GRUPO DE TRABALHO DO ARTIGO 29.º
PARA A PROTEÇÃO DE DADOS

17/PT
WP259 rev.01

Grupo de Trabalho do Artigo 29.º
Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679

Adotadas em 28 de novembro de 2017
Última redação revista e adotada em 10 de abril de 2018

O GRUPO DE PROTEÇÃO DAS PESSOAS NO QUE DIZ RESPEITO AO

TRATAMENTO DE DADOS PESSOAIS

Criado pela Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995,

Tendo em conta os artigos 29.º e 30.º dessa diretiva,

Tendo em conta o seu regulamento interno,

ADOTOU AS PRESENTES ORIENTAÇÕES:

Este grupo de trabalho foi instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE. Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

Os serviços de secretariado são prestados pela Direção C (Direitos Fundamentais e Cidadania da União) da Comissão Europeia, Direção-Geral de Justiça, B-1049 Bruxelas, Bélgica, Gabinete n.º MO-59 02/013.

Sítio: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=6936

Índice

1. Introdução 3
2. Consentimento na aceção do artigo 4.º, n.º 11, do RGPD 4
3. Elementos do consentimento válido 5
3.1. Livre 5
3.1.1. Desequilíbrio de poder 6
3.1.2. Condicionalidade 8
3.1.3. Granularidade 11
3.1.4. Prejuízos 11
3.2. Específica 12
3.3. Informada 14
3.3.1. Requisitos mínimos de conteúdo para um consentimento «informado» 14
3.3.2. Como fornecer informações 15
3.4. Manifestação de vontade inequívoca 17
4. Obter consentimento explícito 20
5. Outras condições para a obtenção de consentimento válido 22
5.1. Demonstrar o consentimento 23
5.2. Retirada do consentimento 24
6. Interação entre o consentimento e outros fundamentos de licitude no artigo 6.º do RGPD 26
7. Preocupações específicas no RGPD 27
7.1. Crianças (artigo 8.º) 27
7.1.1. Serviços da sociedade da informação 28
7.1.2. Oferecidos diretamente a uma criança 28
7.1.3. Idade 28
7.1.4. Consentimento dado por crianças e responsabilidade parental 29
7.2. Investigação científica 31
7.3. Direitos dos titulares dos dados 34
8. Consentimento obtido nos termos da Diretiva 95/46/CE 34

1. Introdução

As presentes orientações fornecem uma análise exaustiva do conceito de consentimento previsto no Regulamento (UE) 2016/679, o Regulamento Geral sobre a Proteção de Dados (doravante: RGPD). O conceito de consentimento utilizado até à data na Diretiva Proteção de Dados (doravante: Diretiva 95/46/CE) e na Diretiva Privacidade Eletrónica evoluiu. O RGPD clarifica e especifica mais pormenorizadamente os requisitos necessários para obter e comprovar o consentimento válido. As presentes orientações incidem nestas alterações, fornecendo conselhos práticos para assegurar o cumprimento do RGPD e tendo por base o Parecer 15/2011 sobre o consentimento. O dever de inovar recai sobre os responsáveis pelo tratamento, devendo estes encontrar novas soluções que se enquadrem nos parâmetros da lei e promovam melhor a proteção dos dados pessoais e os interesses dos titulares dos dados.

O consentimento continua a ser um dos seis fundamentos legais para tratar dados pessoais, tal como previsto no artigo 6.º do RGPD[1]. Quando iniciam atividades que envolvam o tratamento de dados pessoais, os responsáveis pelo tratamento devem sempre dedicar algum tempo a ponderar qual o fundamento legal adequado para o tratamento previsto.

Geralmente, o consentimento só pode constituir fundamento legal adequado se, ao titular dos dados, for oferecido controlo e uma verdadeira opção de aceitar ou recusar os termos propostos ou recusá-los sem ser prejudicado. Ao solicitar o consentimento, os responsáveis pelo tratamento têm o dever de avaliar se irão cumprir todos os requisitos para obter um consentimento válido. Caso seja obtido em conformidade com o RGPD, o consentimento é um instrumento que permite aos titulares dos dados controlarem se os dados pessoais que lhes dizem respeito vão ou não ser tratados. Caso não o seja, o controlo do titular dos dados torna-se ilusório e o consentimento será um fundamento inválido para o tratamento, tornando essa atividade de tratamento ilícita[2].

Os pareceres emitidos pelo Grupo de Trabalho do Artigo 29.º (GT29) sobre o consentimento[3] continuam a ser pertinentes, quando coerentes com o novo quadro jurídico, uma vez que o RGPD codifica as orientações existentes do GT29 e as boas práticas em geral e que os principais elementos do consentimento continuam os mesmos ao abrigo do RGPD. Por conseguinte, no presente documento, o GT29 desenvolve e completa os pareceres emitidos anteriormente sobre tópicos específicos que fazem referência ao consentimento nos termos da Diretiva 95/46/CE, em vez de os substituir.

Como consta do Parecer 15/2011 sobre a definição de consentimento, o ato de convidar alguém a aceitar uma operação de tratamento de dados deve estar sujeito a requisitos rigorosos, uma vez que diz respeito aos direitos fundamentais dos titulares dos dados e o responsável pelo tratamento

[1] O artigo 9.º do RGPD prevê uma lista de possíveis isenções à proibição do tratamento de categorias especiais de dados. Uma das isenções prevista é a situação em que o titular dos dados dá o seu consentimento explícito para a utilização destes dados.

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

[3] Mais especificamente, o Parecer 15/2011 sobre a definição de consentimento (WP 187).

pretende efetuar uma operação de tratamento que não seria lícita sem o consentimento do titular dos dados[4]. O papel crucial do consentimento é realçado nos artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia. Além disso, obter o consentimento também não nega nem diminui de forma alguma as obrigações do responsável pelo tratamento no que toca a observar os princípios relativos ao tratamento consagrados no RGPD, em especial no artigo 5.º do RGPD, no que diz respeito à lealdade, à necessidade e proporcionalidade, bem como à qualidade dos dados. Mesmo que o tratamento dos dados pessoais se baseie no consentimento do titular dos dados, o facto de existir consentimento não legitima a recolha de dados que não seja necessária para a finalidade específica do tratamento e que seja fundamentalmente desleal[5].

Enquanto isso, o GT29 está ciente da revisão da Diretiva Privacidade Eletrónica (2002/58/CE). O conceito de consentimento no projeto de Regulamento Privacidade Eletrónica continua ligado ao conceito de consentimento do RGPD[6]. As organizações são poderão necessitar de consentimento ao abrigo do instrumento sobre privacidade eletrónica para a maioria das mensagens em linha ou chamadas telefónicas de comercialização, bem como métodos de rastreio em linha, nomeadamente para a utilização de *cookies* ou aplicações ou outros programas informáticos. O GT29 já emitiu recomendações e orientações destinadas ao legislador europeu sobre a proposta de regulamento relativo à privacidade eletrónica[7].

No que diz respeito à atual Diretiva Privacidade Eletrónica, o GT29 observa que as remissões para a Diretiva 95/46/CE revogada devem ser interpretadas como remissões para o RGPD[8]. O mesmo se aplica às referências ao consentimento que constam da atual Diretiva 2002/58/CE, uma vez que o Regulamento Privacidade Eletrónica (ainda) não estará em vigor em 25 de maio de 2018. De acordo com o artigo 95.º do RGPD, não serão impostos mais deveres no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações, na medida em que a Diretiva Privacidade Eletrónica imponha deveres com o mesmo objetivo. O GT29 refere que os requisitos relativos ao consentimento nos termos do RGPD não são considerados um «dever suplementar», são antes condições prévias para o tratamento lícito. Por conseguinte, as condições previstas no RGPD para a obtenção de consentimento válido são aplicáveis às situações abrangidas pelo âmbito de aplicação da Diretiva Privacidade Eletrónica.

2. Consentimento na aceção do artigo 4.º, n.º 11, do RGPD

O artigo 4.º, n.º 11, do RGPD define consentimento como: *«uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento».*

[4] Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 8.
[5] Ver também Parecer 15/2011 sobre a definição de consentimento (WP 187) e o artigo 5.º do RGPD.
[6] De acordo com o artigo 9.º da proposta de regulamento sobre privacidade eletrónica, aplicam-se a definição de consentimento e as condições aplicáveis ao consentimento previstas no artigo 4.º, n.º 11, e no artigo 7.º do RGPD.
[7] Ver Parecer 03/2016 sobre a avaliação e revisão da Diretiva Privacidade Eletrónica (WP 240).
[8] Ver artigo 94.º do RGPD.

O conceito básico de consentimento permanece idêntico ao da Diretiva 95/46/CE, sendo o consentimento um dos fundamentos legais em que o tratamento de dados pessoais tem de se basear, nos termos do artigo 6.º do RGPD[9]. Além da definição alterada que consta do artigo 4.º, n.º 11, o RGPD fornece orientações suplementares no artigo 7.º e nos considerandos 32, 33, 42 e 43 sobre a forma como o responsável pelo tratamento deve atuar para cumprir os principais elementos do requisito do consentimento.

