Diretrizes

Orientações 4/2019 relativas ao artigo 25.º

Proteção de Dados desde a Conceção e por Defeito

Versão 2.0

Adotadas em 20 de outubro de 2020

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

Histórico de versões

Versão 1.0	13 de novembro de 2019	Adoção das Orientações para consulta pública
Versão 2.0	20 de outubro de 2020	Adoção das Orientações pelo CEPD após 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,

Tendo em conta o artigo 12.º e o artigo 22.º do seu Regulamento Interno,

ADOTOU AS SEGUINTES ORIENTAÇÕES

Resumo

Num mundo cada vez mais digital, a adesão aos requisitos da Proteção de Dados desde a Conceção e por Defeito desempenha um papel crucial na promoção da proteção da privacidade e dos dados na sociedade. Por conseguinte, é essencial que os responsáveis pelo tratamento assumam esta responsabilidade com seriedade e implementem as obrigações do RGPD ao conceberem as operações de tratamento.

As presentes orientações centram-se na obrigação de proteção de dados desde a conceção e por defeito (a seguir designada «PDdCD»), conforme prevista no artigo 25.º do RGPD. A PDdCD constitui uma obrigação para todos os responsáveis pelo tratamento, independentemente do volume e da complexidade do tratamento. Para poder cumprir os requisitos de PDdCD, é fundamental que o responsável pelo tratamento compreenda os princípios da proteção de dados e os direitos e liberdades dos titulares dos dados.

A obrigação principal consiste em aplicar as medidas *adequadas* e as garantias necessárias que permitam a *aplicação eficaz* dos *princípios da proteção de dados* e, consequentemente, *os direitos e liberdades dos titulares dos dados desde a conceção e por defeito*. O artigo 25.º estipula os elementos de conceção e por defeito que devem ser tidos em conta. Estes elementos serão aprofundados nas presentes orientações.

O artigo 25.º, n.º 1, estipula que os responsável pelo tratamento de dados devem considerar a PDdCD logo aquando do planeamento de uma nova operação de tratamento. Os responsáveis pelo tratamento devem aplicar a PDdCD *antes* do tratamento e também *continuamente* no momento do tratamento, ao reverem com regularidade a eficácia das medidas e das garantias escolhidas. A PDdCD é igualmente aplicável aos sistemas existentes que tratam dados pessoais.

As orientações abordam igualmente a forma de aplicar eficazmente os princípios da proteção de dados enunciados no artigo 5.º do RGPD, enumerando elementos de conceção e por defeito fundamentais, bem como casos práticos a título de exemplo. O responsável pelo tratamento deve considerar a adequação das medidas sugeridas no contexto do tratamento específico em questão.

O CEPD formula recomendações sobre a forma como os responsáveis pelo tratamento, os subcontratantes e os fabricantes podem cooperar para alcançar a proteção de dados desde a conceção

e por defeito. Assim, incentiva os responsáveis pelo tratamento na indústria, os subcontratantes e os fabricantes a usarem a PDdCD como um meio para, aquando da comercialização dos seus produtos, obterem uma vantagem competitiva em relação aos responsáveis pelo tratamento e aos titulares dos dados. Incentiva ainda todos os responsáveis pelo tratamento a utilizarem certificações e códigos de conduta.

1 ÂMBITO DE APLICAÇÃO

1. As orientações centram-se na aplicação da PDdCD pelos responsáveis pelo tratamento, com base na obrigação prevista no artigo 25.º do RGPD.[1] Outros intervenientes, como os subcontratantes e os fabricantes de produtos, serviços e aplicações, que não são diretamente visados no artigo 25.º (a seguir designados «fabricantes»), podem igualmente considerar estas orientações úteis na criação de produtos e serviços que estejam em conformidade com o RGPD e que permitam aos responsáveis pelo tratamento cumprir as suas obrigações em matéria de proteção de dados.[2] O considerando 78 do RGPD acrescenta que a PDdCD deve ser tomada em consideração no contexto dos contratos públicos. Apesar de todos os responsáveis pelo tratamento terem o dever de integrar a PDdCD nas suas atividades de tratamento, esta disposição promove a adoção dos princípios da proteção de dados, relativamente aos quais as administrações públicas devem dar o exemplo. O responsável pelo tratamento é responsável pelo cumprimento das obrigações da PDdCD relativas ao tratamento efetuado pelos respetivos subcontratantes, pelo que deve ter isso em conta aquando da contratação com estas partes.

2. O requisito descrito no artigo 25.º é o de os responsáveis pelo tratamento conceberem a proteção de dados para o tratamento de dados pessoais e definirem-na por defeito para todo o ciclo de vida do tratamento. A PDdCD é igualmente um requisito para sistemas de tratamento existentes antes da entrada em vigor do RGPD. Os responsáveis pelo tratamento devem ter o tratamento constantemente atualizado em conformidade com o RGPD. Para mais informações sobre como manter um sistema existente conforme à PDdCD, ver ponto 2.1.4 das presentes orientações. O cerne da disposição consiste em assegurar uma proteção de dados *adequada* e *eficaz*, tanto*desde a conceção* como por *defeito*, o que significa que os responsáveis pelo tratamento devem ser capazes de demonstrar que têm as garantias e as medidas adequadas durante o tratamento para assegurar que os princípios da proteção de dados e os direitos e liberdades dos titulares dos dados são efetivos.

3. O capítulo 2 das orientações centra-se numa interpretação dos requisitos estabelecidos pelo artigo 25.º e explora as obrigações legais introduzidas pela disposição. O capítulo 3 apresenta exemplos sobre a forma de aplicar a PDdCD no contexto de princípios específicos de proteção de dados.

[1] As interpretações aqui previstas aplicam-se igualmente ao artigo 20.º da Diretiva (UE) 2016/680 e ao artigo 27.º do Regulamento (UE) 2018/1725.

[2] O considerando 78 do RGPD refere claramente esta necessidade: «*No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados*».

4. No capítulo 4, as orientações abordam a possibilidade de criar um procedimento de certificação para demonstrar a conformidade com o artigo 25.º e, no capítulo 5, a forma como o referido artigo pode ser aplicado pelas autoridades de controlo. Por último, as orientações fornecem às partes interessadas novas recomendações sobre a forma de aplicar com êxito a PDdCD. O CEPD reconhece os desafios que se colocam às pequenas e médias empresas (a seguir designadas «PME») para cumprir plenamente as obrigações da PDdCD e, no capítulo 6, formula recomendações adicionais especificamente endereçadas às PME.

2 ANÁLISE DO ARTIGO 25.º, N.OS 1 E 2, PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E POR DEFEITO

5. O objetivo do presente capítulo é explorar e fornecer orientações sobre os requisitos em matéria de proteção de dados desde a conceção previstos no artigo 25.º, n.º 1, do RGPD e em matéria de proteção de dados por defeito previstos no artigo 25.º, n.º 2, do RGPD, respetivamente. A proteção de dados desde a conceção e a proteção de dados por defeito são conceitos complementares que se reforçam mutuamente. Os titulares dos dados beneficiarão mais da proteção de dados por defeito se a proteção de dados desde a conceção for simultaneamente aplicada – e vice-versa.

6. A PDdCD é um requisito aplicável a todos os responsáveis pelo tratamento, das pequenas empresas às empresas multinacionais. Assim, a complexidade da aplicação da PDdCD pode variar em função da operação de tratamento individual. Contudo, independentemente da dimensão, a aplicação da PDdCD tem sempre benefícios para o responsável pelo tratamento e para o titular dos dados.

2.1 Artigo 25.º, n.º 1: Proteção de dados desde a conceção

2.1.1 Obrigação do responsável pelo tratamento de dados de aplicar as medidas técnicas e organizativas adequadas e de incluir as garantias necessárias no tratamento

7. Em consonância com o artigo 25.º, n.º 1, o responsável pelo tratamento aplica as *medidas* técnicas e organizativas *adequadas* destinadas a aplicar os princípios da proteção de dados e a integrar as *garantias necessárias* no tratamento, a fim de cumprir os requisitos e proteger os direitos e as liberdades dos titulares dos dados. Tanto as medidas adequadas como as garantias necessárias destinam-se a servir a mesma finalidade de proteger os direitos dos titulares dos dados e de garantir que a proteção dos seus dados pessoais é incluída no tratamento.

8. *As medidas técnicas e organizacionais* e as *garantias* necessárias podem ser entendidas num sentido amplo como qualquer método ou meio que um responsável pelo tratamento pode aplicar no tratamento. Ser *adequado* significa que as medidas e as garantias necessárias devem permitir alcançar o objetivo pretendido, ou seja, devem aplicar *eficazmente* os princípios da proteção de dados[3]. A exigência de adequação está, pois, estreitamente relacionada com a exigência de eficácia.

9. Uma garantia e medida técnica ou organizativa pode ser qualquer coisa, desde a utilização de soluções técnicas avançadas à formação de base do pessoal. Exemplos que se poderão adequar, dependendo do contexto e dos riscos associados ao tratamento em questão, incluem a pseudonimização dos dados pessoais[4]; armazenar os dados pessoais num formato estruturado e comummente legível por máquina; permitir aos titulares dos dados intervir no tratamento; fornecer informações sobre a

[3] A «eficácia» é abordada no subcapítulo 2.1.2.
[4] Definida no artigo 4.º, n.º 5, do RGPD.

conservação de dados; possuir sistemas de deteção de programas maliciosos; dar formação aos funcionários sobre «ciber-higiene» básica; estabelecer sistemas de gestão da segurança da informação e da privacidade, obrigando contratualmente os fornecedores a aplicar práticas específicas de minimização dos dados, etc.

10. As normas, boas práticas e códigos de conduta reconhecidos por associações e outros organismos representativos de categorias de responsáveis pelo tratamento podem ser úteis na determinação de medidas adequadas. Contudo, o responsável pelo tratamento deve verificar a adequação das medidas ao tratamento específico em questão.

2.1.2 Destinadas a aplicar com eficácia os princípios da proteção de dados e a proteger os direitos e liberdades dos titulares dos dados

11. Os *princípios da proteção de dados* encontram-se no artigo 5.º (a seguir designados «os princípios»), os *direitos e liberdades dos titulares dos dados* são os direitos e liberdades fundamentais das pessoas singulares e, em particular, o direto à proteção dos seus dados pessoais, cuja proteção é referida no artigo 1.º, n.º 2, como o objetivo do RGPD (a seguir designados «os direitos»)[5]. A formulação precisa consta da Carta dos Direitos Fundamentais da UE. É essencial que o responsável pelo tratamento compreenda o significado dos *princípios* e dos *direitos* enquanto base da proteção oferecida pelo RGPD, especificamente a obrigação de PDdCD.

12. Ao aplicar as medidas técnicas e organizativas adequadas, as medidas e garantias devem ser *concebidas* tendo em vista a aplicação eficaz de cada um dos princípios supracitados e a subsequente proteção dos direitos.

Abordagem da eficácia

13. A eficácia está no cerne do conceito de proteção de dados desde a conceção. O requisito de aplicar os princípios com eficácia significa que os responsáveis pelo tratamento devem aplicar as medidas e as garantias necessárias para proteger esses princípios, a fim de garantir os direitos dos titulares dos dados. Cada medida aplicada deve produzir os resultados pretendidos para o tratamento previsto pelo responsável pelo tratamento. Esta observação tem duas consequências.

14. Em primeiro lugar, significa que o artigo 25.º não exige a aplicação de quaisquer medidas técnicas e organizativas específicas, mas que as medidas e garantias escolhidas devem ser específicas para a aplicação dos princípios de proteção de dados no tratamento específico em questão. Ao fazê-lo, as medidas e as garantias devem ser concebidas de modo a serem sólidas e o responsável pelo tratamento deve conseguir aplicar novas medidas a fim de se adequar a um eventual aumento do risco[6]. A eficácia ou ausência de eficácia das medidas dependerá, por conseguinte, do contexto do tratamento em questão e de uma avaliação de determinados elementos que têm de ser tidos em conta

[5] Ver considerando 4 do RGPD.

