prestação do serviço não exigiria o acesso a mais dados das contas de pagamento. Por conseguinte, o prestador de serviços permite que os utilizadores selecionem os tipos de informação específicos em que estão interessados.

O utilizador A pretende uma visão geral das suas despesas nos últimos dois meses. Assim, solicita, relativamente às suas duas contas bancárias, detidas junto de dois PSPGC diferentes, as informações sobre todas as operações dos últimos dois meses, o montante das operações, a data de execução e o nome do destinatário, e assinala as caixas correspondentes na interface de utilizador da Bons Pagamentos.

Em seguida, esta começa por solicitar aos respetivos PSPGC apenas as informações correspondentes aos campos definidos pelo utilizador A e relativas ao período dos últimos dois meses. Não solicita informações como a «comunicação» da transferência ou mesmo o IBAN, uma vez que o utilizador A não as pediu.

O PSPGC, a fim de permitir que a Bons Pagamentos cumpra as suas obrigações de minimização dos dados, autoriza-a a solicitar campos específicos para um determinado intervalo de datas.

65. Importa salientar também, a este respeito, que, nos termos da DSP2, os PSPGC apenas podem conceder acesso a informações sobre contas de pagamento. A DSP2 não prevê qualquer fundamento jurídico para conceder acesso a dados pessoais contidos noutras contas, como contas de poupanças, créditos hipotecários ou investimentos. De igual forma, nos termos da DSP2, é necessário aplicar medidas técnicas para assegurar que o acesso abrange apenas as informações necessárias sobre as contas de pagamento.

66. Além de recolher o mínimo possível de dados, o prestador de serviços tem de aplicar períodos de conservação limitados. O prestador de serviços não deve armazenar os dados pessoais durante

um período superior ao necessário para cumprir as finalidades solicitadas pelo utilizador do serviço de pagamento.

67. Se o contrato entre o titular dos dados e o PSIC exigir a transmissão de dados pessoais a terceiros, apenas poderão ser transmitidos os dados pessoais necessários para a execução do contrato. Os titulares dos dados devem também ser especificamente informados sobre a transmissão e os dados pessoais que serão transmitidos ao terceiro em causa.

6.3 Segurança

68. O CEPD já salientou que a violação de dados pessoais de natureza financeira «*implica claramente que a vida quotidiana do titular dos dados será gravemente afetada*», citando como exemplo os riscos de fraude de pagamentos[36].

69. Quando uma violação de dados está associada a dados financeiros, o titular dos dados pode ser exposto a riscos consideráveis. A fuga de determinadas informações pode expor os titulares dos dados ao risco de usurpação de identidade ou furto de fundos nas contas e outros ativos. Além disso, é possível que a exposição dos dados das operações esteja associado a riscos consideráveis para a privacidade, uma vez que os dados das operações podem conter referências a todos os aspetos da vida privada de um titular de dados. Por outro lado, os dados financeiros são, naturalmente, valiosos para os infratores e constituem, por isso, um alvo atrativo.

70. Enquanto responsáveis pelo tratamento, os prestadores de serviços de pagamento são obrigados a tomar medidas para proteger os dados pessoais dos titulares dos dados (artigo 24.º, n.º 1, do RGPD). Quanto maiores forem os riscos associados à atividade de tratamento realizada pelo responsável, mais elevadas são as normas de segurança a aplicar. Uma vez que está ligado a diversos riscos graves, o tratamento de dados financeiros exige medidas de segurança mais fortes.

71. Os prestadores de serviços devem ser obrigados a respeitar normas elevadas, incluindo mecanismos de autenticação forte dos clientes e normas de segurança elevadas para o equipamento técnico[37]. Existem outros procedimentos importantes, como a verificação dos responsáveis pelo tratamento no que diz respeito às normas de segurança e a aplicação de procedimentos contra acesso não autorizado.

6.4 Transparência e responsabilidade

72. A transparência e a responsabilidade são dois princípios fundamentais do RGPD.

73. No que diz respeito à transparência (artigo 5.º, n.º 1, alínea a), do RGPD), o artigo 12.º do RGPD especifica que os responsáveis pelo tratamento devem tomar as medidas adequadas para fornecer as informações a que se referem os artigos 13.º e 14.º do mesmo regulamento. Além disso, exige que as informações ou comunicações a respeito do tratamento de dados pessoais sejam apresentadas de forma concisa, transparente, inteligível e de fácil acesso. As informações devem ser prestadas numa linguagem clara e simples e por escrito «ou por outros meios, incluindo, se for caso disso, por meios eletrónicos». As Orientações do Grupo de Trabalho do Artigo 29.º relativas à transparência na aceção do Regulamento 2016/679, aprovadas pelo CEPD, apresentam orientações específicas para o cumprimento do princípio da transparência em ambientes digitais.