Por último, a inclusão de disposições e considerandos específicos sobre a retirada do consentimento confirma que o consentimento deve ser uma decisão reversível e que, do lado do titular dos dados, continua a existir algum grau de controlo.

3. Elementos do consentimento válido

O artigo 4.º, n.º 11, do RGPD estabelece que o consentimento do titular dos dados significa uma manifestação de vontade

- livre,
- específica,
- informada e
- explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

Nas secções seguintes, analisa-se em que medida é que a redação do artigo 4.º, n.º 11, exige que os responsáveis pelo tratamento alterem os seus pedidos/formulários de consentimento, por forma a assegurarem o cumprimento do RGPD[10].

3.1. Livre[11]

[9] Na Diretiva 95/46/CE, o consentimento foi definido como «*qualquer manifestação de vontade, livre, específica e informada, pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento*», devendo esse consentimento ser «*dado de forma inequívoca*» para que o tratamento dos dados pessoais seja legítimo [artigo 7.º, alínea a), da Diretiva 95/46/CE]. Ver Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187) para consultar exemplos sobre a adequação do consentimento como fundamento legal. No referido parecer, o GT29 forneceu orientações que ajudam a distinguir os casos em que o consentimento constitui fundamento adequado dos casos em que é suficiente apoiar-se num fundamento de interesse legítimo (possivelmente com oportunidade para o retirar) ou em que se recomenda uma relação contratual. Ver também Parecer 06/2014 do GT29, ponto III.1.2, p. 14 e seguintes. O consentimento explícito também constitui uma das isenções da proibição do tratamento de categorias especiais de dados: ver artigo 9.º do RGPD.

[10] Para mais orientações sobre atividades de tratamento que já se encontrem em curso com base no consentimento dado nos termos da Diretiva 95/46/CE, consultar o capítulo 7 do presente documento e o considerando 171 do RGPD.

[11] Em vários pareceres, o Grupo de Trabalho do Artigo 29.º explorou os limites do consentimento em situações onde este não pode ser dado de livre vontade. Trata-se designadamente do Parecer 15/2011 sobre a definição de consentimento (WP 187), do documento de trabalho sobre o tratamento de dados pessoais ligados à saúde em registos de saúde eletrónicos (WP 131), do Parecer 8/2001 sobre o tratamento de dados pessoais no âmbito do emprego (WP 48) e do Segundo parecer 4/2009 sobre a Norma Internacional relativa à proteção da privacidade e dos dados pessoais da Agência Mundial Antidopagem (AMA), sobre as disposições pertinentes do Código AMA e sobre outros aspetos relacionados com a privacidade no contexto da luta contra a dopagem no desporto por parte da AMA e de outras organizações antidopagem (nacionais) (WP 162).

O elemento «livre» implica uma verdadeira escolha e controlo para os titulares dos dados. Regra geral, o RGPD prevê que se o titular dos dados não puder exercer uma verdadeira escolha, se sentir coagido a dar o consentimento ou sofrer consequências negativas caso não consinta, então o consentimento não é válido[12]. Se o consentimento estiver agregado a uma parte não negociável das condições gerais do contrato, presume-se que não foi dado livremente. Assim sendo, não se considera que o consentimento foi dado de livre vontade se o titular dos dados não o puder recusar nem o puder retirar sem ficar prejudicado[13]. A noção de desequilíbrio entre o responsável pelo tratamento e o titular dos dados também é tida em consideração no RGPD.

Ao avaliar se o consentimento é dado livremente, importa ter em conta a situação específica em que o consentimento está subordinado à execução de um contrato ou à prestação de um serviço, tal como descrito no artigo 7.º, n.º 4. O artigo 7.º, n.º 4, foi redigido de forma não exaustiva com palavras como «designadamente», significando que pode haver uma variedade de outras situações que se enquadram nesta disposição. Em termos gerais, qualquer elemento que constitua pressão ou influência desadequada sobre o titular dos dados (que se pode manifestar de formas muito diversas) e que o impeça de exercer livremente a sua vontade tornará o consentimento inválido.

> [Exemplo 1]
> Uma aplicação para telemóvel de edição de fotografias solicita aos utilizadores que ativem a localização por GPS para fins de prestação dos serviços. A aplicação também os informa de que utilizará os dados recolhidos para efeitos de publicidade comportamental. Nem a geolocalização nem a publicidade comportamental em linha são necessárias para a prestação do serviço de edição de fotografias, indo além da concretização do serviço principal prestado. Uma vez que os utilizadores não podem utilizar a aplicação sem darem o seu consentimento para estes efeitos, o consentimento não pode ser considerado livre.

3.1.1. Desequilíbrio de poder

O considerando 43[14] indica claramente que é improvável que as **autoridades públicas** possam utilizar o consentimento para o tratamento quando o responsável pelo tratamento for uma autoridade pública, uma vez que existe frequentemente um desequilíbrio de poder na relação entre o responsável pelo tratamento e o titular dos dados. Na maioria dos casos, também é evidente que o titular dos dados não tem alternativas realistas a aceitar (as condições de) o tratamento realizado pelo seu responsável pelo tratamento. O GT29 considera que existem outros fundamentos legais em princípio mais adequados à atividade das autoridades públicas[15].

Sem prejuízo destas considerações gerais, a utilização do consentimento como fundamento legal para o tratamento dos dados pelas autoridades públicas não se encontra totalmente excluída do

[12] Ver Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 12.
[13] Ver considerandos 42 e 43 do RGPD e Parecer 15/2011 do GT29 sobre a definição de consentimento, adotado em 13 de julho de 2011 (WP 187), p. 12.
[14] O considerando 43 do RGPD determina: *«A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. […]»*
[15] Ver artigo 6.º do RGPD, designadamente o n.º 1, alíneas c) e e).

quadro jurídico do RGPD. Os exemplos apresentados a seguir mostram que a utilização do consentimento pode ser adequada em determinadas circunstâncias.

> [Exemplo 2] Um município local está a planear realizar obras de manutenção rodoviária. Uma vez que essas obras podem perturbar o trânsito durante muito tempo, o município oferece aos cidadãos a oportunidade de se registarem numa lista de correio eletrónico para receberem atualizações sobre a evolução das obras e os atrasos previstos. O município deixa bem claro que não existe obrigação de participar e solicita o consentimento para utilizar os endereços de correio eletrónico (exclusivamente) para este efeito. Os cidadãos que não derem o seu consentimento não deixarão de beneficiar de qualquer serviço essencial do município nem deixarão de exercer qualquer direito, pelo que poderão dar ou recusar livremente o seu consentimento para esta utilização dos seus dados. Todas as informações sobre as obras de manutenção rodoviária também estarão disponíveis no sítio web do município.
>
> [Exemplo 3] Um indivíduo que seja proprietário de terrenos necessita de licenças, tanto do município local como do governo provincial onde se insere o município. Estes dois organismos públicos exigem as mesmas informações para emitirem as respetivas licenças, mas não têm acesso às bases de dados um do outro. Por conseguinte, ambos solicitam as mesmas informações e a proprietária dos terrenos envia aos dois organismos públicos as informações necessárias. O município e a autoridade provincial solicitam o consentimento da senhora para juntar os processos a fim de evitar duplicação de procedimentos e de correspondência. Os dois organismos públicos asseguram que se trata de algo opcional e que os pedidos das licenças serão tratados separadamente caso a senhora decida não dar o seu consentimento à junção dos seus dados. A proprietária dos terrenos pode dar o seu consentimento livremente às autoridades para efeitos da junção dos processos.
>
> [Exemplo 4] Uma escola pública solicita aos estudantes consentimento para utilizar as suas fotografias numa revista estudantil impressa. O consentimento nestas situações seria uma verdadeira escolha desde que não fosse negado aos estudantes o ensino ou os serviços a que têm direito e estes pudessem recusar a utilização das referidas fotografias sem ficarem prejudicados[16].

Também ocorrem desequilíbrios de poder em contexto **laboral**[17]. Atendendo à dependência que resulta da relação empregador/trabalhador, é improvável que o titular dos dados possa recusar ao seu empregador o consentimento para o tratamento dos dados sem que haja medo ou risco real de consequências negativas decorrentes da recusa. É improvável que um trabalhador responda livremente ao pedido de consentimento do empregador para, por exemplo, ativar sistemas de controlo como a observação do local de trabalho através de câmaras ou preencher formulários de avaliação, sem sentir qualquer tipo de pressão para dar esse consentimento[18]. Por conseguinte, o GT29 considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos seus trabalhadores atuais ou futuros com base no consentimento, uma vez que é improvável que esse consentimento seja dado de livre vontade. Relativamente à maior parte deste tratamento de dados no local de trabalho, o fundamento legal não pode nem deve ser o

[16] Para efeitos deste exemplo, uma escola pública significa uma escola financiada com fundos públicos ou qualquer instalação de caráter educativo que, ao abrigo do direito nacional, seja considerada autoridade pública ou organismo público.