[6] Os princípios fundamentais aplicáveis aos responsáveis pelo tratamento (isto é, legitimidade, minimização dos dados, limitação das finalidades, transparência, integridade dos dados, exatidão dos dados) devem manter-se, independentemente do tratamento e dos riscos para os titulares dos dados. No entanto, o devido respeito pela natureza e pelo âmbito desse tratamento sempre foi parte integrante da aplicação desses princípios, pelo que estes são intrinsecamente moduláveis. Grupo de Trabalho do Artigo 29.º, «Declaração sobre o papel de uma abordagem baseada no risco em relação aos quadros jurídicos em matéria de proteção de dados», WP 218 de 30 de maio de 2014, p. 3. ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

aquando da definição dos meios de tratamento. Os elementos supramencionados são abordados no ponto 2.1.3.

15. Em segundo lugar, os responsáveis pelo tratamento devem poder demonstrar que os princípios foram mantidos.

16. As medidas e as garantias aplicadas devem alcançar o efeito pretendido em termos de proteção de dados, devendo o responsável pelo tratamento possuir documentação relativa às medidas técnicas e organizacionais aplicadas.[7] Para o efeito, o responsável pelo tratamento pode determinar indicadores-chave de desempenho (ICD) adequados para demonstrar a conformidade. Um ICD é um valor mensurável escolhido pelo responsável pelo tratamento que demonstra a eficácia com que o responsável pelo tratamento cumpre o seu objetivo de proteção de dados. Os ICD podem ser *quantitativos*, como a percentagem de falsos positivos ou falsos negativos, a redução de reclamações e a redução do tempo de resposta quando os titulares dos dados exercem os seus direitos, ou *qualitativos*, como as avaliações de desempenho, a utilização de grelhas de classificação ou as avaliações de peritos. Em alternativa aos ICD, os responsáveis pelo tratamento podem demonstrar a aplicação efetiva dos princípios apresentando a lógica subjacente à sua avaliação da eficácia das medidas e garantias escolhidas.

2.1.3 Elementos a ter em conta

17. O artigo 25.º, n.º 1, enumera os elementos que o responsável pelo tratamento tem de ter em conta ao determinar as medidas de uma operação de tratamento específica. A seguir, forneceremos orientações sobre a forma de aplicar estes elementos no processo de conceção, que inclui a conceção das definições por defeito. Todos estes elementos contribuem para determinar se uma medida é adequada para aplicar eficazmente os princípios. Assim, cada um destes elementos não é um objetivo *per se*, mas um de vários fatores a considerar conjuntamente para cumprir o objetivo.

2.1.3.1 «[T]écnicas mais avançadas»

18. O conceito de «técnicas mais avançadas» está presente em vários acervos da UE, por exemplo, na proteção do ambiente e na segurança dos produtos. No RGPD, a referência a «técnicas mais avançadas»[8] é feita não só no artigo 32.º, no que se refere às medidas de segurança[9][10] , mas também no artigo 25.º, alargando assim este critério de referência a todas as medidas técnicas e organizativas integradas no tratamento.

19. No contexto do artigo 25.º, a referência às «técnicas mais avançadas» impõe uma obrigação aos responsáveis pelo tratamento, aquando da determinação das medidas técnicas e organizativas adequadas, de **terem em conta os atuais progressos da tecnologia** disponível no mercado. É exigido que os responsáveis pelo tratamento tenham conhecimento e se mantenham a par dos avanços

[7] Ver considerandos 74 e 78.

[8] Ver a decisão proferida pelo Tribunal Constitucional Federal alemão no processo «Kalkar» em 1978: https://germanlawarchive.iuscomp.org/?p=67, que pode servir de base a uma metodologia para uma definição objetiva do conceito. Nessa base, o nível tecnológico das «técnicas mais avançadas» seria identificado entre o nível tecnológico «da investigação e dos conhecimentos científicos existentes» e as «regras tecnológicas geralmente aceites» mais estabelecidas. As «técnicas mais avançadas» podem, portanto, ser identificadas como o nível tecnológico de um serviço, tecnologia ou produto que existe no mercado e que é mais eficaz para alcançar os objetivos identificados.

[9] https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security

[10] www.teletrust.de/en/publikationen/broschueren/state-of-the-art-in-it-security/

tecnológicos; da forma como a tecnologia pode representar riscos ou oportunidades em matéria de proteção de dados para a operação de tratamento e da forma de aplicar e atualizar as medidas e garantias que *garantem a aplicação eficaz* dos princípios e dos direitos dos titulares dos dados, tendo em consideração o panorama tecnológico em evolução.

20. O conceito de «técnicas mais avançadas» é dinâmico e não pode ser definido de forma estática num determinado momento, devendo ser avaliado de forma *contínua* no contexto do progresso tecnológico. Perante os avanços tecnológicos, um responsável pelo tratamento poderia verificar que uma medida que outrora havia assegurado um nível adequado de proteção já não o faz. O facto de não se manter a par das evoluções tecnológicas poderia, por conseguinte, resultar no incumprimento do artigo 25.º.

21. O critério de «técnicas mais avançadas» não se aplica apenas às medidas tecnológicas, mas também às medidas organizativas. A ausência de medidas organizativas adequadas pode reduzir, ou mesmo comprometer totalmente, a eficácia de uma tecnologia escolhida. Podem constituir exemplos de medidas organizativas a adoção de políticas internas, formação atualizada sobre tecnologia, segurança e proteção de dados, bem como políticas de gestão e governação da segurança informática.

22. Os quadros, as normas, as certificações, os códigos de conduta, etc., existentes e reconhecidos em diversos domínios podem contribuir para a indicação das «técnicas mais avançadas» atuais no domínio de utilização em causa. Sempre que essas normas existam e assegurem um elevado nível de proteção ao titular dos dados, no mínimo, em conformidade com os requisitos legais, os responsáveis pelo tratamento devem tê-las em conta na conceção e na aplicação de medidas de proteção de dados.

2.1.3.2 «[C]ustos da sua aplicação»

23. O responsável pelo tratamento pode ter em conta os custos de aplicação na escolha e na aplicação das medidas técnicas e organizativas adequadas e das garantias necessárias para aplicar efetivamente os princípios a fim de proteger os direitos dos titulares dos dados. Os custos referem-se aos recursos em geral, incluindo tempo e recursos humanos.

24. O elemento de custo não exige que o responsável pelo tratamento gaste uma quantidade desproporcional de recursos quando existam medidas alternativas, menos exigentes em termos de recursos, apesar de eficazes. Contudo, o custo da aplicação é um fator a considerar para aplicar a proteção de dados desde a conceção e não um motivo para não a aplicar.

25. Assim, as medidas escolhidas devem assegurar que a atividade de tratamento prevista pelo responsável pelo tratamento não trata dados pessoais em violação dos princípios, independentemente do custo. Os responsáveis pelo tratamento devem poder gerir os custos globais a fim de poderem aplicar eficazmente todos os princípios e, consequentemente, proteger os direitos.

2.1.3.3 «[A] natureza, o âmbito, o contexto e as finalidades do tratamento dos dados»

26. Os responsáveis pelo tratamento devem ter em conta a natureza, o âmbito, o contexto e a finalidade do tratamento aquando da determinação das medidas necessárias.

27. Estes fatores devem ser interpretados de forma coerente com o seu papel noutras disposições do RGPD, como os artigos 24.º, 32.º e 35.º, com o objetivo de conceber princípios de proteção de dados no tratamento.

28. Em suma, o conceito de **natureza** pode ser entendido como o conjunto de características inerentes[11] ao tratamento. O **âmbito** refere-se à dimensão e ao alcance do tratamento. O **contexto** refere-se às circunstâncias do tratamento, que podem influenciar as expectativas do titular dos dados, enquanto a **finalidade** diz respeito aos objetivos do tratamento.

2.1.3.4 «[R]iscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis»

29. O RGPD adota uma abordagem coerente baseada no risco em muitas das suas disposições, nos artigos 24.º, 25.º, 32.º e 35.º, com vista a identificar medidas técnicas e organizativas adequadas para proteger as pessoas singulares e os seus dados pessoais e a cumprir os requisitos do RGPD. Os bens a proteger são sempre os mesmos (as pessoas, através da proteção dos seus dados pessoais), contra os mesmos riscos (para os direitos individuais), tendo em conta as mesmas condições (a natureza, o âmbito, o contexto e as finalidades do tratamento).

30. Ao efetuar a análise de risco necessária para dar cumprimento ao artigo 25.º, o responsável pelo tratamento deve identificar os riscos para os direitos dos titulares dos dados de que se reveste uma violação dos princípios e determinar a sua probabilidade e gravidade, a fim de aplicar medidas para atenuar efetivamente os riscos identificados. Uma avaliação sistemática e exaustiva do tratamento é crucial aquando das avaliações dos riscos. Por exemplo, um responsável pelo tratamento avalia os riscos específicos inerentes à ausência de consentimento livremente dado, o que constitui uma violação do princípio da licitude, no decurso do tratamento de dados pessoais de crianças e jovens com menos de 18 anos enquanto grupo vulnerável, num caso em que não existe outro fundamento jurídico, e aplica medidas adequadas para abordar e atenuar eficazmente os riscos inerentes a este grupo de titulares de dados identificados.

31. As «Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD)[12]» do CEPD, que se centram na determinação da probabilidade de uma operação de tratamento resultar ou não num elevado risco para o titular dos dados, fornecem igualmente orientações sobre a forma de avaliar os riscos em matéria de proteção de dados e realizar uma avaliação dos riscos em matéria de proteção de dados. Estas orientações podem igualmente ser úteis durante a avaliação dos riscos em todos os artigos supracitados, incluindo o artigo 25.º.

32. A abordagem baseada no risco não exclui a utilização de linhas de base, boas práticas e normas. Estas poderão constituir instrumentos úteis aos responsáveis pelo tratamento para fazer face a riscos semelhantes em situações semelhantes (natureza, âmbito, contexto e finalidade do tratamento). No entanto, mantém-se a obrigação prevista no artigo 25.º (bem como no artigo 24.º, no artigo 32.º e no artigo 35.º, n.º 7, alínea c)) de ter em conta os «*riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis*». Por conseguinte, os responsáveis pelo tratamento, embora apoiados por esses instrumentos, devem realizar sempre uma avaliação dos riscos em matéria de proteção de dados numa base casuística para a atividade de tratamento em causa e verificar a eficácia das medidas e garantias adequadas propostas. Adicionalmente, poderá ser necessária uma AIPD ou a atualização de uma AIPD existente.

---

[11] Entre os exemplo incluem-se categorias especiais de dados pessoais, decisões automáticas, relações de poder assimétricas, tratamento imprevisível, dificuldade do titular dos dados em exercer os seus direitos, etc.

[12] Grupo de Trabalho do Artigo 29.º, «Orientações 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», WP 248 rev.01, 4 de outubro de 2017, ec.europa.eu/newsroom/document.cfm?doc_id=47711 – subscritas pelo CEPD.

2.1.4 Aspeto temporal

2.1.4.1 No momento de definição dos meios de tratamento

33. A proteção de dados desde a conceção deve ser aplicada «*no momento de definição dos meios de tratamento*».

34. Os «*meios de tratamento*» variam entre os elementos de conceção gerais e pormenorizados do tratamento, incluindo a arquitetura, os procedimentos, os protocolos, a disposição e a imagem.

35. O «*momento de definição dos meios de tratamento*» refere-se ao período em que o responsável pelo tratamento está a decidir como será realizado o tratamento e a forma como este ocorrerá, bem como os mecanismos que serão utilizados para a realização desse tratamento. É no processo de tomada de tais decisões que o responsável pelo tratamento tem de avaliar as garantias e medidas adequadas para aplicar eficazmente os princípios e direitos dos titulares dos dados no tratamento, e ter em conta elementos como as técnicas mais avançadas, os custos da sua aplicação, a natureza, o âmbito, o contexto e as finalidades, bem como os riscos. O que precede inclui o tempo de aquisição e implementação do *software*, *hardware* e serviços de tratamento de dados.