---

36 Orientações do Grupo de Trabalho do Artigo 29.º relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é «suscetível de resultar num elevado risco» para efeitos do Regulamento (UE) 2016/679, WP248 rev.01 — aprovadas pelo CEPD.

37 Ver as NTR.

74. Segundo as referidas Orientações relativas à transparência na aceção do Regulamento 2016/679, o artigo 11.º do RGPD deve ser interpretado como forma de aplicar uma verdadeira minimização de dados sem prejudicar o exercício dos direitos dos titulares dos dados e o exercício dos direitos dos titulares dos dados deve ser possível com a ajuda de informações adicionais fornecidas pelo titular dos dados. Pode haver situações em que um responsável pelo tratamento esteja a tratar dados pessoais que não exijam a identificação dos titulares dos dados (por exemplo, com dados pseudonimizados). Nestes casos, o artigo 11.º, n.º 1, também pode ser pertinente, uma vez que determina que um responsável pelo tratamento não é obrigado a manter, obter ou tratar informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento ao RGPD.

75. No que diz respeito aos serviços ao abrigo da DSP2, o artigo 13.º do RGPD é aplicável aos dados pessoais recolhidos junto do titular e o artigo 14.º é aplicável quando os dados pessoais não são recolhidos junto do titular.

76. Em particular, o titular dos dados deve ser informado sobre o prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo, e, quando aplicável, os interesses legítimos do responsável pelo tratamento ou de um eventual terceiro. Se o tratamento se basear no consentimento, nos termos do artigo 6.º, n.º 1, alínea a), do RGPD, ou no consentimento explícito, nos termos do artigo 9.º, n.º 2, alínea a), do RGPD, o titular dos dados tem de ser informado da existência do direito de retirar consentimento em qualquer altura.

77. O responsável pelo tratamento deve prestar as informações ao titular dos dados tendo em conta as circunstâncias específicas em que os dados pessoais forem tratados. Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados[38], o que, provavelmente acontecerá no caso dos PSIC, as informações devem ser prestadas o mais tardar no momento da primeira comunicação ao titular dos dados. Se os dados pessoais se destinarem a ser divulgados a outro destinatário, as informações devem ser prestadas o mais tardar aquando da primeira divulgação desses dados.

78. No que se refere aos serviços de pagamento em linha, as orientações supramencionadas esclarecem que os responsáveis pelo tratamento podem adotar uma abordagem estruturada quando escolhem utilizar uma combinação de métodos para garantir a transparência. As orientações recomendam, em especial, que as declarações de confidencialidade estruturadas sejam utilizadas para ligar as várias categorias de informações que importa fornecer ao titular dos dados, em vez de conterem todas essas informações num único documento no ecrã, por forma a evitar a fadiga informativa e, ao mesmo tempo, assegurar a eficácia da informação.

79. As orientações esclarecem também que os responsáveis pelo tratamento podem optar por utilizar ferramentas adicionais para prestar informações ao titular de dados individualmente, como painéis de controlo da confidencialidade. Um painel de controlo da confidencialidade é um ponto único a partir do qual os titulares dos dados podem ver «informações sobre confidencialidade» e gerir as suas preferências em matéria de confidencialidade, autorizando ou impedindo que os seus dados sejam utilizados de determinadas formas pelo responsável pelo tratamento em causa[39]. Um

---

38 Artigo 14.º, n.º 3, alínea b), do RGPD.

39 Segundo as Orientações do Grupo de Trabalho do Artigo 29.º relativas à transparência na aceção do Regulamento 2016/679, aprovadas pelo CEPD, os painéis de controlo da confidencialidade são particularmente úteis quando o mesmo serviço é utilizado por titulares de dados numa série de dispositivos diferentes, uma vez que estes podem aceder e controlar os seus dados pessoais

painel de controlo da confidencialidade pode proporcionar uma visão geral dos TPS que obtiveram o consentimento explícito dos titulares dos dados e podem também prestar informações pertinentes sobre a natureza e a quantidade dos dados pessoais a que os TPS acederam. Em princípio, um PSPGC poderá dar ao utilizador a possibilidade de retirar um consentimento expresso ao abrigo da DSP2[40] através da visão geral, o que poderia resultar numa negação de acesso de um ou mais TPS às suas contas de pagamento. O utilizador pode também solicitar ao PSPGC que negue o acesso de um ou mais TPS específicos[41] à(s) suas(s) conta(s) de pagamento, já que tem o direito de (não) utilizar um serviço de informação sobre contas. Para poderem ser utilizados para dar ou retirar consentimento expresso, os painéis de controlo da confidencialidade devem ser concebidos e aplicados de forma lícita e, em particular, evitar criar obstáculos ao direito dos TPS de prestar serviços em conformidade com a DSP2. Neste contexto, e em conformidade com as disposições aplicáveis nos termos da DSP2, um TPS tem a possibilidade de obter novamente o consentimento expresso do utilizador após a retirada do consentimento.