[17] Ver também o artigo 88.º do RGPD, onde se enfatiza a necessidade de proteger os interesses específicos dos trabalhadores e onde é estipulada a possibilidade de existirem exceções na lei dos Estados-Membros. Ver também o considerando 155.

[18] Ver Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 12-14; Parecer 8/2001 sobre o tratamento de dados pessoais no âmbito do emprego (WP 48), capítulo 10; documento de trabalho sobre a vigilância das comunicações eletrónicas no local de trabalho (WP 55), ponto 4.2; e Parecer 2/2017 sobre o tratamento de dados no local de trabalho (WP 249), ponto 6.2.

consentimento dos trabalhadores [artigo 6.º, n.º 1, alínea a)], devido à natureza da relação entre empregador e trabalhador[19].

Contudo, isto não significa que os empregadores nunca possam utilizar o consentimento como fundamento legal para o tratamento. Pode haver situações em que seja possível ao empregador demonstrar que o consentimento foi dado livremente. Atendendo ao desequilíbrio de poder entre empregadores e empregados, estes só podem dar o seu consentimento livremente em circunstâncias excecionais, quando o ato de dar ou recusar o consentimento não produza quaisquer consequências negativas[20].

> [Exemplo 5]
> Uma equipa de filmagem pretende filmar determinada parte de um escritório. O empregador solicita o consentimento de todos os trabalhadores que se sentam nessa zona do escritório para serem filmados, uma vez que podem aparecer em segundo plano nas filmagens do vídeo. Os trabalhadores que não quiserem ser filmados não serão de forma alguma penalizados, uma vez que serão colocados noutro local de trabalho equivalente numa outra zona do edifício enquanto durar a filmagem.

Os desequilíbrios de poder não são exclusivos das autoridades públicas e dos trabalhadores, também podem ocorrer noutras situações. Tal como foi realçado pelo GT29 em vários pareceres, o consentimento só pode ser válido se o titular dos dados puder exercer uma verdadeira escolha e não existir qualquer risco de fraude, intimidação, coação ou consequências negativas importantes (p. ex. custos adicionais substanciais) se o consentimento for recusado. O consentimento não será dado livremente nos casos em que exista qualquer elemento de obrigatoriedade, pressão, incapacidade de exercício da livre vontade.

3.1.2. Condicionalidade

O artigo 7.º, n.º 4, é muito importante para avaliar se o consentimento é dado livremente[21].

O artigo 7.º, n.º 4, do RGPD indica que, entre outras, a situação de consentimento «agregado» à aceitação de condições gerais, ou a situação de «associar» a execução de um contrato ou a prestação de um serviço a um pedido de consentimento para tratamento de dados pessoais que não sejam necessários para a execução desse contrato ou para a prestação desse serviço, é considerada muito indesejável. Caso o consentimento seja dado nesta situação, presume-se que não é dado de livre vontade (considerando 43). O artigo 7.º, n.º 4, procura assegurar que a finalidade do tratamento dos dados pessoais não está camuflada nem agregada à execução de um contrato ou à prestação de um serviço para os quais esses dados pessoais não são necessários. Ao fazê-lo, o RGPD assegura que o tratamento dos dados pessoais relativamente ao qual se solicita o consentimento não pode ser direta ou indiretamente uma contrapartida da execução de um contrato. Os dois fundamentos para o

[19] Ver Parecer 2/2017 sobre o tratamento de dados no local de trabalho, p. 6-7.
[20] Ver também Parecer 2/2017 sobre o tratamento de dados no local de trabalho (WP 249), ponto 6.2.
[21] Artigo 7.º, n.º 4, do RGPD: «*Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato.*» Ver também o considerando 43 do RGPD que determina: «*[...] Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.*»

tratamento lícito dos dados pessoais, ou seja, o consentimento e o contrato, não podem fundir-se nem misturar-se.

A obrigatoriedade de concordar com a utilização de dados pessoais para além do que é estritamente necessário limita as escolhas do titular dos dados e constitui um obstáculo ao consentimento dado de livre vontade. Uma vez que as normas de proteção de dados visam proteger os direitos fundamentais, o controlo que as pessoas têm sobre os seus dados pessoais é essencial, existindo uma forte presunção de que o consentimento para o tratamento de dados pessoais que não é necessário não pode ser encarado como algo obrigatório em troca da execução do contrato ou da prestação do serviço.

Daí que, sempre que o responsável pelo tratamento associe o pedido de consentimento à execução do contrato, o titular dos dados que não pretenda disponibilizar os seus dados pessoais para tratamento por parte desse responsável corre o risco de lhe serem negados os serviços que solicitou.

Para aferir se estamos perante uma situação de agregação ou associação do consentimento, é importante determinar qual o âmbito do contrato e quais os dados necessários para a sua execução. De acordo com o Parecer 06/2014 do GT29, a expressão «necessário para a execução de um contrato» deve ser interpretada de forma restritiva. O tratamento deve ser necessário para o cumprimento do contrato em relação a cada um dos titulares dos dados. Tal pode incluir, por exemplo, o tratamento dos dados relativos ao endereço da pessoa em causa para que os bens adquiridos em linha possam ser entregues ou o tratamento dos dados relativos ao cartão de crédito para que o pagamento seja efetuado. No contexto laboral, este fundamento pode permitir, por exemplo, o tratamento das informações relativas ao salário e dos dados relativos à conta bancária para que os salários possam ser pagos[22]. Tem de existir uma relação direta e objetiva entre o tratamento dos dados e a finalidade da execução do contrato.

Se o responsável pelo tratamento pretender tratar dados pessoais que são efetivamente necessários para a execução do contrato, o consentimento não é o fundamento legal[23].

O artigo 7.º, n.º 4, só é aplicável se os dados solicitados **não** forem necessários para a execução do contrato (incluindo a prestação de um serviço) e a execução desse contrato ficar subordinada à obtenção desses dados com base no consentimento. Em contrapartida, se o tratamento **for** necessário para a execução do contrato (incluindo a prestação de um serviço), então o artigo 7.º, n.º 4, não é aplicável.

> [Exemplo 6]
> Um banco solicita aos clientes consentimento para que terceiros possam utilizar os seus dados de pagamento para fins de comercialização direta. Esta atividade de tratamento não é necessária para a execução do contrato nem para a prestação dos serviços bancários normais. Se a recusa do cliente em consentir o tratamento para

[22] Para mais informações e exemplos, consultar 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, adotado pelo GT29 em 9 de abril de 2014, p. 16-17. (WP 217).
[23] O fundamento legal adequado poderá então ser o artigo 6.º, n.º 1, alínea b) (contrato).

estes fins implicar a não prestação dos serviços bancários, o encerramento da conta bancária ou, dependendo do caso, um aumento das comissões, o consentimento não pode ser dado livremente.

A escolha do legislador em realçar a condicionalidade, entre outros, como elemento que pressupõe a falta de liberdade para consentir demonstra que a ocorrência de condicionalidade deve ser alvo de escrutínio criterioso. A expressão «com a máxima atenção» que consta do artigo 7.º, n.º 4, sugere que o responsável pelo tratamento deve ter um cuidado especial se o contrato (que pode incluir a prestação de um serviço) tiver associado um pedido de consentimento para o tratamento dos dados pessoais.

Como a redação do artigo 7.º, n.º 4, não é interpretada de maneira absoluta, pode haver muito pouca margem para casos em que esta condicionalidade não possa tornar o consentimento inválido. Contudo, a palavra «presume-se» que consta do considerando 43 indica claramente que esses casos só ocorrerão muito excecionalmente.

Em todo o caso, o ónus da prova no artigo 7.º, n.º 4, recai sobre o responsável pelo tratamento[24]. Esta norma reflete o princípio geral da responsabilização que permeia todo o RGPD. Contudo, quando o artigo 7.º, n.º 4, for aplicável, será mais difícil para o responsável pelo tratamento provar que o consentimento foi dado de livre vontade pelo titular dos dados[25].

O responsável pelo tratamento pode alegar que a sua organização oferece aos titulares dos dados uma verdadeira escolha se estes puderem optar entre um serviço que inclua consentimento para utilização dos dados pessoais para fins complementares, por um lado, e um serviço equivalente oferecido pelo mesmo responsável pelo tratamento que não envolva consentimento para a utilização dos dados para fins complementares, por outro. Desde que haja a possibilidade de o contrato ser executado ou de o serviço contratado ser prestado por esse responsável pelo tratamento sem consentimento para uma outra utilização dos dados ou para a utilização complementar em causa, significa isto que deixa de existir um serviço sujeito a condicionalidade. Contudo, os dois serviços têm de ser genuinamente equivalentes.