36. A tomada em consideração precoce da PDdCD é crucial para uma aplicação bem-sucedida dos princípios e para a proteção dos direitos dos titulares dos dados. Acresce que, do ponto de vista da relação custo-benefício, também é do interesse dos responsáveis pelo tratamento avaliar a PDdCD o mais rapidamente possível, uma vez que poderá ser difícil e dispendioso introduzir posteriormente alterações nos planos já elaborados e nas operações de tratamento já concebidas.

2.1.4.2 Aquando do tratamento propriamente dito (manutenção e revisão dos requisitos de proteção de dados)

37. Uma vez iniciado o tratamento, o responsável pelo tratamento tem a obrigação permanente de manter a PDdCD, ou seja, a aplicação efetiva e continuada dos princípios para proteger os direitos, de se manter a par das técnicas mais avançadas, de reavaliar o nível de risco, etc. A natureza, o âmbito e o contexto das operações de tratamento, bem como o risco, podem mudar ao longo do tratamento, o que significa que o responsável pelo tratamento deve reavaliar as operações de tratamento através de revisões e avaliações regulares da eficácia das medidas e garantias escolhidas.

38. A obrigação de manter, rever e atualizar, na medida do necessário, a operação de tratamento também se aplica aos sistemas pré-existentes, o que significa que os sistemas herdados concebidos antes da entrada em vigor do RGPD devem ser objeto de revisões e de manutenção destinadas a garantir a aplicação de medidas e garantias que apliquem os princípios e os direitos dos titulares dos dados com eficácia, conforme descrito nas presentes orientações.

39. Esta obrigação é igualmente extensível a qualquer tratamento efetuado através de subcontratantes de dados. As operações dos subcontratantes devem ser regularmente revistas e avaliadas pelos responsáveis pelo tratamento para garantir que permitem o cumprimento contínuo dos princípios e possibilitam que o responsável pelo tratamento de dados cumpra as suas obrigações a este respeito.

2.2 Artigo 25.º, n.º 2: Proteção de dados por defeito

2.2.1 Por defeito, apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento.

40. Um «defeito», na definição geral das ciências informáticas, refere-se ao valor pré-existente ou pré-selecionado de um parâmetro configurável que é atribuído a uma aplicação informática, programa informático ou dispositivo. Tais parâmetros são igualmente designados por «pré-seleções» ou «pré-seleções de fábrica», especialmente no que se refere a dispositivos eletrónicos.

41. Por conseguinte, a expressão «por defeito» no tratamento de dados pessoais refere-se a fazer escolhas relativas aos valores de configuração ou às opções de tratamento que são estabelecidos ou estipulados num sistema de tratamento, tais como uma aplicação de *software*, serviço ou dispositivo, ou um procedimento de tratamento manual que afeta a quantidade de dados pessoais recolhidos, a amplitude do tratamento, o período de conservação e a sua acessibilidade.

42. O responsável pelo tratamento deve escolher e ser responsável pela aplicação de definições e opções de tratamento por defeito de forma que apenas o tratamento estritamente necessário para cumprir a finalidade definida e legítima seja realizado por defeito. Neste caso, os responsáveis pelo tratamento devem basear-se na sua avaliação da necessidade do tratamento no que diz respeito aos fundamentos jurídicos do artigo 6.º, n.º 1. Tal significa que, por defeito, o responsável pelo tratamento não deve recolher mais dados do que os necessários, não deve tratar os dados recolhidos mais do que o necessário para as suas finalidades, nem deve armazenar os dados durante mais tempo do que o necessário. O requisito básico é a integração da proteção de dados no tratamento por defeito.

43. O responsável pelo tratamento é obrigado a determinar previamente para que finalidades específicas, explícitas e legítimas os dados pessoais são recolhidos e tratados[13]. Por defeito, as medidas têm de ser adequadas para assegurar que apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. As orientações da AEPD para avaliar a necessidade e a proporcionalidade das medidas que limitam o direito à proteção de dados pessoais podem também ser úteis para decidir os dados que é necessário tratar para alcançar uma finalidade específica[14] [15] [16].

44. Se utilizar *software* de terceiros ou *software* disponível no comércio, o responsável pelo tratamento deve realizar uma avaliação dos riscos do produto e certificar-se de que as funções que não têm base jurídica ou não são compatíveis com as finalidades a que se destina o tratamento não estão ativas.

45. As mesmas considerações aplicam-se às medidas organizativas de apoio às operações de tratamento. Devem ser concebidas para tratar, no início, apenas a quantidade mínima de dados pessoais necessária

[13] Artigo 5.º, n.º 1, alíneas b), c), d) e e), do RGPD.
[14] AEPD, «Guidelines on assessing the necessity and proportionality of measures that limit the right to data protection» [Orientações relativas à avaliação da necessidade e da proporcionalidade das medidas que limitam o direito à proteção de dados], 25 de fevereiro de 2019, edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf.
[15] Ver igualmente AEPD, «Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit» [Avaliação da necessidade de medidas que limitem o direito fundamental à proteção de dados pessoais: um conjunto de ferramentas] https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_en
[16] Para mais informações sobre necessidade, ver Grupo de Trabalho do Artigo 29.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, 9 de abril de 2014, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_pt.pdf.

para as operações específicas. Este aspeto deve ser especialmente tido em consideração ao atribuir o acesso aos dados a pessoal com diferentes funções e diferentes necessidades de acesso.

46. As «medidas técnicas e organizativas» adequadas no contexto da proteção de dados por defeito são entendidas da mesma forma que no ponto 2.1.1, mas aplicadas especificamente à implementação do princípio da minimização dos dados.

47. A obrigação supracitada de apenas tratar os dados pessoais que forem necessários para cada finalidade específica aplica-se aos elementos que se seguem.

2.2.2 Dimensões da obrigação de minimização dos dados

48. O artigo 25.º, n.º 2, enumera as dimensões da obrigação de minimização de dados para tratamento por defeito e estipula que essa obrigação se aplica à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade.

2.2.2.1 «[Q]uantidade de dados pessoais recolhidos»

49. Os responsáveis pelo tratamento devem ter em consideração tanto o volume de dados pessoais como os tipos, as categorias e o nível de pormenor dos dados pessoais necessários para efeitos do tratamento. As suas escolhas em termos de conceção devem ter em conta os riscos acrescidos para os princípios da integridade e da confidencialidade, da minimização dos dados e da limitação da conservação ao recolherem grandes quantidades de dados pessoais pormenorizados e compará-los com os riscos reduzidos da recolha de menos informações e/ou de informações menos pormenorizadas sobre os titulares dos dados. Em todo o caso, a configuração por defeito não deve incluir a recolha de dados pessoais que não sejam necessários para a finalidade específica do tratamento. Por outras palavras, se determinadas categorias de dados pessoais forem desnecessárias ou se não forem necessários dados pormenorizados por serem suficientes dados menos granulares, não serão recolhidos quaisquer dados pessoais excedentários.

50. Os mesmos requisitos por defeito aplicam-se aos serviços, independentemente da plataforma ou do dispositivo utilizado: só podem ser recolhidos os dados pessoais necessários para a finalidade em causa.

2.2.2.2 «[E]xtensão do seu tratamento»

51. As operações de tratamento[17] de dados pessoais devem limitar-se ao necessário. Muitas operações de tratamento podem contribuir para uma finalidade de tratamento. Não obstante, o facto de determinados dados pessoais serem necessários para alcançar uma finalidade não significa que possam ser aplicados todos os tipos e frequências de operações de tratamento dos dados. Os responsáveis pelo tratamento devem igualmente ter o cuidado de não alargar os limites das «finalidades compatíveis» do artigo 6.º, n.º 4, e ter em mente qual será o tratamento dentro das expectativas razoáveis dos titulares dos dados.

[17] De acordo com o artigo 4.º, n.º 2,do RGPD, estas incluem a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição.

2.2.2.3 «[S]eu prazo de conservação»

52. Os dados pessoais recolhidos não são armazenados se tal não for necessário para a finalidade do tratamento e se não existirem outras finalidades e fundamentos jurídicos compatíveis nos termos do artigo 6.º, n.º 4. Qualquer conservação deve ser objetivamente justificável, na medida do necessário, pelo responsável pelo tratamento de dados em conformidade com o princípio da responsabilidade.

53. O responsável pelo tratamento deve limitar o período de conservação ao necessário para a finalidade em causa. Se os dados pessoais deixarem de ser necessários para a finalidades do tratamento, devem, por defeito, ser apagados ou anonimizados. A duração do período de conservação varia, assim, em função da finalidade do tratamento em causa. Esta obrigação está diretamente relacionada com o princípio da limitação da conservação previsto no artigo 5.º, n.º 1, alínea e), e deve ser cumprida por defeito, isto é, o responsável pelo tratamento deve dispor de procedimentos sistemáticos de apagamento ou anonimização de dados integrados no tratamento.

54. A anonimização[18] de dados pessoais é uma alternativa ao apagamento, desde que todos os elementos contextuais pertinentes sejam tidos em conta e que a probabilidade e a gravidade do risco, incluindo o risco de reidentificação, sejam regularmente avaliados[19].

2.2.2.4 «[S]ua acessibilidade»

55. O responsável pelo tratamento tem de limitar as pessoas que podem ter acesso aos dados pessoais com base numa avaliação da necessidade e garantir igualmente que os dados pessoais estão, de facto, acessíveis a quem deles necessita quando necessário, por exemplo em situações críticas. Os controlos de acesso devem ser monitorizados no que se refere a todo o fluxo de dados durante o tratamento.

56. O artigo 25.º, n.º 2, estabelece ainda que os dados pessoais não podem ser disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. O responsável pelo tratamento deve, por defeito, dar ao titular dos dados a possibilidade de intervir antes publicar ou disponibilizar, de qualquer outra forma, dados pessoais sobre o titular dos dados a um número indeterminado de pessoas singulares.

57. A disponibilização de dados pessoais a um número indeterminado de pessoas pode resultar numa divulgação dos dados ainda mais vasta do que a inicialmente prevista. Este aspeto é de particular importância no contexto da Internet e dos motores de pesquisa. Tal significa que os responsáveis pelo tratamento devem, por defeito, dar aos titulares dos dados a oportunidade de intervirem antes de os dados pessoais serem disponibilizados na Internet aberta. Este aspeto assume particular importância no caso de crianças e de grupos vulneráveis.

58. Consoante os fundamentos jurídicos do tratamento, a oportunidade de intervir pode variar de acordo com o contexto do tratamento. Por exemplo, pedir consentimento para tornar os dados pessoais

[18] Grupo de Trabalho do Artigo 29.º, «Parecer 05/2014 sobre técnicas de anonimização», WP 216, 10 de abril de 2014, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf.

[19] Ver o artigo 4.º, n.º 1, do RGPD, o considerando 26 do RGPD, e o «Parecer 05/2014 sobre técnicas de anonimização» do Grupo de Trabalho do Artigo 29.º. Ver também a subsecção sobre a «limitação da conservação» da secção 3 do presente documento, onde é referida a necessidade de o responsável pelo tratamento assegurar a eficácia da(s) técnica(s) de anonimização aplicada(s).

acessíveis ao público ou para ter definições de privacidade que permitam aos próprios titulares dos dados controlar o acesso do público.

59. Mesmo que os dados pessoais sejam disponibilizados ao público com a permissão e compreensão de um titular de dados, tal não significa que quaisquer outros responsáveis pelo tratamento com acesso aos dados pessoais possam tratá-los livremente, para fins próprios – deve, para este efeito, existir uma base jurídica própria[20].