80. Os princípios da responsabilidade exigem que o responsável pelo tratamento estabeleça as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o RGPD, nomeadamente os principais princípios da proteção de dados previstos no artigo 5.º, n.º 1. Essas medidas devem ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares, e devem ser revistas e atualizadas quando necessário[42].

6.5 Definição de perfis

81. O tratamento de dados pessoais por prestadores de serviços de pagamento pode implicar a «definição de perfis» a que se refere o artigo 4.º, ponto 4, do RGPD. Por exemplo, os PSIC podem utilizar o tratamento automatizado de dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular. Consoante as características específicas do serviço, pode ser possível avaliar a situação financeira pessoal do titular dos dados. Os serviços de informação sobre contas, que devem ser prestados conforme solicitado pelos utilizadores, poderão implicar uma avaliação pormenorizada dos dados pessoais da conta de pagamento.

82. O responsável deve também informar de forma transparente o titular dos dados da existência de decisões automatizadas, incluindo a definição de perfis. Nestes casos, o responsável pelo tratamento deve prestar informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados (artigo 13.º, n.º 2, alínea f), artigo 14.º, n.º 2, alínea g), e considerando 60)[43]. De igual modo, o artigo 15.° do RGPD estabelece que o titular dos dados tem o direito de solicitar e obter do responsável pelo tratamento informações relativas à existência de decisões automatizadas, incluindo a definição de perfis, à lógica subjacente e às consequências para o titular dos dados e, em determinadas circunstâncias,

---

independentemente da forma como utilizam o serviço. Permitir que os titulares dos dados ajustem manualmente as suas definições de confidencialidade através de um painel de controlo da confidencialidade também pode facilitar a criação de uma declaração de confidencialidade personalizada que reflita apenas os tipos de tratamento possíveis para aquele titular de dados específico.

40 Ver, por exemplo, o «consentimento expresso» mencionado no artigo 67.º, n.º 2, alínea a), da DSP2.

41 Ver também EBA/OP/2020/10, ponto 45.

42 Artigo 5.º, n.º 2, e artigo 24.º do RGPD.

43 Orientações relativas à transparência na aceção do Regulamento 2016/679, WP 260 rev.01 — aprovadas pelo CEPD.

o direito de se opor à definição de perfis, independentemente de serem ou não tomadas decisões individuais exclusivamente automatizadas com base na definição de perfis[44].

83. Além disso, é igualmente relevante neste contexto o direito do titular dos dados de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, conforme disposto no artigo 22.º do RGPD. Esta norma também inclui, em determinadas circunstâncias, a necessidade de os responsáveis pelo tratamento aplicarem medidas adequadas para salvaguardar os direitos do titular dos dados, como a informação específica ao titular dos dados, o direito de obter a intervenção humana na tomada de decisões e o direito de manifestar o seu ponto de vista e contestar a decisão. Conforme referido também no considerando 71 do RGPD, tal implica, nomeadamente, que os titulares dos dados têm o direito de não ficarem sujeitos a uma decisão, como a recusa automática de um pedido de crédito por via eletrónica, sem qualquer intervenção humana[45].

84. As decisões automatizadas, incluindo a definição de perfis, que digam respeito a categorias especiais de dados pessoais são permitidas apenas se forem preenchidas as seguintes condições cumulativas previstas no artigo 22.º, n.º 4, do RGPD:

- é aplicável uma isenção ao artigo 22.º, n.º 2;
- e aplica-se o artigo 9.º, n.º 2, alínea a) ou g) do RGPD. Nos dois casos, o responsável pelo tratamento deve aplicar medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados[46].

85. Importa também cumprir os requisitos para o tratamento posterior, conforme descrito nas presentes diretrizes. Os esclarecimentos e as instruções sobre as decisões individuais automatizadas e a definição de perfis fornecidos pelas Orientações do Grupo de Trabalho do Artigo 29.º sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, aprovadas pelo CEPD, são plenamente relevantes no contexto dos serviços de pagamento e devem, portanto, ser devidamente tidas em consideração.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

---

44 Orientações do Grupo de Trabalho do Artigo 29.º sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, WP251rev.01.

45 Considerando 71 do RGPD.

46 Orientações do Grupo de Trabalho do Artigo 29.º sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679, WP251rev.01, página 27.