O GT29 considera que o consentimento não pode ser considerado livre se o responsável pelo tratamento alegar que existe uma escolha entre o seu serviço que inclui consentimento para a utilização dos dados pessoais para fins complementares, por um lado, e um serviço equivalente oferecido por um responsável pelo tratamento diferente, por outro. Neste caso, a liberdade de escolha dependeria daquilo que fizessem os outros intervenientes no mercado e dependeria se o titular dos dados ponderasse recorrer aos serviços de outro responsável pelo tratamento

[24] Ver também o artigo 7.º, n.º 1, que determina que o responsável pelo tratamento tem de demonstrar que o titular dos dados deu o seu consentimento de livre vontade.

[25] Em certa medida, a introdução deste número é uma codificação das orientações emitida pelo GT29. Tal como foi descrito no Parecer 15/2011, quando o titular dos dados se encontra numa situação de dependência em relação ao responsável pelo tratamento dos dados – devido à natureza da relação ou a circunstâncias especiais – pode existir uma forte presunção de que a liberdade para consentir está limitada nestes contextos (p. ex. numa relação laboral ou se a recolha de dados for efetuada por uma autoridade pública). Com o artigo 7.º, n.º 4, em vigor, será mais difícil para o responsável pelo tratamento provar que o consentimento foi dado livremente pelo titular dos dados. Ver: Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 12-17.

genuinamente equivalentes ou não. Implicaria igualmente, para os responsáveis pelo tratamento, o dever de controlarem a evolução do mercado para assegurar a contínua validade do consentimento para as suas atividades de tratamento de dados, uma vez que os concorrentes podem alterar posteriormente os respetivos serviços. Como tal, a utilização deste argumento significa que este consentimento não cumpre o RGPD.

3.1.3. Granularidade

Um serviço pode envolver múltiplas operações de tratamento para mais do que uma finalidade. Nestes casos, os titulares dos dados devem poder escolher quais são as finalidades que aceitam e não ter de dar consentimento para um conjunto de finalidades de tratamento. Num determinado caso, pode ser necessário conseguir vários consentimentos para se poder começar a oferecer um serviço, nos termos do RGPD.

O considerando 43 clarifica que se presume que o consentimento não é dado de livre vontade se o processo/procedimento para obter o consentimento não permitir aos titulares dos dados dar consentimento separadamente para diferentes operações de tratamento de dados pessoais (p. ex. só para algumas operações de tratamento e não para outras), ainda que seja adequado no caso específico. O considerando 32 determina que: «*O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins*».

Se o responsável pelo tratamento interligar várias finalidades de tratamento sem tentar procurar separar o consentimento para cada finalidade, estamos perante falta de liberdade. Esta granularidade está estreitamente relacionada com a necessidade de o consentimento ser específico, tal como será analisado no ponto 3.2. Quando o tratamento dos dados for realizado procurando alcançar várias finalidades, a solução para satisfazer as condições inerentes a um consentimento válido passa pela granularidade, ou seja, a separação dessas finalidades e a obtenção de consentimento para cada uma das delas.

> [Exemplo 7]
> Num mesmo pedido de consentimento, o retalhista solicita aos clientes consentimento para utilizar os dados destes para lhes enviar publicidade via correio eletrónico e também para partilhar esses dados com outras empresas do seu grupo. Este consentimento não é granular, uma vez que não separa os consentimentos para estas duas finalidades distintas; por conseguinte, o consentimento não é válido. Neste caso, deve ser recolhido um consentimento específico para enviar os dados de contacto dos clientes para os parceiros comerciais. Esse consentimento específico será considerado válido para cada parceiro (ver também o ponto 3.3.1), cuja identidade tem de ser fornecida ao titular dos dados aquando da recolha do seu consentimento, desde que lhes seja enviado com a mesma finalidade (neste exemplo: a finalidade é a publicidade).

3.1.4. Prejuízos

O responsável pelo tratamento tem de demonstrar que é possível recusar ou retirar o consentimento sem que o titular dos dados seja prejudicado (considerando 42). Por exemplo, o responsável pelo tratamento tem de demonstrar que a retirada do consentimento não implica quaisquer custos para o titular dos dados e, logo, que não existe desvantagem evidente para quem retira o consentimento.

Outros exemplos de prejuízo são a fraude, a intimidação, a coação ou consequências negativas importantes caso um titular de dados não dê o seu consentimento. O responsável pelo tratamento deve poder provar que o titular dos dados tinha uma escolha verdadeira ou livre para dar o consentimento e que era possível retirar o consentimento sem ser prejudicado.

Se o responsável pelo tratamento for capaz de demonstrar que o serviço inclui a possibilidade de retirar o consentimento sem que daí advenham quaisquer consequências negativas, nomeadamente que a prestação do serviço perca qualidade prejudicando o utilizador, tal pode servir para comprovar que o consentimento foi dado livremente. O RGPD não exclui todos os incentivos, mas o ónus de demonstrar que o consentimento foi dado livremente em todas as circunstâncias recai sobre o responsável pelo tratamento.

[Exemplo 8]
Ao descarregar uma aplicação para telemóvel relativa a hábitos de vida, a aplicação solicita consentimento para aceder ao acelerómetro do telefone. Não se trata de algo necessário para a aplicação funcionar, mas é útil para os responsáveis pelo tratamento que pretendem saber mais acerca dos movimentos e dos níveis de atividade dos utilizadores. Posteriormente, se a utilizadora revogar esse consentimento, descobre que a aplicação só funciona parcialmente. Estamos perante um exemplo de prejuízo na aceção do considerando 42, o que significa que o consentimento nunca foi obtido validamente (e logo, o responsável pelo tratamento tem de apagar todos os dados pessoais acerca dos movimentos dos utilizadores recolhidos desta forma).

[Exemplo 9]
O titular de dados subscreve o boletim informativo de um retalhista de moda com descontos gerais. O retalhista solicita ao titular dos dados consentimento para recolher mais dados sobre preferências de compras para personalizar as ofertas em função das preferências do titular dos dados com base no histórico de compras ou num questionário cujo preenchimento é voluntário. Posteriormente, quando o titular dos dados revoga o consentimento, passa novamente a receber descontos de moda não personalizados. Esta situação não implica prejuízo, uma vez que apenas se perdeu o incentivo admissível.

[Exemplo: 10]
Uma revista de moda oferece aos leitores acesso para comprarem novos produtos de maquilhagem antes do lançamento oficial.
Os produtos estarão disponíveis para venda brevemente, mas oferece-se aos leitores da revista uma antevisão exclusiva dos referidos produtos. Para beneficiarem da oferta, as pessoas devem dar a morada e concordar em subscrever a lista de endereços da revista. A morada é necessária para o envio dos produtos e a lista de endereços é utilizada para enviar ofertas comerciais de produtos, tais como cosméticos ou *t-shirts*, durante todo o ano.
A empresa explica que os dados que constam da lista de endereços apenas serão utilizados para o envio de artigos e publicidade em papel pela própria revista e que não são partilhados com outras organizações.
Caso o leitor não queira divulgar o seu endereço por esta razão, não existe prejuízo, uma vez que os produtos estarão disponíveis de qualquer forma.

3.2. Específica

O artigo 6.º, n.º 1, alínea a), confirma que o consentimento do titular dos dados deve ser dado em relação a «uma ou mais finalidades específicas» e que um titular de dados tem uma escolha em relação a cada uma delas[26]. O requisito de que o consentimento deve ser «*específico*» destina-se a

[26] Pode consultar outras orientações sobre a determinação de «finalidades» no Parecer 3/2013 sobre limitação da finalidade (WP 203).

assegurar um certo grau de controlo do utilizador e transparência em relação ao titular dos dados. Este requisito não foi alterado pelo RGPD e permanece estreitamente ligado ao requisito de consentimento «informado». Ao mesmo tempo, deve ser interpretado em consonância com o requisito de «granularidade» aquando da obtenção de consentimento «livre»[27]. Resumindo, para cumprir o elemento «específico», o responsável pelo tratamento deve aplicar:

(i) especificação em função da finalidade como salvaguarda contra o desvirtuamento da função,
(ii) granularidade nos pedidos de consentimento, e
(iii) separação clara entre as informações relacionadas com a obtenção de consentimento para atividades de tratamento de dados e as informações sobre outras questões.

Subalínea i): Nos termos do artigo 5.º, n.º 1, alínea b), do RGPD, a obtenção de consentimento válido é sempre precedida pela determinação de uma finalidade determinada, explícita e legítima para a atividade de tratamento pretendida[28]. A necessidade de consentimento específico em combinação com a noção de limitação da finalidade que consta do artigo 5.º, n.º 1, alínea b), funciona como salvaguarda contra o alargamento ou a diluição progressiva das finalidades para as quais os dados são processados, após o titular de dados ter concordado com a recolha inicial dos dados. Este fenómeno, também conhecido como desvirtuamento da função, é um risco para os titulares dos dados, uma vez que pode resultar na utilização imprevista dos dados pessoais pelo responsável pelo tratamento ou por terceiros e na perda de controlo do titular dos dados.