3 APLICAÇÃO DOS PRINCÍPIOS DA PROTEÇÃO DE DADOS NO TRATAMENTO DE DADOS PESSOAIS RECORRENDO À PROTEÇÃO DE DADOS DESDE A CONCEÇÃO E POR DEFEITO

60. Em todas as fases de conceção das atividades de tratamento, nomeadamente adjudicação de contratos, concursos, externalização, desenvolvimento, apoio, manutenção, ensaios, conservação, apagamento, etc., o responsável pelo tratamento deve ter em conta e considerar os vários elementos da PDdCD, que serão ilustrados pelos exemplos apresentados no presente capítulo, no contexto da aplicação dos princípios[21] [22] [23].

61. Os responsáveis pelo tratamento devem aplicar os princípios para assegurar a PDdCD. Estes princípios incluem transparência, licitude, equidade, limitação da finalidade, minimização dos dados, exatidão, limitação da conservação, integridade e confidencialidade e responsabilidade. Estes princípios estão descritos no artigo 5.º e no considerando 39 do RGPD. Para ter uma compreensão perfeita de como aplicar a PDdCD, é sublinhada a importância de compreender o significado de cada um dos princípios.

62. Ao apresentar exemplos de como operacionalizar a PDdCD, elaborámos listas de **elementos essenciais da PDdCD** para cada um dos princípios. Os exemplos, embora realcem o princípio específico da proteção de dados em questão, podem igualmente coincidir com outros princípios estreitamente relacionados. O CEPD sublinha que os elementos-chave e os exemplos apresentados a seguir não são exaustivos nem vinculativos, destinando-se a servir de elementos orientadores para cada um dos princípios. Os responsáveis pelo tratamento necessitam de avaliar a forma de garantir o cumprimento dos princípios no contexto da operação de tratamento concreta em questão.

63. Embora esta secção se centre na aplicação dos princípios, o responsável pelo tratamento deve igualmente implementar formas *adequadas* e *eficazes* de proteger os direitos dos titulares dos dados, também em conformidade com o capítulo III do RGPD se tal não for já mandatado pelos próprios princípios.

64. O princípio da responsabilidade é abrangente: exige que o responsável pelo tratamento seja responsável pela escolha das medidas técnicas e organizativas necessárias.

[20] Ver processo Satakunnan Markkinapörssi Oy e Satamedia Oy/Finlândia, petição n.º 931/13.
[21] É possível encontrar mais exemplos no documento da Autoridade Norueguesa de Proteção de Dados intitulado «Software Development with Data Protection by Design and by Default» [Desenvolvimento de programas informáticos com proteção de dados desde a conceção e por defeito], de 28 de novembro de 2017, www.datatilsynet.no/en/about-privacy/virksomhetenes-plikter/innebygd-personvern/data-protection-by-design-and-by-default/?id=7729.
[22] https://www.cnil.fr/en/cnil-publishes-gdpr-guide-developers
[23] https://www.aepd.es/sites/default/files/2019-12/guia-privacidad-desde-diseno_en.pdf

3.1 Transparência[24]

65. O responsável pelo tratamento tem de ser claro e aberto com o titular dos dados sobre a forma como irá recolher, utilizar e partilhar os dados pessoais. A transparência consiste em permitir que os titulares dos dados compreendam e, se necessário, exerçam os seus direitos previstos nos artigos 15.º a 22.º. O princípio está consagrado nos artigos 12.º, 13.º, 14.º e 34.º. As medidas e garantias adotadas para apoiar o princípio da transparência devem igualmente apoiar a aplicação destes artigos.

66. Os principais elementos de conceção e por defeito relativos ao princípio da transparência podem incluir:

- Clareza – As informações devem ser redigidas em linguagem clara e simples e ser concisas e inteligíveis.
- Semântica – A comunicação deve ter um significado claro para o público em questão.
- Acessibilidade – As informações devem ser facilmente acessíveis para o titular dos dados.
- Contextual – As informações devem ser fornecidas no momento oportuno e na forma adequada.
- Pertinência – As informações devem ser pertinentes e aplicáveis ao titular dos dados em questão.
- Conceção universal – As informações devem ser acessíveis a todos os titulares de dados, incluindo a utilização de línguas legíveis por máquinas, para facilitar e automatizar a legibilidade e a clareza.
- Compreensível – Os titulares dos dados devem ter uma compreensão razoável do que podem esperar no que diz respeito ao tratamento dos seus dados pessoais, especialmente quando os titulares dos dados são crianças ou outros grupos vulneráveis.
- Multicanal – As informações devem ser fornecidas em diferentes canais e meios, e não apenas nos textuais, para aumentar a probabilidade de a informação chegar efetivamente ao titular dos dados.
- Em camadas – As informações devem ser dispostas em camadas, de modo a resolver a tensão entre a integridade e a compreensão, tendo simultaneamente em conta as expectativas razoáveis dos titulares dos dados.

Exemplo[25]

Um responsável pelo tratamento está a elaborar uma política de privacidade para o seu sítio Web, a fim de cumprir os requisitos de transparência. A política de privacidade não deve conter uma grande quantidade de informação que seja difícil de penetrar e de compreender para o titular de dados médio. Deve ser redigida numa linguagem clara e concisa e permitir que o utilizador do sítio Web compreenda facilmente a forma como os seus dados pessoais são tratados. Por conseguinte, o responsável pelo tratamento fornece informações em vários níveis, nos quais são realçados os pontos mais importantes. Deve haver informações mais pormenorizadas facilmente acessíveis. São fornecidos menus pendentes e ligações para outras páginas para explicar melhor os diferentes elementos e conceitos utilizados na política. O responsável pelo tratamento garante igualmente que as informações sejam fornecidas em

[24] O Grupo de Trabalho do Artigo 29.º apresenta uma explicação mais pormenorizada do conceito de transparência nas suas «Orientações relativas à transparência na aceção do Regulamento 2016/679», WP 260 rev.01, 11 de abril de 2018, ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025 – subscritas pelo CEPD.

[25] A Autoridade Francesa de Proteção de Dados publicou vários exemplos que ilustram boas práticas no que se refere à prestação de informações aos utilizadores, bem como a outros princípios de transparência: https://design.cnil.fr/en/.

múltiplos canais, disponibilizando vídeos para explicar os pontos mais importantes das informações escritas. A sinergia entre as várias páginas é vital para garantir que a abordagem em camadas não aumenta a confusão, antes a reduz.

Os titulares dos dados não devem ter dificuldade em aceder à política de privacidade. Por conseguinte, a política de privacidade é disponibilizada e está visível em todas as páginas Web do sítio em questão, de modo que o titular dos dados esteja sempre apenas a um clique de distância do acesso às informações. As informações fornecidas são igualmente concebidas em conformidade com as boas práticas e as normas de desenho universal, de modo a torná-las acessíveis a todos.

Além disso, as informações necessárias devem igualmente ser fornecidas no contexto certo e no momento apropriado. Uma vez que o responsável pelo tratamento realiza muitas operações de tratamento utilizando os dados recolhidos no sítio Web, uma política geral de privacidade para o sítio Web não é por si só suficiente para que o responsável pelo tratamento cumpra os requisitos de transparência. Por conseguinte, o responsável pelo tratamento concebe um fluxo de informações, apresentando ao titular dos dados informações pertinentes nos contextos adequados, com recurso, nomeadamente, a fragmentos informativos ou janelas instantâneas. Por exemplo, ao solicitar ao titular dos dados que introduza dados pessoais, o responsável pelo tratamento informa-o da forma como os dados pessoais serão tratados e da razão pela qual esses dados pessoais são necessários para o tratamento.

3.2 Licitude

67. O responsável pelo tratamento tem de identificar uma base jurídica válida para o tratamento de dados pessoais. As medidas e garantias adotadas devem apoiar o requisito de garantir que todo o ciclo de vida do tratamento está em consonância com os fundamentos jurídicos pertinentes do tratamento.

68. Os principais elementos de conceção e por defeito relativos à licitude podem incluir:
    - Pertinência – Deve ser aplicada a base jurídica correta ao tratamento.
    - Diferenciação[26] – A base jurídica utilizada para cada atividade de tratamento deve ser diferenciada.
    - Finalidade especificada – A base jurídica adequada tem de estar claramente ligada à finalidade específica do tratamento[27].
    - Necessidade – O tratamento tem de ser necessário e incondicional para que a finalidade seja lícita.
    - Autonomia – Deve ser concedido ao titular dos dados o mais elevado grau de autonomia possível no que diz respeito ao controlo sobre os dados pessoais no âmbito da base jurídica.
    - Concessão do consentimento – O consentimento deve ser dado através de uma manifestação de vontade livre, específica, informada e inequívoca[28]. Deve ser dada especial atenção à capacidade das crianças e dos jovens de darem o seu consentimento informado.

[26] CEPD, «Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects» [Orientações 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], versão 2.0, 8 de outubro de 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf.

[27] Ver abaixo a secção sobre a limitação das finalidades.

[28] Ver «Guidelines 05/2020 on consent under Regulation 2016/679» [Orientações 05/2020 sobre o consentimento ao abrigo do Regulamento 2016/679]. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

- Retirada do consentimento – Quando o consentimento for a base jurídica, o tratamento deve facilitar a retirada do consentimento. A retirada deve ser tão fácil como a concessão do consentimento. Caso contrário, o mecanismo de consentimento do responsável pelo tratamento não cumpre o RGPD.[29]
- Equilíbrio de interesses – Nos casos em que interesses legítimos constituam a base jurídica, o responsável pelo tratamento deve ponderar os interesses de forma equilibrada, tendo especialmente em conta o desequilíbrio de poder, nomeadamente no caso de crianças com idade inferior a 18 anos e de outros grupos vulneráveis. Devem ser adotadas medidas e garantias para atenuar o impacto negativo sobre os titulares de direitos.
- Predeterminação – A base jurídica deve ser estabelecida antes de o tratamento ter lugar.
- Cessação – Se a base jurídica deixar de ser aplicável, o tratamento deve cessar em conformidade.
- Ajustamento – Se houver uma alteração válida da base jurídica para o tratamento, o tratamento propriamente dito tem de ser ajustado de acordo com a nova base jurídica[30].
- Repartição de responsabilidades – Sempre que se preveja um controlo conjunto, as partes têm de repartir de forma clara e transparente as respetivas responsabilidades para com o titular dos dados e conceber as medidas para o tratamento em conformidade com essa repartição.

Exemplo

Um banco tenciona disponibilizar um serviço para melhorar a eficiência na gestão dos pedidos de empréstimo. A ideia subjacente ao serviço é a de que o banco, ao solicitar a permissão do cliente, pode recuperar dados sobre o cliente diretamente junto das autoridades fiscais. Este exemplo não tem em conta o tratamento de dados pessoais de outras fontes.

A obtenção de dados pessoais sobre a situação financeira do titular dos dados é necessária para diligências a pedido do titular dos dados prévias à celebração de um contrato de empréstimo[31]. No entanto, a recolha de dados pessoais diretamente junto da administração fiscal não é considerada necessária, dado que o cliente pode celebrar um contrato em que forneça ele próprio as informações da administração fiscal. Embora o banco possa ter um interesse legítimo em obter a documentação diretamente junto das autoridades fiscais, por exemplo para garantir a eficiência no tratamento dos empréstimos, conceder aos bancos acesso direto aos dados pessoais dos requerentes comporta riscos relacionados com a utilização ou potencial utilização abusiva de direitos de acesso.