Se o responsável pelo tratamento se basear no artigo 6.º, n.º 1, alínea a), os titulares dos dados devem sempre dar o seu consentimento para uma finalidade específica do tratamento[29]. Em consonância com o conceito de *limitação da finalidade*, com o artigo 5.º, n.º 1, alínea b), e com o considerando 32, o consentimento pode abranger operações diferentes, desde que essas operações sirvam a mesma finalidade. Escusado será dizer que o consentimento específico só pode ser obtido quando os titulares dos dados são especificamente informados das finalidades previstas de utilização dos dados que lhes dizem respeito.

Não obstante as disposições sobre compatibilidade das finalidades, o consentimento deve ser específico em relação à finalidade. Os titulares dos dados darão o seu consentimento sabendo que detêm controlo sobre os seus dados e que esses dados apenas serão tratados para as finalidades especificadas. Se o responsável tratar os dados com base no consentimento e pretender tratar os dados também para outra finalidade, deve procurar obter outro consentimento para a nova finalidade exceto se existir outro fundamento legal que reflita melhor a situação.

---

[27] O considerando 43 do RGPD determina que é necessário dar consentimento separadamente para diferentes operações de tratamento, quando adequado. Devem ser fornecidas opções granulares de consentimento para permitir que os titulares dos dados consintam separadamente para finalidades distintas.

[28] Ver Parecer 3/2013 do GT29 sobre a limitação da finalidade (WP 203), p. 16: «*Por estas razões, uma finalidade que seja vaga ou geral, como por exemplo "melhorar a experiência dos utilizadores", "para fins de comercialização", "para fins de segurança das TI" ou "para investigação futura" geralmente, sem mais pormenores, não cumpre os critérios de ser "específica".*»

[29] É coerente com o Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), por exemplo, na p. 17.

[Exemplo 11] Uma operadora de TV por cabo recolhe os dados pessoais dos subscritores, com base no seu consentimento, para lhes apresentar sugestões personalizadas de novos filmes que possam ser do seu interesse com base nos hábitos televisivos. Após algum tempo, a operadora de TV decide que gostaria de permitir que terceiros enviem (ou exibam) publicidade personalizada com base nos hábitos televisivos dos subscritores. Atendendo a esta nova finalidade, é necessário obter novo consentimento.

Subalínea ii): Não basta que os mecanismos de consentimento sejam granulares para cumprir o requisito «livre», devem também cumprir o elemento «específico». Significa isto que o responsável pelo tratamento que procure obter consentimento para várias finalidades diferentes deve oferecer a possibilidade de adesão separada para cada finalidade, por forma a permitir que os utilizadores deem consentimento específico para finalidades específicas.

Subalínea iii): Por último, os responsáveis pelo tratamento devem fornecer, com cada um dos pedidos de consentimento distintos, informações específicas acerca dos dados que são tratados para cada finalidade, com vista a sensibilizar os titulares dos dados para os efeitos das diferentes escolhas que têm. Os titulares dos dados podem assim dar um consentimento específico. Esta questão sobrepõe-se ao requisito que exige que os responsáveis pelo tratamento forneçam informações claras, tal como será analisado no ponto 3.3.

3.3. Informada

O RGPD reforça o requisito de que o consentimento deve ser informado. Com base no artigo 5.º do RGPD, o requisito de transparência é um dos princípios fundamentais, estreitamente relacionado com os princípios da lealdade e da licitude. É fundamental fornecer informações aos titulares dos dados antes da obtenção do consentimento para que estes possam tomar decisões informadas, compreendendo com o que estão a concordar e, por exemplo, exercer o direito de retirar o consentimento dado. Se o responsável pelo tratamento não fornecer informações acessíveis, o controlo do utilizador torna-se ilusório e o consentimento será um fundamento inválido para o tratamento.

A consequência de não cumprir os requisitos de consentimento informado é que o consentimento será inválido e o responsável pelo tratamento pode estar a violar o artigo 6.º do RGPD.

3.3.1. Requisitos mínimos de conteúdo para um consentimento «informado»

Para que o consentimento seja informado, é necessário informar o titular dos dados acerca de determinados elementos cruciais para se poder escolher. Por conseguinte, o GT29 considera que, pelo menos, as informações seguintes são necessárias para se obter um consentimento válido:

(i) identidade do responsável pelo tratamento, [30]

(ii) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento[31],

(iii) que (tipo de) dados serão recolhidos e utilizados, [32]

[30] Ver também considerando 42 do RGPD: «*[...] Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. [...]*.»

[31] Uma vez mais, ver considerando 42 do RGPD

(iv) existência do direito de retirar o consentimento[33],

(v) informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º, n.º 2, alínea c)[34], quando pertinente, e

(vi) sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no artigo 46.º[35].

No que diz respeito às subalíneas i) e iii), o GT29 refere que, se o consentimento pretendido puder ser invocado por múltiplos responsáveis (conjuntos) pelo tratamento ou se os dados puderem ser transferidos ou tratados por outros responsáveis pelo tratamento que pretendam invocar o consentimento original, estas organizações devem ser todas identificadas. Não é preciso identificar os subcontratantes como parte dos requisitos do consentimento, embora os responsáveis pelo tratamento, para cumprirem os artigos 13.º e 14.º do RGPD, devam de fornecer uma lista completa dos destinatários ou das categorias de destinatários, incluindo os subcontratantes. Para concluir, o GT29 refere que, dependendo das circunstâncias e do contexto de um caso, podem ser necessárias mais informações para permitir ao titular dos dados compreender verdadeiramente as operações de tratamento em causa.

3.3.2. Como fornecer informações

O RGPD não define a forma nem o formato em que as informações devem ser fornecidas, para cumprir o requisito de consentimento informado. Significa isto que é possível apresentar informações válidas de várias maneiras, tais como declarações escritas ou orais, mensagens áudio ou vídeo. Contudo, o RGPD estipula vários requisitos para o consentimento informado, sobretudo no artigo 7.º, n.º 2, e no considerando 32. Este aspeto implica maior exigência no que toca à clareza e acessibilidade das informações.

Quando procuram obter consentimento, os responsáveis pelo tratamento devem certificar-se de que utilizam uma linguagem clara e informal em todos os casos. Significa isto que a mensagem deve ser fácil de compreender para uma pessoa comum e não só para os advogados. Os responsáveis pelo tratamento utilizam extensos avisos de confidencialidade, que dificultam a compreensão, ou declarações repletas de terminologia jurídica. O consentimento deve ser claro e fácil de distinguir dos outros assuntos e deve ser apresentado de forma inteligível e de fácil acesso. Este requisito significa basicamente que as informações pertinentes para se tomarem decisões informadas sobre dar consentimento não podem estar escondidas nas condições gerais[36].

O responsável pelo tratamento deve assegurar que o consentimento é dado com base em informações que permitem aos titulares dos dados identificar quem é o responsável pelo tratamento

---

[32] Ver também Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 19-20.
[33] Ver artigo 7.º, n.º 3, do RGPD.
[34] Ver também as orientações do GT29 sobre decisões individuais automatizadas, atualmente apenas disponíveis na versão inglesa [Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (WP251), ponto IV.B, p. 20 e seguintes].
[35] Nos termos do artigo 49.º, n.º 1, alínea a), é necessário fornecer informações específicas acerca da inexistência das garantias descritas no artigo 46.º quando se procura obter consentimento explícito. Ver também Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 19.
[36] A declaração de consentimento deve estar identificada como tal. Estilos de redação, como «Sei que...», não cumprem o requisito da linguagem clara.

e compreender aquilo que estão a aceitar. O responsável pelo tratamento deve descrever claramente a finalidade do tratamento dos dados para o qual o consentimento é solicitado[37].

O GT29 forneceu indicações mais específicas sobre a acessibilidade nas orientações sobre transparência. Se o consentimento for dado por meios eletrónicos, o pedido deve ser claro e conciso. Transmitir as informações de forma estruturada e granular pode ser uma maneira adequada de satisfazer o duplo dever de serem rigorosas e completas, por um lado, e compreensíveis, por outro.

O responsável pelo tratamento deve avaliar qual é o tipo de público que fornece dados pessoais à sua organização. Por exemplo, se o público-alvo incluir titulares de dados que sejam menores, espera-se que o responsável pelo tratamento garanta que as informações são compreensíveis para menores[38]. Após identificar o seu público, os responsáveis pelo tratamento devem determinar quais as informações a fornecer e, subsequentemente, como devem apresentar as informações aos titulares dos dados.

O artigo 7.º, n.º 2, abrange declarações de consentimento escritas previamente formuladas que digam também respeito a outros assuntos. Se o consentimento for solicitado como parte do contrato (em papel), o pedido de consentimento deve distinguir-se claramente dos outros assuntos. Se o contrato em papel incluir muitos aspetos que não estejam relacionados com a questão do consentimento para a utilização de dados pessoais, a questão do consentimento deve ser apresentada de maneira a que se destaque claramente ou em documento separado. De igual modo, se o consentimento for solicitado por meios eletrónicos, o pedido de consentimento tem de ser separado e distinto, não podendo simplesmente ser um parágrafo das condições gerais, segundo o considerando 32[39]. Para atender à questão dos ecrãs de pequenas dimensões ou às situações em que o espaço de apresentação de informações é reduzido, pode ponderar-se uma forma estruturada de apresentar as informações, quando adequado, para evitar perturbar excessivamente a experiência do utilizador ou o *design* do produto.

O responsável pelo tratamento que invoque o consentimento do titular dos dados também deve atender aos deveres de informação distintos que constam dos artigos 13.º e 14.º, por forma a cumprir o RGPD. Na prática, o cumprimento dos deveres de informação e o cumprimento do requisito de consentimento informado podem conduzir a uma abordagem integrada em muito casos. Contudo, este ponto foi redigido com base no pressuposto de que pode existir consentimento «informado» válido mesmo que nem todos os elementos dos artigos 13.º e/ou 14.º sejam mencionados no processo de obtenção do consentimento (estes elementos devem evidentemente ser mencionados noutros sítios, como numa declaração de confidencialidade de uma empresa). O GT29 emitiu orientações distintas sobre o requisito da transparência.

[37] Ver artigos 4.º, n.º 11, e 7.º, n.º 2, do RGPD.

[38] Ver também considerando 58 relativamente a informações compreensíveis para crianças.

[39] Ver também o considerando 42 e a Diretiva 93/13/CE, designadamente o artigo 5.º (linguagem clara e compreensível e, em caso de dúvida, prevalece a interpretação mais favorável ao consumidor) e o artigo 6.º (invalidade de cláusulas abusivas, o contrato subsiste sem essas cláusulas somente se ainda vincular as partes, caso contrário é inválido).

[Exemplo 12]
A empresa X é a responsável pelo tratamento das queixas recebidas de que não é claro para os titulares dos dados quais as finalidades de utilização dos dados em relação às quais lhes foi solicitado consentimento. A empresa sente necessidade de verificar se as suas informações no pedido de consentimento são compreensíveis para os titulares dos dados. X organiza painéis de avaliação voluntária para categorias específicas dos seus clientes e apresenta novas atualizações das suas informações de consentimento aos públicos-alvo das avaliações antes de comunicar essas informações externamente. A seleção do painel respeita o princípio da independência e é feita com base em normas que asseguram um resultado representativo e não enviesado. O painel recebe um questionário e os seus membros indicam o que compreenderam das informações e como as avaliariam em termos de compreensão e pertinência. O responsável pelo tratamento continua a fazer avaliações até que os painéis deem indicações de que as informações são compreensíveis. A empresa X elabora um relatório sobre a avaliação e mantém o relatório disponível para referência futura. Este exemplo mostra uma das maneiras possíveis ao dispor de X para demonstrar que os titulares dos dados receberam informações claras antes de darem o seu consentimento para o tratamento dos dados pessoais por X.

[Exemplo 13]
Uma empresa desenvolve a atividade de tratamento de dados com base no consentimento. A empresa utiliza uma declaração de confidencialidade estruturada que inclui um pedido de consentimento. A empresa divulga todos os contactos básicos do responsável pelo tratamento e as atividades de tratamento de dados visadas[40]. Contudo, a empresa não indica de que forma o seu encarregado da proteção de dados pode ser contactado na primeira parte das informações estruturadas que constam da declaração. Para efeitos de fundamento legal válido na aceção do artigo 6.º, esta empresa responsável pelo tratamento obteve consentimento «informado» válido, mesmo não tendo comunicado os contactos do seu encarregado da proteção de dados ao titular dos dados (na primeira parte das informações estruturadas), nos termos dos artigo 13.º, n.º 1, alínea b), ou 14.º, n.º 1, alínea b), do RGPD.

3.4. Manifestação de vontade inequívoca

O RGPD expressa claramente que o consentimento exige da parte do titular dos dados uma declaração ou um ato positivo inequívoco, o que significa que tem de ser dado por meio de ação positiva ou declaração. Tem de ser óbvio que o titular dos dados deu o consentimento para o tratamento em causa.

O artigo 2.º, alínea h), da Diretiva 95/46/CE descreve consentimento como *«manifestação de vontade [...], pela qual a pessoa em causa aceita que dados pessoais que lhe dizem respeito sejam objeto de tratamento»*. O artigo 4.º, n.º 11, do RGPD desenvolve esta definição, clarificando que o consentimento válido exige uma manifestação *explícita* mediante *declaração ou ato positivo inequívoco*, em consonância com as orientações anteriores emitidas pelo GT29.

Um «ato positivo inequívoco» significa que o titular dos dados deve agir deliberadamente para consentir o tratamento em causa[41]. O considerando 32 fornece orientações complementares sobre

[40] Refira-se que, quando a identidade do responsável pelo tratamento ou a finalidade do tratamento não for evidente na primeira parte das informações estruturadas da declaração de privacidade estruturada (e se encontrem noutras partes das informações estruturadas), será difícil para o responsável pelo tratamento dos dados demonstrar que o titular dos dados deu consentimento informado, exceto se o responsável pelo tratamento conseguir comprovar que o titular dos dados em causa acedeu a essas informações antes de dar o consentimento.
[41] Ver documento de trabalho dos serviços da Comissão, avaliação de impacto, anexo 2, p. 20 e também p. 105-106: «*Como também foi referido no parecer adotado pelo GT29 sobre o consentimento, parece fundamental clarificar que o consentimento válido exige a utilização de mecanismos que não deixem dúvidas quanto à intenção do titular dos dados em consentir, deixando ao mesmo tempo claro que – no contexto do ambiente em linha – a utilização de opções*

este assunto. O consentimento pode ser obtido por meio de declaração escrita ou oral (gravada), inclusivamente em formato eletrónico.

Talvez a forma mais literal de cumprir o critério da «declaração escrita» seja garantir que o titular dos dados escreve uma carta ou redige uma mensagem de correio eletrónico ao responsável pelo tratamento explicando exatamente com o que concorda. Contudo, trata-se de algo que frequentemente não é realista. As declarações escritas podem ter muitos formatos e muitas dimensões que podem estar em conformidade com o RGPD.

Sem prejuízo do direito dos contratos em vigor (a nível nacional), o consentimento pode ser obtido por declaração oral gravada, embora importe ter devidamente em atenção quais as informações à disposição do titular dos dados antes de este manifestar o consentimento. A utilização de opções pré-assinaladas de adesão é inválida nos termos do RGPD. O silêncio ou a inatividade da parte do titular dos dados, bem como a mera utilização de um serviço, não podem ser encarados como manifestação ativa de escolha.

> [Exemplo 14]
> Aquando da instalação de um programa informático, a aplicação solicita aos titular dos dados consentimento para utilizar relatórios de falha não anonimizados para melhorar o programa informático. Uma declaração de confidencialidade estruturada com as informações necessárias acompanha o pedido de consentimento. Ao assinalar ativamente a opção que indica «Concordo», o utilizador pode realizar validamente um «ato positivo inequívoco» dando consentimento para o tratamento.

O responsável pelo tratamento também deve ter cuidado com o facto de o consentimento não poder ser obtido através da mesma ação de concordar com o contrato ou aceitar as condições gerais do serviço. A aceitação generalizada de condições gerais não pode ser encarada como ato positivo inequívoco que dá consentimento para a utilização dos dados pessoais. O RGPD não permite que os responsáveis pelo tratamento apresentem opções pré-assinaladas ou outras formas de exclusão que exijam a intervenção do titular dos dados para impedir a aceitação (por exemplo, opções de exclusão)[42].

Quando o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido de consentimento não deve perturbar *desnecessariamente* a utilização do serviço para o qual o consentimento é fornecido[43]. Pode ser necessária uma ação positiva ativa através da qual o titular dos dados dê o seu consentimento sempre que um modo menos invasivo ou

---

pré-assinaladas que o titular dos dados é obrigado a modificar para recusar o tratamento («consentimento baseado no silêncio») não constitui por si só um consentimento inequívoco. As pessoas passam a ter mais controlo sobre os seus próprios dados, sempre que o tratamento se baseie no seu consentimento. No que diz respeito ao impacto sobre os responsáveis pelo tratamento dos dados, o impacto não é grande uma vez que apenas clarifica e especifica melhor as implicações da atual diretiva em relação às condições de obtenção de um consentimento válido e relevante do titular dos dados. Em especial, na medida em que o consentimento «explícito» clarifica – ao substituir «inequívoco» – as modalidades e a qualidade do consentimento e que não se destina a alargar os casos e as situações em que o consentimento (explícito) deve ser utilizado como fundamento para o tratamento, não se prevê que o impacto desta medida nos responsáveis pelo tratamento seja grande.»

[42] Ver artigo 7.º, n.º 2. Ver também o Documento de trabalho 02/2013 sobre a obtenção de consentimento para a utilização de testemunhos de conexão (WP 208), p. 3-6.