Ao aplicar o princípio da licitude, o responsável pelo tratamento apercebe-se de que, neste contexto, não pode utilizar a base do que é «necessário para o contrato» na parte do tratamento que envolve a recolha de dados pessoais diretamente junto das autoridades fiscais. O facto de este tratamento específico apresentar o risco de o titular dos dados se envolver menos no tratamento dos seus dados é também um fator pertinente para avaliar a licitude do próprio tratamento. O banco conclui que esta parte do tratamento carece de outra base jurídica. No Estado-Membro em que o responsável pelo

[29] Ver «Guidelines 05/2020 on consent under Regulation 2016/679» [Orientações 05/2020 sobre o consentimento ao abrigo do Regulamento 2016/679], p. 24. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[30] Se a base jurídica original for o consentimento, ver «Guidelines 05/2020 on consent under Regulation 2016/679» [Orientações 05/2020 sobre o consentimento ao abrigo do Regulamento 2016/679]. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

[31] Ver artigo 6.º, n.º 1, alínea b), do RGPD.

tratamento está situado, há legislação nacional que permite que o banco recolha informações diretamente junto da administração fiscal sempre que o titular dos dados o consinta previamente.

Por conseguinte, o banco apresenta informações sobre o tratamento na plataforma de pedidos em linha de uma forma que facilite a compreensão, pelos titulares dos dados, do tratamento obrigatório e do tratamento facultativo. As opções de tratamento, por defeito, não permitem a recuperação de dados diretamente junto de outras fontes que não o próprio titular dos dados, e a opção de recuperação direta de informações é apresentada de uma forma que não desencoraja o titular dos dados de se abster. Qualquer consentimento dado para recolher dados diretamente junto de outros responsáveis pelo tratamento é um direito temporário de acesso a um conjunto específico de informações.

Qualquer consentimento dado é tratado eletronicamente de forma documentável, e os titulares dos dados dispõem de uma forma fácil de controlar o que consentiram e de retirar o seu consentimento.

O responsável pelo tratamento avaliou previamente estes requisitos em matéria de PDdCD e inclui todos estes critérios na sua especificação dos requisitos para o concurso relativo à aquisição da plataforma. O responsável pelo tratamento está ciente de que, se não incluir os requisitos em matéria de PDdCD no concurso, poderá ser demasiado tarde, ou muito dispendioso, aplicar a proteção de dados posteriormente.

3.3 Lealdade

69. A lealdade é um princípio basilar que exige que os dados pessoais não sejam tratados de forma injustificadamente prejudicial, ilicitamente discriminatória, inesperada ou enganadora para o titular dos dados. As medidas e garantias que aplicam o princípio da lealdade apoiam igualmente os direitos e liberdades dos titulares dos dados, especificamente o direito à informação (transparência), o direito de intervir (acesso, apagamento, portabilidade dos dados, retificação) e o direito de limitar o tratamento (direito de não estar sujeito a decisões individuais automatizadas e à não discriminação dos titulares dos dados em tais processos).

70. Os principais elementos de lealdade da conceção e por defeito podem incluir:
    - Autonomia – Os titulares dos dados devem beneficiar do mais elevado grau de autonomia possível para determinar a utilização dos seus dados pessoais, bem como em relação ao âmbito e às condições dessa utilização ou tratamento.
    - Interação – Os titulares dos dados têm de ser capazes de comunicar com o responsável pelo tratamento e exercer os seus direitos em relação aos dados pessoais por este tratados.
    - Expectativa – O tratamento deve corresponder às expectativas razoáveis dos titulares dos dados.
    - Não discriminação – O responsável pelo tratamento não deve discriminar injustamente os titulares dos dados.
    - Não exploração – O responsável pelo tratamento não deve explorar as necessidades ou vulnerabilidades dos titulares dos dados.
    - Escolha do consumidor – O responsável pelo tratamento não deve «vincular» os seus utilizadores de forma injusta. Sempre que um serviço que trate dados pessoais tenha direitos de propriedade, pode criar um bloqueio ao serviço, o que pode não ser justo, se prejudicar a possibilidade de os titulares dos dados exercerem o seu direito de portabilidade de dados nos termos do artigo 20.º.

- Equilíbrio de poder – O equilíbrio de poder deve ser um objetivo fundamental da relação entre o responsável pelo tratamento e o titular dos dados. Devem ser evitados desequilíbrios de poder. Quando tal não for possível, tais desequilíbrios devem ser reconhecidos e devem ser tomadas as contramedidas adequadas.
- Ausência de transferência de riscos – Os responsáveis pelo tratamento não devem transferir os riscos da empresa para os titulares dos dados.
- Sem engano – As informações e opções do tratamento de dados devem ser apresentadas de forma objetiva e neutra, evitando qualquer linguagem ou conceção enganosa ou manipuladora.
- Respeito dos direitos – O responsável pelo tratamento deve respeitar os direitos fundamentais dos titulares dos dados, aplicar medidas e garantias adequadas e não interferir com esses direitos, a menos que expressamente justificado por lei.
- Ética – O responsável pelo tratamento deve ver o impacto mais amplo do tratamento nos direitos e na dignidade das pessoas singulares.
- Verdadeiro – O responsável pelo tratamento deve disponibilizar informações sobre a forma como trata os dados pessoais, agir como afirma que fará e não induzir em erro as pessoas em causa.
- Intervenção humana – O responsável pelo tratamento tem de incorporar uma intervenção humana *qualificada* capaz de revelar distorções que as máquinas possam criar, em conformidade com o direito de não estar sujeito a decisões individuais automatizadas constante do artigo 22.º[32].
- Algoritmos justos – Avaliar regularmente se os algoritmos estão a funcionar em consonância com as finalidades e ajustá-los para atenuar desequilíbrios detetados e garantir a lealdade no tratamento. Os titulares dos dados devem ser informados sobre o funcionamento do tratamento de dados pessoais com base em algoritmos que analisam ou fazem previsões sobre os mesmos, tais como aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências pessoais, fiabilidade ou comportamento, localização ou deslocações[33].

Exemplo 1

Um responsável pelo tratamento opera um motor de busca que trata principalmente dados pessoais gerados pelos utilizadores. O responsável pelo tratamento beneficia da existência de grandes quantidades de dados pessoais e da possibilidade de utilizar esses dados pessoais para fins publicitários específicos. Por conseguinte, o responsável pelo tratamento pretende influenciar os titulares dos dados a permitirem uma recolha e utilização mais exaustivas dos seus dados pessoais. O consentimento deve ser obtido mediante a apresentação de opções de tratamento ao titular dos dados.

Ao aplicar o princípio da lealdade, tendo em conta a natureza, o âmbito, o contexto e a finalidade do tratamento, o responsável pelo tratamento apercebe-se de que não pode apresentar as opções de uma forma que incentive o titular dos dados a permitir que o responsável pelo tratamento recolha

[32] Ver «Orientações sobre as decisões individuais automatizadas e a definição de perfis para efeitos do Regulamento (UE) 2016/679»https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
[33] Ver o considerando 71 do RGPD.

mais dados pessoais do que se as opções fossem apresentadas de forma igual e neutra. Tal significa que não pode apresentar as opções de tratamento de uma forma que dificulte aos titulares dos dados a opção de se absterem de partilhar os seus dados ou de ajustarem as suas configurações de privacidade e limitarem o tratamento. Estes são exemplos de padrões obscuros, contrários ao espírito do artigo 25.º. As opções por defeito para o tratamento não devem ser invasivas, e a escolha do tratamento posterior deve ser apresentada de modo a não pressionar o titular dos dados a dar o seu consentimento. Em consequência, o responsável pelo tratamento apresenta as opções de consentimento ou abstenção como duas opções igualmente visíveis, apresentando com rigor as ramificações de cada opção para o titular dos dados.

Exemplo 2

Outro responsável pelo tratamento trata dados pessoais para a prestação de um serviço de transferência em contínuo (*streaming*), em que os utilizadores podem escolher entre uma assinatura comum de qualidade normal e uma assinatura *premium* de qualidade superior. Como parte da assinatura *premium*, os assinantes obtêm um serviço a clientes prioritário.

No que se refere ao princípio da lealdade, o serviço a clientes prioritário concedido aos assinantes *premium* não pode discriminar o acesso dos assinantes normais ao exercício dos seus direitos em virtude do artigo 12.º do RGPD. Tal significa que, embora seja prestado aos assinantes *premium* um serviço prioritário, esta prioridade não pode resultar na ausência de medidas adequadas para responder às solicitações dos assinantes regulares sem atrasos indevidos e, em todo o caso, no prazo de um mês a contar da receção das solicitações.

Os clientes com serviço prioritário podem pagar para obter um serviço melhor, mas todos os titulares de dados devem ter acesso igual e indiscriminado para fazer valer os seus direitos e liberdades conforme previsto no artigo 12.º.

3.4 Limitação das finalidades[34]

71. O responsável pelo tratamento tem de recolher os dados para finalidades determinadas, explícitas e legítimas e não pode tratá-los posteriormente de uma forma incompatível com as finalidades para que foram recolhidos[35]. A conceção do tratamento deve, por conseguinte, basear-se no que é necessário para alcançar as finalidades. Se for necessário proceder a um tratamento posterior, o responsável pelo tratamento tem de começar por assegurar que esse tratamento tem finalidades compatíveis com as finalidades originais e conceber esse tratamento em conformidade. A compatibilidade ou não de uma nova finalidade deve ser avaliada de acordo com os critérios enunciados no artigo 6.º., n.º 4.

72. Os principais elementos de conceção e por defeito em matéria de limitação da finalidade podem incluir:

[34] O Grupo de Trabalho do Artigo 29.º forneceu orientações para a compreensão do princípio da limitação das finalidades nos termos da Diretiva 95/46/CE. Embora o parecer não tenha sido adotado pelo Grupo de Trabalho do Artigo 29.º, pode ser pertinente, uma vez que a redação do princípio é a mesma no âmbito do RGPD. Grupo de Trabalho do Artigo 29.º, «Parecer 03/2013 sobre a limitação da finalidade», WP 203, 2 de abril de 2013, ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

[35] Artigo 5.º, n.º 1, alínea b), do RGPD.

- Predeterminação – As finalidades legítimas devem ser determinadas antes da conceção do tratamento.
- Especificidade – As finalidades devem ser especificadas e explícitas quanto ao motivo do tratamento dos dados pessoais.
- Orientação para a finalidade – A finalidade do tratamento deve orientar a conceção do tratamento e estabelecer limites para o tratamento.
- Necessidade – A finalidade determina os dados pessoais que são necessários para o tratamento.
- Compatibilidade – Qualquer nova finalidade tem de ser compatível com a finalidade inicial para a qual os dados foram recolhidos e orientar as alterações pertinentes no que se refere à conceção.
- Limitar o tratamento posterior – O responsável pelo tratamento não deve conectar conjuntos de dados ou realizar qualquer tratamento posterior para novas finalidades incompatíveis.
- Limitações de reutilização – O responsável pelo tratamento deve recorrer a medidas técnicas, incluindo o *hashing* e a cifragem, para limitar a possibilidade de reorientação dos dados pessoais. O responsável pelo tratamento deve igualmente dispor de medidas organizativas, como políticas e obrigações contratuais, que limitem a reutilização de dados pessoais.
- Exame – O responsável pelo tratamento deve examinar regularmente se o tratamento é necessário para as finalidades para as quais os dados foram recolhidos e testar a conceção em função da limitação das finalidades.

Exemplo

O responsável pelo tratamento trata dados pessoais dos seus clientes. A finalidade do tratamento é cumprir um contrato, isto é, conseguir entregar bens no endereço correto e obter o pagamento. Os dados pessoais armazenados são o histórico de compras, nome, endereço, endereço de correio eletrónico e número de telefone.

O responsável pelo tratamento está a ponderar a aquisição de um produto de gestão das relações com os clientes que reúne todos os dados dos clientes sobre as vendas, a comercialização e o serviço a clientes, num único local. O produto permite armazenar todas as chamadas telefónicas, atividades, documentos, mensagens de correio eletrónico e campanhas de comercialização para obter uma visão de 360 graus do cliente. Além disso, o produto de gestão das relações com os clientes é capaz de analisar automaticamente o poder de compra dos clientes recorrendo a informações públicas. O objetivo da análise consiste em direcionar melhor as atividades de publicidade. Essas atividades não fazem parte da finalidade lícita original do tratamento.