[43] Ver considerando 32 do RGPD.

perturbador dar azo a ambiguidade. Como tal, pode ser necessário que o pedido de consentimento interrompa a experiência de utilização até certo ponto para garantir a eficácia do pedido.

Contudo, no âmbito dos requisitos do RGPD, os responsáveis pelo tratamento têm liberdade para desenvolver um fluxo de consentimento que se adeque às respetivas organizações. A este respeito, as ações físicas podem ser consideradas um ato positivo inequívoco em conformidade com o RGPD.

Os responsáveis pelo tratamento devem conceber mecanismos de consentimento que sejam claros para os titulares dos dados. Os responsáveis pelo tratamento devem evitar ambiguidades e devem assegurar que o ato através do qual o titular dos dados dá consentimento pode ser distinguido de outros atos. Por conseguinte, prosseguir meramente com a utilização normal do sítio web não é uma conduta a partir da qual se possa inferir uma manifestação de vontade do titular dos dados que signifique o seu consentimento em relação à operação de tratamento proposta.

> **[**Exemplo 15]
> Deslizar o dedo por uma barra no ecrã, assentir com a cabeça em frente a uma câmara inteligente, rodar o telemóvel no sentido dos ponteiros do relógio ou movimentá-lo de forma a desenhar no ar o número oito podem ser opções para indicar concordância, desde que sejam fornecidas informações claras e desde que seja evidente que o movimento em causa significa concordância com um pedido específico (p. ex. se deslizar o dedo para a esquerda por cima desta barra, concorda em utilizar as informações X para a finalidade Y. Repetir a ação para confirmar). O responsável pelo tratamento deve conseguir demonstrar que o consentimento foi obtido desta forma e os titulares dos dados devem conseguir retirar o consentimento tão facilmente como quando o deram.

> [Exemplo 16]
> Fazer descer a página com o cursor ou com o dedo num sítio web não satisfaz o requisito de um ato positivo e inequívoco. Isto porque o aviso de que continuar a percorrer a página constitui consentimento pode ser difícil de distinguir e/ou pode não ser visto quando o titular dos dados estiver a percorrer rapidamente a página através de grandes quantidades de texto, uma vez que essa ação não é suficientemente inequívoca.

No contexto digital, muitos serviços necessitam de dados pessoais para funcionar, daí que os titulares dos dados recebam diariamente vários pedidos de consentimento que exigem respostas através de cliques ou do deslizar do dedo. Esta situação pode resultar num certo «cansaço» em relação aos cliques: quando aparecem demasiadas vezes, o efeito de alerta dos mecanismos de consentimento começa a diminuir.

Resulta daqui que as questões ligadas ao consentimento começam a deixar de ser lidas. Esta situação constitui um risco particular para os titulares dos dados, uma vez que, tipicamente, o consentimento é solicitado para ações que, em princípio, são ilícitas sem o seu consentimento. O RGPD imputa aos responsáveis pelo tratamento o dever de desenvolver formas de dar resposta a esta questão.

Um exemplo que é muitas vezes referido no contexto em linha é a obtenção de consentimento dos utilizadores da Internet através das respetivas definições do programa de navegação. Essas definições devem ser desenvolvidas em consonância com as condições aplicáveis ao consentimento válido no RGPD, como por exemplo o facto de o consentimento dever ser granular para cada uma

das finalidades visadas e de as informações fornecidas deverem identificar os responsáveis pelo tratamento.

Em todo o caso, o consentimento deve sempre ser obtido antes de o responsável pelo tratamento começar o tratamento dos dados pessoais em relação aos quais o consentimento é necessário. O GT29 tem defendido reiteradamente em pareceres anteriores que o consentimento deve ser dado antes da atividade de tratamento[44]. Embora o RGPD não estipule literalmente no artigo 4.º, n.º 11, que o consentimento deve ser dado antes da atividade de tratamento, trata-se de um aspeto claramente implícito. A parte introdutória do artigo 6.º, n.º 1, e a redação «tiver dado» que consta do artigo 6.º, n.º 1, alínea a), corrobora esta interpretação. Pela lógica, decorre do artigo 6.º e do considerando 40 que o fundamento legal válido deve verificar-se antes do tratamento dos dados. Por conseguinte, o consentimento deve ser dado antes da atividade de tratamento. Em princípio, pode ser suficiente solicitar o consentimento do titular dos dados uma única vez. Contudo, os responsáveis pelo tratamento devem obter um consentimento novo e específico caso as finalidades do tratamento dos dados mudem após a obtenção do consentimento ou se pretenderem acrescentar alguma outra finalidade.

4. Obter consentimento explícito

O consentimento explícito é necessário em determinadas situações em que surge um risco grave para a proteção dos dados e, portanto, em que se considera adequado existir um nível elevado de controlo individual em relação aos dados pessoais. Nos termos do RGPD, o consentimento explícito desempenha um papel no artigo 9.º relativo ao tratamento de categorias especiais de dados, nas disposições sobre transferências de dados para países terceiros ou organizações internacionais na ausência de garantias adequadas no artigo 49.º[45], bem como no artigo 22.º relativo a decisões individuais automatizadas, incluindo definição de perfis[46].

O RGPD prevê uma «declaração ou ato afirmativo inequívoco» como requisito prévio do consentimento «conforme às regras». Uma vez que, no RGPD, o requisito de consentimento «conforme às regras» é mais exigente do que o requisito de consentimento que consta da Diretiva 95/46/CE, importa clarificar quais são os esforços adicionais que o responsável pelo

[44] O GT29 tem adotado reiteradamente esta posição desde o Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 30-31.

[45] De acordo com o artigo 49.º, n.º 1, alínea a), do RGPD, o consentimento explícito pode afastar a proibição de transferir dados para países que não dispõem de níveis adequados de proteção de dados na sua legislação. Consultar também o documento de trabalho sobre uma interpretação comum do n.º 1 do artigo 26.º da Diretiva 95/46/CE de 24 de outubro de 1995 (WP 114), p. 11, em que o GT29 indica que o consentimento para transferências de dados que ocorram periódica ou repetidamente é inadequado.

[46] No artigo 22.º, o RGPD introduz disposições para proteger os titulares de dados contra decisões baseadas unicamente no tratamento automatizado, incluindo definição de perfis. As decisões tomadas com este fundamento são permitidas em determinadas condições jurídicas. O consentimento desempenha um papel importante neste mecanismo de proteção, dado que o artigo 22.º, n.º 2, alínea c), do RGPD deixa claro que o responsável pelo tratamento pode avançar com decisões automatizadas, incluindo definição de perfis, que possam afetar significativamente o indivíduo com o consentimento explícito do titular dos dados. O GT29 emitiu orientações distintas sobre esta questão: orientações do GT29 sobre decisões individuais automatizadas, atualmente apenas disponíveis na versão inglesa (Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679), de 3 de outubro de 2017, (WP251).

tratamento deve envidar para obter o consentimento *explícito* de um titular de dados em consonância com o RGPD.

O termo *explícito* refere-se à forma como o consentimento é manifestado pelo titular dos dados. Significa que o titular dos dados deve manifestar expressamente o consentimento. Uma maneira óbvia de garantir que o consentimento é explícito seria confirmar expressamente o consentimento numa declaração escrita. Quando adequado, o responsável pelo tratamento pode certificar-se de que a declaração escrita é assinada pelo titular dos dados, por forma a eliminar todas as dúvidas possíveis e uma potencial falta de provas no futuro[47].

Contudo, a referida declaração escrita não é a única maneira de obter consentimento explícito e não se pode dizer que o RGPD recomenda declarações escritas e assinadas em todas as circunstâncias que exigem um consentimento explícito válido. Por exemplo, num contexto digital ou em linha, o titular de dados pode emitir a declaração necessária preenchendo um formulário eletrónico, enviando uma mensagem de correio eletrónico, carregando um documento digitalizado com a assinatura do titular dos dados ou utilizando uma assinatura eletrónica. Em teoria, a utilização de declarações orais também pode ser suficiente para obter um consentimento explícito válido. Contudo, pode ser difícil para o responsável pelo tratamento provar que todas as condições aplicáveis ao consentimento explícito válido foram satisfeitas quando a declaração foi gravada. Uma organização também pode obter consentimento explícito através de uma conversa telefónica, desde que as informações acerca da escolha sejam leais, inteligíveis e claras, e desde que a organização solicite uma confirmação específica ao titular dos dados (p. ex. pressionar uma tecla ou fornecer confirmação oral).