Para cumprir o princípio da limitação das finalidades, o responsável pelo tratamento exige ao fornecedor do produto que faça um levantamento das diferentes atividades de tratamento utilizando dados pessoais com as finalidades pertinentes para o responsável pelo tratamento.

Após receção dos resultados do levantamento, o responsável pelo tratamento avalia se o novo objetivo de comercialização e a finalidade publicitária visada são compatíveis com as finalidades originais definidas aquando da recolha dos dados e se a base jurídica é suficiente para o tratamento em causa. Se o resultado da avaliação não for positivo, o responsável pelo tratamento não deve continuar a utilizar as funcionalidades em causa. Em alternativa, o responsável pelo tratamento pode optar por renunciar à avaliação e simplesmente não utilizar as funcionalidades descritas do produto.

3.5 Minimização dos dados

73. Só devem ser tratados os dados pessoais adequados, pertinentes e limitados ao que é **necessário** para as finalidades[36]. Consequentemente, o responsável pelo tratamento tem de determinar previamente que características e parâmetros dos sistemas de tratamento e respetivas funções de apoio são admissíveis. A minimização dos dados concretiza e operacionaliza o princípio da necessidade. No tratamento posterior, o responsável pelo tratamento deve verificar periodicamente se os dados pessoais tratados continuam a ser adequados, pertinentes e necessários ou se os dados devem ser apagados ou anonimizados.

74. Em primeiro lugar, os responsáveis pelo tratamento devem determinar se é mesmo necessário tratar dados pessoais para as suas finalidades pertinentes. O responsável pelo tratamento deve verificar se as finalidades pertinentes podem ser alcançadas mediante o tratamento de menos dados pessoais, dispondo de menos dados pessoais agregados ou sem quaisquer dados pessoais.[37] Essa verificação deve ser efetuada antes de qualquer tratamento, embora também possa ser realizada a qualquer momento do ciclo de vida do tratamento. Tal está igualmente em conformidade com o artigo 11.º.

75. A minimização pode igualmente referir-se ao grau de identificação. Se a finalidade do tratamento não exigir que o conjunto final de dados se refira a uma pessoa identificada ou identificável (por exemplo, nas estatísticas), mas o tratamento inicial o exigir (por exemplo, antes da agregação de dados), o responsável pelo tratamento deve apagar ou anonimizar os dados pessoais assim que a identificação deixar de ser necessária. Por outro lado, se for necessária uma identificação contínua para outras atividades de tratamento, os dados pessoais devem ser pseudonimizados com vista a atenuar os riscos para os direitos dos titulares dos dados.

76. Os principais elementos de conceção e por defeito em matéria de minimização de dados podem incluir:
    - Evitar o tratamento de dados – Evitar o próprio tratamento de dados pessoais quando a finalidade em questão o permitir.
    - Limitação – Limitar a quantidade de dados pessoais recolhidos ao necessário para a finalidade a que se destinam.
    - Limitação de acesso – Organizar o tratamento de dados de forma que um número mínimo de pessoas necessite de aceder a dados pessoais para desempenhar as suas funções e limitar o acesso em conformidade.
    - Pertinência – Os dados pessoais devem ser pertinentes para o tratamento em questão e o responsável pelo tratamento deve ser capaz de demonstrar essa pertinência.
    - Necessidade – Cada categoria dos dados pessoais deve ser necessária para as finalidades especificadas e só deve ser tratada se não for possível alcançar a finalidade por outros meios.
    - Agregação – Utilização de dados agregados sempre que possível.
    - Pseudonimização – Pseudonimizar os dados pessoais assim que deixar de ser necessário ter dados pessoais diretamente identificáveis e armazenar as chaves de identificação separadamente.
    - Anonimização e apagamento – Se os dados pessoais não forem, ou deixarem de ser, necessários para a finalidade, devem ser anonimizados ou apagados.
    - Fluxo de dados – O fluxo de dados deve ser suficientemente eficiente para não criar mais cópias do que o necessário.

[36] Artigo 5.º, n.º 1, alínea c), do RGPD.
[37] O considerando 39 do RGPD diz o seguinte; «(...) Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios.»

- «Técnicas mais avançadas» – O responsável pelo tratamento deve aplicar tecnologias atuais e adequadas para evitar e minimizar os dados.

Exemplo 1

Uma livraria quer aumentar as suas receitas vendendo os seus livros em linha. O proprietário da livraria pretende criar um formulário normalizado para o processo de encomenda. Para assegurar que os clientes preenchem todas as informações necessárias, o proprietário da livraria torna obrigatório o preenchimento de todos os campos do formulário (se não preencher todos os campos, o cliente não consegue fazer a encomenda). O proprietário da loja virtual utiliza inicialmente um formulário de contacto normalizado, que solicita informações, incluindo a data de nascimento, o número de telefone e o endereço residencial do cliente. No entanto, nem todos os campos do formulário são necessários para a finalidade de aquisição e entrega dos livros. Neste caso específico, se o titular dos dados pagar antecipadamente o produto, a data de nascimento e o número de telefone do titular dos dados não são necessários para a compra do produto. Tal significa que estes campos não podem ser obrigatórios no formulário Web para encomendar o produto, a menos que o responsável pelo tratamento possa demonstrar claramente que é necessário para outro efeito, bem como o motivo por que os campos são necessários. Além disso, há situações em que um endereço não será necessário. Por exemplo, quando encomenda um livro eletrónico, o cliente pode descarregar o produto diretamente para o seu dispositivo.

Por conseguinte, o proprietário da loja virtual decide criar dois formulários Web: um para encomendar livros, com um campo para o endereço do cliente, e um formulário Web para encomendar livros eletrónicos, sem um campo para o endereço do cliente.

Exemplo 2

Uma empresa de transportes públicos pretende recolher informações estatísticas com base nos itinerários dos viajantes. Estas informações são úteis para fazer escolhas adequadas sobre alterações nos horários dos transportes públicos e rotas adequadas dos comboios. Os passageiros têm de passar os seus bilhetes num leitor sempre que entram ou saem de um meio de transporte. Tendo realizado uma avaliação dos riscos relacionada com os direitos e liberdades dos passageiros no que respeita à recolha dos seus itinerários, o responsável pelo tratamento conclui que é possível identificar passageiros que vivam ou trabalhem em zonas pouco povoadas com base apenas na identificação dos itinerários, graças ao identificador do bilhete. Por conseguinte, uma vez que o identificador do bilhete não é necessário para a finalidade de otimizar os horários dos transportes públicos e as rotas dos comboios, o responsável pelo tratamento não o armazena. Terminada a viagem, o responsável pelo tratamento armazena apenas os itinerários individuais, de modo a impedir a identificação de viagens ligadas a um bilhete único, conservando apenas informações sobre itinerários separados.

Nos casos em que ainda pode haver o risco de identificar uma pessoa apenas através do seu itinerário nos transportes públicos, o responsável pelo tratamento aplica medidas estatísticas para reduzir o riscos, nomeadamente o corte do início e do fim do itinerário.

Exemplo 3

Uma empresa de serviços postais pretende avaliar a eficácia das suas entregas em termos de prazos de entrega, programação da carga de trabalho e consumo de combustível. Para alcançar este objetivo, a empresa tem de tratar uma série de dados pessoais relativos aos funcionários (motoristas) e clientes (endereços, artigos a entregar, etc.). Esta operação de tratamento acarreta riscos, no que se refere quer à monitorização dos funcionários, que exige garantias jurídicas específicas, quer ao rastreio dos hábitos dos clientes através do conhecimento dos artigos entregues ao longo do tempo. Estes riscos podem ser significativamente reduzidos com a pseudonimização adequada de funcionários e clientes. Em particular, se as chaves de pseudonimização forem frequentemente alternadas e se se tiverem em consideração macrorregiões em vez de endereços pormenorizados, efetua-se uma minimização dos dados eficaz, e o responsável pelo tratamento pode concentrar-se apenas no processo de entrega e na finalidade da otimização de recursos, sem ultrapassar o limiar de monitorização dos comportamentos das pessoas (clientes ou funcionários).

Exemplo 4

Um hospital está a recolher dados sobre os seus doentes num sistema de informação hospitalar (registo eletrónico de saúde). A equipa do hospital necessita de aceder aos processos dos doentes para informar as suas decisões sobre os cuidados e o tratamento a prestar aos doentes e para documentar todas as medidas de diagnóstico, cuidados e tratamento tomadas. Por defeito, apenas têm acesso os membros da equipa médica designados para o tratamento do doente em causa no serviço de especialidade a que o doente foi afetado. O grupo de pessoas com acesso ao processo de um doente é mais vasto se outros serviços ou unidades de diagnóstico estiverem envolvidos no tratamento. Depois de o doente ter alta e de o processo de faturação ter sido concluído, o acesso é reduzido a um pequeno grupo de funcionários por serviço de especialidade que respondem a pedidos de informações médicas ou a consultas de outros prestadores de serviços médicos, mediante autorização do doente em causa.

3.6 Exatidão

77. Os dados pessoais devem ser exatos e atualizados, devendo ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora[38].

78. Os requisitos devem ser vistos em função dos riscos e das consequências da utilização concreta dos dados. A inexatidão dos dados pessoais pode constituir um risco para os direitos e liberdades dos titulares dos dados, por exemplo quando conduz a um diagnóstico deficiente ou a um tratamento incorreto de um protocolo de saúde, ou quando uma imagem incorreta de uma pessoa pode resultar em decisões tomadas numa base errada, quer manualmente, através da tomada de decisões automatizada, quer através da inteligência artificial.

79. Os principais elementos de conceção e por defeito em matéria de exatidão podem incluir:
    - Fonte de dados – As fontes de dados pessoais devem ser fiáveis em termos de exatidão dos dados.

[38] Artigo 5.º, n.º 1, alínea d), do RGPD.

- Grau de exatidão – Cada elemento dos dados pessoais deve ser tão exato quanto necessário para as finalidades especificadas.
- Mensuravelmente exato – Reduzir o número de falsos positivos/negativos, por exemplo, desequilíbrio em decisões automáticas e inteligência artificial.
- Verificação – Dependendo da natureza dos dados, em relação à frequência com que podem mudar, o responsável pelo tratamento deve verificar a exatidão dos dados pessoais junto do titular dos dados antes e em diferentes fases do tratamento (por exemplo, a idade).
- Apagamento/retificação – O responsável pelo tratamento deve apagar ou retificar sem demora os dados inexatos. Deve, em particular, facilitar esta ação quando os titulares dos dados forem ou fossem crianças e mais tarde desejem suprimir esses dados pessoais[39]
- Atenuação da propagação de erros – Os responsáveis pelo tratamento devem atenuar o efeito de um erro acumulado na cadeia de tratamento.
- Acesso – Deve ser facultada aos titulares dos dados informação e acesso efetivo aos dados pessoais, em conformidade com os artigos 12.º a 15.º do RGPD, para que possam controlar a sua exatidão e retificá-los conforme necessário.
- Exatidão contínua – Os dados pessoais devem ser exatos em todas as fases do tratamento, devendo ser realizados testes de exatidão em fases críticas.
- Atualização – Os dados pessoais devem ser atualizados se a finalidade assim o exigir.
- Conceção de dados – Utilização de características de conceção tecnológicas e organizativas para diminuir a inexatidão, por exemplo apresentar opções predeterminadas concisas em vez de campos de texto livre.

Exemplo 1

Uma companhia de seguros deseja usar inteligência artificial (IA) para traçar o perfil dos clientes que compram seguros, para servir de base à tomada de decisões aquando do cálculo do risco segurado. Ao determinar a forma como suas soluções de IA devem ser desenvolvidas, está a determinar os meios de tratamento e deve ter em consideração a proteção de dados desde a conceção ao escolher uma aplicação de IA de um fornecedor e ao decidir sobre a forma como irá treinar a IA.

Ao determinar a forma como irá treinar a IA, o responsável pelo tratamento deve ter dados exatos para obter resultados precisos. Por conseguinte, o responsável pelo tratamento deve garantir que os dados utilizados para treinar a IA são exatos.

Partindo do princípio de que o banco dispõe de uma base jurídica válida para treinar a IA recorrendo a dados pessoais de um grande subconjunto dos seus clientes, o responsável pelo tratamento escolhe um conjunto de clientes que seja representativo da população, também para evitar a parcialidade.

Os dados do cliente são então recolhidos do respetivo sistema de gestão de dados, incluindo dados sobre o tipo de seguro, por exemplo seguro de saúde, seguro de habitação, seguro de viagem, etc., bem como dados de registos públicos a que tem licitamente acesso. Todos os dados são pseudonimizados antes da transferência para o sistema dedicado ao treino do modelo de IA.

Para garantir que os dados utilizados para treinar a IA sejam o mais exatos possível, o responsável pelo tratamento só recolhe dados de fontes de dados com informações corretas e atualizadas.

A companhia de seguros testa se a IA é fiável e fornece resultados não discriminatórios tanto durante o seu desenvolvimento como, por último, antes do lançamento do produto. Quando a IA estiver totalmente treinada e operacional, a companhia de seguros utiliza os resultados para apoiar as

[39] Ver considerando 65.

avaliações do risco segurado, mas sem depender apenas da IA para decidir se contrata o seguro, salvo se a decisão for tomada de acordo com as exceções do artigo 22.º, n.º 2, do RGPD.

A companhia de seguros também analisará regularmente os resultados da IA, a fim de manter a sua fiabilidade e, quando necessário, ajustar o algoritmo.

Exemplo 2

O responsável pelo tratamento é uma instituição de saúde que procura encontrar métodos para garantir a integridade e exatidão dos dados pessoais nos seus registos de clientes.

Em situações em que duas pessoas chegam à instituição ao mesmo tempo e recebem o mesmo tratamento, existe o risco de as confundir se o único parâmetro para as distinguir for o seu nome. Para garantir a exatidão, o responsável pelo tratamento necessita de um identificador único para cada pessoa e, por conseguinte, de mais informações do que apenas o nome do cliente.

A instituição utiliza vários sistemas que contêm informações pessoais de clientes e necessita de assegurar que as informações relativas ao cliente são corretas, exatas e coerentes em todos os sistemas e em qualquer momento. A instituição identificou vários riscos que podem surgir se as informações forem alteradas num sistema, mas não nos outros.

O responsável pelo tratamento decide atenuar o risco utilizando uma técnica de «hashing» que pode ser utilizada para assegurar a integridade dos dados no diário de tratamento. São criados registos de hora criptográficos imutáveis para os registos do diário de tratamento e do cliente a eles associado para que quaisquer alterações possam ser reconhecidas, correlacionadas e rastreadas, se necessário.

3.7 Limitação da conservação

80. O responsável pelo tratamento tem de assegurar que os dados pessoais sejam conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados[40].
É vital que o responsável pelo tratamento saiba exatamente que dados pessoais são tratados pela empresa e por que motivo. A finalidade do tratamento deve ser o principal critério para decidir do período de conservação dos dados pessoais.

81. As medidas e garantias que aplicam o princípio da limitação da conservação complementam os direitos e liberdades dos titulares dos dados, especificamente o direito ao apagamento e o direito de oposição.

82. Os principais elementos de conceção e por defeito em matéria de limitação da conservação podem incluir:
- Apagamento e anonimização – O responsável pelo tratamento deve ter procedimentos internos claros e funcionalidades para apagamento e/ou anonimização.
- Eficácia da anonimização/apagamento – O responsável pelo tratamento deve certificar-se de que não é possível reidentificar dados anonimizados ou recuperar dados apagados, devendo testar se tal é possível.
- Automação – O apagamento de determinados dados pessoais deve ser automatizado.

[40] Artigo 5.º, n.º 1, alínea c), do RGPD.

- Critérios de conservação – O responsável pelo tratamento deve determinar que dados e prazo de conservação são necessários para a finalidade.
- Justificação – O responsável pelo tratamento deve poder justificar por que razão o período de conservação é necessário para a finalidade e os dados pessoais em questão e divulgar a lógica subjacente e os fundamentos jurídicos para o período de conservação.
- Execução de políticas de conservação – O responsável pelo tratamento deve executar políticas de conservação internas e realizar testes que lhe permitam saber se a organização pratica as suas políticas.
- Cópias de segurança/registos – Os responsáveis pelo tratamento devem determinar que dados pessoais e prazo de conservação são necessários para efeitos das cópias de segurança e dos registos.
- Fluxo de dados – Os responsáveis pelo tratamento devem estar atentos ao fluxo de dados pessoais e à conservação de quaisquer cópias dos mesmos e procurar limitar a sua conservação «temporária».

Exemplo

O responsável pelo tratamento recolhe dados pessoais sendo a finalidade do tratamento gerir a filiação do titular dos dados. Os dados pessoais devem ser apagados quando a filiação terminar e não houver qualquer base jurídica para a conservação dos dados.

O responsável pelo tratamento estabelece previamente um procedimento interno para a conservação e o apagamento dos dados. De acordo com este procedimento, os funcionários devem apagar manualmente os dados pessoais após o termo do prazo de conservação. O funcionário segue o procedimento para apagar e corrigir regularmente os dados de quaisquer dispositivos, cópias de segurança, registos, mensagens de correio eletrónico e outros suportes de conservação pertinentes.

Para tornar o apagamento mais eficaz e menos propenso a erros, o responsável pelo tratamento implementa um sistema automático para apagar dados de forma automática, fiável e mais regular. O sistema está configurado para seguir o procedimento indicado para o apagamento dos dados, que ocorre num intervalo regular predefinido para remover dados pessoais de todos os suportes de conservação da empresa. O responsável pelo tratamento revê e ensaia o procedimento de conservação regularmente e garante que este está conforme à política de retenção atualizada.

3.8 Integridade e confidencialidade

83. O princípio da integridade e da confidencialidade inclui a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas. A segurança dos dados pessoais requer medidas adequadas destinadas a prevenir e a gerir incidentes de violação de dados, a garantir a execução adequada das tarefas de tratamento de dados e o respeito dos outros princípios e a facilitar o exercício efetivo dos direitos individuais.

84. O considerando 78 estabelece que uma das medidas da PDdCD poderia consistir na possibilidade de o responsável pelo tratamento *«criar e melhorar medidas de segurança»*. Juntamente com outras medidas da PDdCD, o considerando 78 sugere que se imponha aos responsáveis pelo tratamento de dados a responsabilidade de avaliar continuamente se utilizam sempre os meios de tratamento adequados e se as medidas escolhidas combatem, efetivamente, as vulnerabilidades existentes. Além disso, os responsáveis pelo tratamento devem proceder a revisões periódicas das medidas de

segurança da informação que enquadram e protegem os dados pessoais e do procedimento de tratamento das violações de dados.

85. Os principais elementos de conceção e por defeito em matéria de integridade e confidencialidade podem incluir:
    - Sistema de gestão da segurança da informação (SGSI) – Dispor de um meio operacional de gestão das políticas e dos procedimentos de segurança da informação.
    - Análise de risco – Avaliar os riscos em relação à segurança dos dados pessoais, tendo em conta o impacto nos direitos individuais, e combater os riscos identificados. Para utilizar na avaliação dos riscos; desenvolver e manter uma «modelização de ameaças» abrangente, sistemática e realista e uma análise da superfície de ataque do *software* concebido para reduzir vetores de ataque e oportunidades de explorar pontos fracos e vulnerabilidades.
    - Segurança desde a conceção – Ter em conta os requisitos de segurança o mais cedo possível na conceção e no desenvolvimento do sistema e integrar e executar continuamente ensaios pertinentes.
    - Manutenção – Revisão regular e ensaio de *software*, *hardware*, sistemas e serviços, etc., para detetar vulnerabilidades dos sistemas que suportam o tratamento.
    - Gestão do controlo do acesso – Apenas o pessoal autorizado que necessite de ter acesso aos dados pessoais necessários para as suas tarefas de tratamento, devendo o responsável pelo tratamento estabelecer uma distinção entre privilégios de acesso do pessoal autorizado.
        - Limitação de acesso (agentes) – Organizar o tratamento de dados de forma que um número mínimo de pessoas necessite de aceder a dados pessoais para desempenhar as suas funções e limitar o acesso em conformidade.
        - Limitação de acesso (conteúdos) – No contexto de cada operação de tratamento, limitar o acesso aos atributos por conjunto de dados necessários para executar essa operação. Além disso, limitar o acesso aos dados pertencentes aos titulares de dados que são da competência do funcionário correspondente.
        - Segregação de acesso – Organizar o tratamento de dados de forma que nenhum indivíduo tenha necessidade de ter acesso a todos os dados recolhidos sobre um titular de dados, menos ainda a todos os dados pessoais de uma determinada categoria de titulares de dados.
    - Transferências seguras – As transferências devem ser protegidas contra o acesso e alterações não autorizados e acidentais.
    - Conservação segura – A conservação de dados deve ser protegida contra o acesso não autorizado e alterações. Deve haver procedimentos para avaliar o risco da conservação centralizada ou descentralizada e as categorias de dados pessoais a que tal se aplica. Alguns dados podem necessitar de mais medidas de segurança do que outros ou de ser isolados dos outros.
    - Pseudonimização – Os dados pessoais e as cópias de segurança/registos devem ser pseudonimizados como medida de segurança para minimizar os riscos de eventuais violações de dados, por exemplo, recorrendo ao «hashing» ou à cifragem.
    - Cópias de segurança/registos – Manter cópias de segurança e registos na medida do necessário para a segurança da informação, recorrer a pistas de auditoria e à monitorização de acontecimentos como um controlo de segurança de rotina. Estes devem ser protegidos contra acesso e alteração não autorizados e acidentais e revistos regularmente, devendo os incidentes ser abordados de imediato.

- Recuperação em caso de catástrofes/continuidade da atividade – Abordar os requisitos de recuperação do sistema de informações em caso de catástrofes e continuidade da atividade para restaurar a disponibilidade de dados pessoais após incidentes graves.
- Proteção de acordo com o risco – Todas as categorias de dados pessoais devem ser protegidas com medidas adequadas no que diz respeito ao risco de violação da segurança. Os dados que apresentem riscos especiais devem, sempre que possível, ser mantidos separados dos restantes dados pessoais.
- Gestão de resposta a incidentes de segurança – Dispor de rotinas, procedimentos e recursos para detetar, conter, tratar e comunicar violações de dados e aprender com as mesmas.
- Gestão de incidentes – O responsável pelo tratamento deve dispor de processos para lidar com violações e incidentes, a fim de tornar o sistema de tratamento mais robusto. Tal inclui procedimentos de notificação, como a gestão da notificação (à autoridade de controlo) e da informação (aos titulares dos dados).

Exemplo

Um responsável pelo tratamento pretende extrair grandes quantidades de dados pessoais de uma base de dados médica que contém registos de saúde eletrónicos (dos doentes) para um servidor de base de dados específico da empresa, a fim de tratar os dados extraídos para efeitos de garantia da qualidade. A empresa avaliou o risco de encaminhar os extratos para um servidor acessível a todos os funcionários da empresa como suscetível de ser elevado para os direitos e liberdades dos titulares dos dados. Como há apenas um departamento na empresa que necessita de tratar os extratos de dados dos doentes, o responsável pelo tratamento decide limitar o acesso ao servidor específico aos funcionários desse departamento. Além disso, para reduzir ainda mais o risco, os dados serão pseudonimizados antes de serem transferidos.

Para regulamentar o acesso e mitigar eventuais danos causados por programas maliciosos, a empresa decide segregar a rede e estabelecer controlos de acesso ao servidor. Além disso, instala um sistema de acompanhamento da segurança e de deteção e prevenção de intrusões, que isola da utilização regular. É criado um sistema de auditoria automatizado para monitorizar o acesso e as alterações. O referido sistema gera relatórios e alertas automáticos quando determinados acontecimentos relacionados com a utilização são configurados. O responsável pelo tratamento garantirá que os utilizadores apenas tenham acesso com base na necessidade de tomar conhecimento e com o nível de acesso adequado. A utilização inadequada pode ser rápida e facilmente detetada.

Alguns dos extratos têm de ser comparados com novos extratos, pelo que têm de ser conservados durante três meses. O responsável pelo tratamento decide colocá-los em bases de dados separadas no mesmo servidor e usar encriptação transparente e de nível de coluna para os armazenar. As chaves para decifração de dados de coluna são armazenadas em módulos de segurança específicos que apenas podem ser utilizados por pessoal autorizado, mas não podem ser extraídas.

Estar preparados para eventuais incidentes torna o sistema mais robusto e fiável. O responsável pelo tratamento de dados compreende que devem ser incorporadas garantias e medidas preventivas e eficazes em todas as operações de tratamento de dados pessoais, atualmente e no futuro, e que tal pode ajudar a prevenir futuros incidentes de violação de dados.

O responsável pelo tratamento cria estas medidas de segurança tanto para assegurar a exatidão, a integridade e a confidencialidade como para impedir a propagação de programas maliciosos por ciberataques e tornar a solução sólida. Ter medidas de segurança sólidas contribui para criar confiança nos titulares dos dados.

3.9 Responsabilidade[41]

86. De acordo com o princípio da responsabilidade, o responsável pelo tratamento é responsável pelo respeito de todos os princípios supramencionados e tem de poder comprová-lo.

87. O responsável pelo tratamento tem de poder comprovar o respeito dos princípios. Ao fazê-lo, o responsável pelo tratamento pode demonstrar os efeitos das medidas adotadas para proteger os direitos dos titulares dos dados e as razões pelas quais essas medidas são consideradas adequadas e eficazes. Por exemplo, demonstrar por que razão uma medida é adequada para garantir com eficácia o princípio da limitação da conservação.

88. Para poder tratar os dados pessoais de forma responsável, o responsável pelo tratamento deve possuir os conhecimentos e a capacidade necessários para aplicar a proteção de dados. Tal implica que o responsável pelo tratamento compreenda as obrigações de proteção de dados que para si decorrem do RGPD e possa cumprir essas obrigações.

4 ARTIGO 25.º, N.º 3, CERTIFICAÇÃO

89. Em conformidade com o artigo 25.º, n.º 3, a certificação nos termos do artigo 42.º pode ser utilizada como elemento para demonstrar o cumprimento da PDdCD. Por outro lado, os documentos que demonstram a conformidade com a PDdCD também podem ser úteis num processo de certificação. Tal significa que, quando é concedida uma certificação em conformidade com o artigo 42.º a uma operação de tratamento de um responsável pelo tratamento ou de um subcontratante, as autoridades de controlo devem ter este facto em conta na sua avaliação do cumprimento do RGPD, especificamente no que diz respeito à PDdCD.

90. Quando uma operação de tratamento por um responsável pelo tratamento ou subcontratante é certificada em conformidade com o artigo 42.º, os elementos que contribuem para demonstrar a conformidade com o artigo 25.º, n.^{os} 1 e 2, são os processos de conceção, ou seja, o processo de determinação dos meios de tratamento, a governação e as medidas técnicas e organizativas para aplicar os princípios de proteção de dados. Os critérios de certificação da proteção de dados são determinados pelos organismos de certificação ou pelos proprietários de sistemas de certificação e, em seguida, aprovados pela autoridade de controlo competente ou pelo CEPD. Para mais informações sobre os mecanismos de certificação, remetemos para as orientações do CEPD sobre certificação[42] e para outras orientações pertinentes, conforme publicadas no sítio Web do CEPD.

91. Mesmo quando uma operação de tratamento obtém uma certificação nos termos do artigo 42.º, o responsável pelo tratamento continua a ter a responsabilidade de acompanhar e melhorar em permanência o cumprimento dos critérios de PDdCD do artigo 25.º.

[41] Ver o considerando 74, em que os responsáveis pelo tratamento têm de comprovar a eficácia das suas medidas.
[42] CEPD, «Orientações 1/2018 sobre a certificação e a seleção de critérios de certificação em conformidade com os artigos 42.º e 43.º do Regulamento (UE) 2016/679», versão 3.0, 4 de junho de 2019, edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf .

5 APLICAÇÃO DO ARTIGO 25.º E CONSEQUÊNCIAS

92. As autoridades de controlo podem avaliar o cumprimento do artigo 25.º em conformidade com os procedimentos enumerados no artigo 58.º. Os poderes de correção encontram-se especificados no artigo 58.º, n.º 2, e incluem fazer advertências e repreensões, ordenar que se respeitem os direitos dos titulares dos dados, impor limitações ao tratamento, ou mesmo a sua proibição, aplicar coimas, etc.

93. A PDdCD é também um fator a ter em conta na determinação do nível das sanções monetárias em caso de violação do RGPD – ver artigo 83.º, n.º 4[43] [44].

6 RECOMENDAÇÕES

94. Embora não sejam abordados diretamente no artigo 25.º, os subcontratantes e os fabricantes também são reconhecidos como elementos essenciais da PDdCD, pelo que devem estar cientes de que os responsáveis pelo tratamento são obrigados a tratar dados pessoais apenas com sistemas e tecnologias com proteção de dados integrada.

95. Aquando do tratamento em nome dos responsáveis pelo tratamento ou do fornecimento de soluções aos responsáveis pelo tratamento, os subcontratantes e os fabricantes devem utilizar os seus conhecimentos especializados para criar confiança e orientar os seus clientes na conceção/aquisição de soluções que integrem a proteção de dados no tratamento. Tal significa que a conceção de produtos e serviços deve ir ao encontro das necessidades dos responsáveis pelo tratamento.

96. Ao aplicar o artigo 25.º, deve ter-se presente que o principal objetivo em termos de conceção é a *aplicação eficaz* dos princípios e a *proteção* dos direitos dos titulares dos dados nas medidas adequadas do tratamento. Para facilitar e melhorar a adoção da PDdCD, formulamos as seguintes recomendações aos responsáveis pelo tratamento, bem como aos fabricantes e subcontratantes:
    - Os responsáveis pelo tratamento devem pensar na proteção de dados desde as *fases iniciais* de planeamento de uma operação de tratamento, inclusivamente antes do momento da definição dos meios de tratamento.
    - Caso o responsável pelo tratamento tenha um responsável pela proteção de dados (RPD), o CEPD incentiva a participação ativa do RPD na integração da PDdCD nos procedimentos de contratação e de desenvolvimento, bem como em todo o ciclo de vida do tratamento.
    - Uma operação de tratamento pode ser *certificada*. A possibilidade de obter a certificação de uma operação de tratamento confere valor acrescentado a um responsável pelo tratamento aquando da escolha entre diferentes sistemas de *software* e *hardware*, serviços e/ou sistemas de tratamento de fabricantes ou subcontratantes. Por conseguinte, os fabricantes devem esforçar-se por demonstrar a PDdCD durante o ciclo de vida do desenvolvimento de uma solução de tratamento. Um selo de certificação pode também orientar os titulares dos dados na escolha entre diferentes bens e serviços. Ter condições para conseguir a certificação de um

[43] O artigo 83.º, n.º 2, alínea d), do RGPD estipula que, ao determinar a aplicação de coimas por violação do RGPD, *é tido em «devida consideração» «[o] grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º»*.

[44] Para mais informações sobre coimas, consultar o documento do Grupo de Trabalho do Artigo 29.º intitulado «Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento 2016/679», WP 253, 3 de outubro de 2017, ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 – subscritas pelo CEPD.

tratamento pode constituir uma vantagem competitiva para fabricantes, subcontratantes e responsáveis pelo tratamento e aumenta a confiança dos titulares dos dados no tratamento dos seus dados pessoais. Se não for oferecida uma certificação, os responsáveis pelo tratamento devem procurar obter outras *garantias* de que os fabricantes ou contratantes cumprem os requisitos da PDdCD.

- Os responsáveis pelo tratamento, subcontratantes e fornecedores devem ter em conta as suas fabricantes de assegurar às crianças menores de 18 anos e a outros grupos vulneráveis proteção específica em matéria de PDdCD.
- Os fabricantes e subcontratantes devem procurar facilitar a aplicação da PDdCD, a fim de apoiar a capacidade do responsável pelo tratamento para cumprir as obrigações do artigo 25.º. Os responsáveis pelo tratamento, por outro lado, não devem escolher fabricantes ou subcontratantes que não proponham sistemas que permitam ao responsável pelo tratamento cumprir o disposto no artigo 25.º, uma vez que os responsáveis pelo tratamento serão responsabilizados pela não aplicação do disposto no referido artigo.
- Os fabricantes e os subcontratantes devem trabalhar ativamente para garantir o cumprimento dos critérios das «técnicas mais avançadas» e notificar os responsáveis pelo tratamento de quaisquer alterações das «técnicas mais avançadas» que possam afetar a eficácia das medidas por si postas em prática. Os responsáveis pelo tratamento devem incluir este requisito como uma cláusula contratual para garantir a sua atualização.
- O CEPD recomenda que os responsáveis pelo tratamento exijam que os fabricantes e os subcontratantes demonstrem de que forma o seu *hardware*, *software*, serviços ou sistemas permitem que o responsável pelo tratamento cumpra os requisitos de responsabilidade em conformidade com a PDdCD, por exemplo com recurso a indicadores-chave de desempenho para demonstrar a eficácia das medidas e garantias na aplicação dos princípios e direitos.
- O CEPD enfatiza a necessidade de uma abordagem harmonizada para aplicar os princípios e os direitos de forma eficaz e incentiva as associações ou organismos que elaboram códigos de conduta em conformidade com o artigo 40.º a incorporarem igualmente orientações setoriais na PDdCD.
- Os responsáveis pelo tratamento devem ser justos para com os titulares dos dados e transparentes sobre a forma como avaliam e demonstram a aplicação eficaz da PDdCD, da mesma forma que os responsáveis pelo tratamento demonstram o cumprimento do RGPD ao abrigo do princípio da responsabilidade.
- As tecnologias de proteção da privacidade que tenham atingido a maturidade podem ser utilizadas como medida, em conformidade com os requisitos da PDdCD, se for caso disso, numa abordagem baseada no risco. Por si só, estas tecnologias não abrangem necessariamente as obrigações previstas no artigo 25.º. Os responsáveis pelo tratamento devem verificar se a medida é adequada e eficaz na aplicação dos princípios de proteção de dados e dos direitos dos titulares de dados.
- Os sistemas herdados estão sujeitos às mesmas obrigações de PDdCD que os novos sistemas. Se os sistemas herdados ainda não estiverem em conformidade com a PDdCD e não puderem ser feitas alterações para os conformar, o sistema herdado simplesmente não cumpre as obrigações do RGPD e não pode ser usado para tratar dados pessoais.
- O artigo 25.º não diminui os requisitos para as PME. Os seguintes pontos podem facilitar a observância do artigo 25.º pelas PME:
    - Avaliação precoce dos riscos

- Começar com tratamentos de pequena dimensão – aumentar posteriormente o âmbito e a sofisticação
- Procurar obter garantias dos fabricantes e dos subcontratantes em matéria de PDdCD, como certificação e adesão a códigos de conduta
- Utilizar parceiros com um bom historial
- Falar com as autoridades de proteção de dados (APD)
- Ler as orientações das APD e do CEPD
- Aderir a códigos de conduta, caso existam
- Obter ajuda e aconselhamento profissional

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)