> [Exemplo 17] O responsável pelo tratamento também pode obter o consentimento explícito de uma pessoa que visite o seu sítio web exibindo um ecrã de consentimento explícito que contenha as opções Sim e Não, desde que o texto indique claramente o consentimento. Por exemplo, «Pelo presente, dou o meu consentimento para o tratamento dos meus dados» e não, por exemplo, «É evidente para mim que os meus dados serão tratados». Escusado será dizer que as condições aplicáveis ao consentimento informado, bem como a outras condições aplicáveis à obtenção de consentimento válido, devem ser satisfeitas.
>
> [Exemplo 18] Uma clínica de cirurgia cosmética solicita o consentimento explícito do paciente para transferir os registos médicos deste para um especialista a quem será pedida uma segunda opinião acerca da sua situação clínica. O registo médico é um ficheiro digital. Atendendo à natureza específica das informações em causa, a clínica solicita uma assinatura eletrónica ao titular dos dados para obter o consentimento explícito válido e para poder comprovar que foi obtido esse consentimento explícito[48].

A verificação de consentimento em duas fases também pode ser uma forma de garantir a validade do consentimento explícito. Por exemplo, o titular de dados recebe uma mensagem de correio eletrónico notificando-o da intenção do responsável pelo tratamento de tratar um registo que contém dados clínicos. O responsável pelo tratamento explica na mensagem de correio eletrónico que

[47] Ver também Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 25.
[48] Este exemplo não prejudica as disposições do Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno.

solicita o consentimento para a utilização de um conjunto específico de informações para uma finalidade específica. Se o titular dos dados concordar com a utilização destes dados, o responsável pelo tratamento solicita-lhe que responda à mensagem de correio eletrónico com a declaração «Concordo». Após envio da resposta, o titular dos dados recebe um *link* de verificação no qual deve clicar ou uma mensagem SMS com um código de verificação para confirmar que concorda.

O artigo 9.º, n.º 2, não reconhece «necessário para a execução de um contrato» como uma exceção à proibição geral de tratamento de categorias especiais de dados. Por conseguinte, os responsáveis pelo tratamento e os Estados-Membros que se defrontam com esta situação devem recorrer às exceções previstas no artigo 9.º, n.º 2, alíneas b) a j). Caso nenhuma das exceções que constam das alíneas b) a j) se aplique, a obtenção de consentimento explícito em conformidade com as condições aplicáveis ao consentimento válido no RGPD será a única exceção lícita possível para tratar os referidos dados.

[Exemplo 19]
A companhia aérea Holiday Airways oferece um serviço de viagem assistido para os passageiros que não conseguem viajar sem assistência, por exemplo devido a uma deficiência. Uma cliente marca um voo de Amesterdão para Budapeste e solicita assistência em viagem para poder entrar no avião. A Holiday Airways solicita à passageira informações sobre o seu estado de saúde para poder disponibilizar os serviços adequados (uma vez que as possibilidades são muitas, por exemplo, cadeira de rodas na porta de embarque ou um assistente que viaje com ela de A. para B.). A Holiday Airways solicita consentimento explícito para proceder ao tratamento dos dados clínicos da sua cliente com a finalidade de disponibilizar a assistência em viagem solicitada. Os dados tratados com base no consentimento devem ser necessários para o serviço solicitado. Além disso, os voos para Budapeste permanecem disponíveis sem assistência em viagem. Importa referir que, uma vez que os dados referidos são necessários para a prestação do serviço solicitado, o artigo 7.º, n.º 4, não é aplicável.

[Exemplo 20]
Uma empresa de sucesso especializou-se em óculos personalizados para a prática de esqui e *snowboard* e noutros tipos de equipamentos oculares para desportos ao ar livre. A ideia é fazer com que as pessoas possam usar estes equipamentos sem terem de utilizar simultaneamente os seus próprios óculos. A empresa recebe encomendas de forma centralizada e entrega os produtos a partir de um único local em toda a UE. Para poder fornecer os seus produtos personalizados aos clientes com miopia, este responsável pelo tratamento solicita-lhes o consentimento para a utilização de informações sobre os respetivos problemas oculares. Os clientes fornecem os dados clínicos necessários, tais como os dados das receitas médicas, em linha, quando fazem a encomenda. Sem estes dados, não será possível à empresa fornecer os equipamentos oculares personalizados solicitados. A empresa também oferece uma gama de óculos com valores corretivos normalizados. Os clientes que não pretendam partilhar os seus dados clínicos podem optar por versões normalizadas. Por conseguinte, é necessário um consentimento explícito ao abrigo do artigo 9.º e pode-se considerar que o consentimento foi dado livremente.

5. Outras condições para a obtenção de consentimento válido

O RGPD introduz requisitos para que os responsáveis pelo tratamento tomem medidas complementares para se certificarem de que obtêm, conservam e conseguem comprovar um consentimento válido. O artigo 7.º do RGPD prevê condições adicionais aplicáveis ao consentimento válido, com normas específicas sobre a conservação de registos relativos ao consentimento e o direito a retirar facilmente o consentimento. O artigo 7.º também é aplicável ao consentimento referido noutros artigos do RGPD, por exemplo nos artigos 8.º e 9.º. Abaixo, são

fornecidas orientações sobre os requisitos adicionais para demonstrar o consentimento válido e sobre a retirada do consentimento.

5.1. Demonstrar o consentimento

No artigo 7.º, n.º 1, o RGPD descreve claramente a obrigação explícita que recai sobre o responsável pelo tratamento de demonstrar que o titular dos dados deu o seu consentimento. O ónus da prova recai sobre o responsável pelo tratamento, de acordo com o artigo 7.º, n.º 1.

O considerando 42 determina: *«Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados.»*

Os responsáveis pelo tratamento têm liberdade para desenvolver métodos que visem o cumprimento desta disposição de maneira que se adeque às suas operações quotidianas. Ao mesmo tempo, o dever de demonstrar que o responsável pelo tratamento obteve um consentimento válido não deve, por si só, conduzir a quantidades excessivas de tratamento de dados adicionais. Significa isto que os responsáveis pelo tratamento devem ter dados suficientes para mostrar uma ligação ao tratamento (mostrar que foi obtido consentimento), mas não devem recolher mais informações do que as necessárias.

Cabe ao responsável pelo tratamento provar que o consentimento válido foi obtido junto do titular dos dados. O RGPD não prevê exatamente como é que isso deve ser feito. Contudo, o responsável pelo tratamento deve conseguir provar que o titular de dados deu o seu consentimento em determinada situação. Enquanto a atividade de tratamento de dados em causa perdurar, a obrigação de demonstrar o consentimento existe. Quando terminar a atividade de tratamento, a prova do consentimento não deve ser conservada mais do que o necessário para o cumprimento de um dever legal ou para efeitos de declaração, exercício ou defesa de direitos num processo judicial, em conformidade com o artigo 17.º, n.º 3, alínea b) e e).

Por exemplo, o responsável pelo tratamento pode conservar um registo das declarações de consentimento recebidas para poder mostrar e comprovar de que forma o consentimento foi obtido, quando foi obtido e quais as informações fornecidas ao titular dos dados na altura. O responsável pelo tratamento deve também poder mostrar que o titular dos dados foi informado e que o fluxo de trabalho do responsável pelo tratamento cumpriu todos os critérios aplicáveis ao consentimento válido. A lógica subjacente a este dever previsto no RGPD é que os responsáveis pelo tratamento devem ser responsabilizados relativamente à obtenção de consentimento válido junto dos titulares dos dados e à aplicação de mecanismos de consentimento. Por exemplo, num contexto em linha, o responsável pelo tratamento pode conservar informações sobre a sessão em que o consentimento foi dado, juntamente com documentação do fluxo de trabalho para obtenção do consentimento na altura da sessão, bem como uma cópia das informações que foram apresentadas ao titular dos dados na altura. Não seria suficiente fazer apenas referência a uma configuração correta do respetivo sítio web.

[Exemplo 21] Um hospital cria um programa de investigação científica, denominado projeto X, para o qual são necessários os registos dentários de pacientes reais. Os participantes são recrutados através de chamadas telefónicas para pacientes que concordam voluntariamente em integrar a lista de candidatos que podem ser abordados para o efeito. O responsável pelo tratamento procura obter o consentimento explícito dos titulares dos dados para a utilização dos seus registos dentários. O consentimento é obtido durante a chamada telefónica através da gravação da declaração oral do titular dos dados em que este confirma que concorda com a utilização dos seus dados para efeitos do projeto X.

Não existe prazo no RGPD que determine a duração da validade do consentimento, que dependerá do contexto, do âmbito do consentimento original e das expectativas do titular dos dados. Se as operações de tratamento se alterarem ou evoluírem consideravelmente, o consentimento original deixa de ser válido. Nesse caso, será necessário obter novo consentimento.

O GT29 recomenda como boa prática a renovação do consentimento em intervalos temporais adequados. Fornecer novamente todas as informações ajuda a assegurar que o titular dos dados continua bem informado acerca da forma como os seus dados estão a ser utilizados e como pode exercer os seus direitos[49].

5.2. Retirada do consentimento

A retirada do consentimento ocupa um lugar de destaque no RGPD. As disposições e os considerandos sobre a retirada do consentimento no RGPD podem ser encarados como uma codificação da interpretação que consta nos pareceres do GT29 sobre esta matéria[50].

O artigo 7.º, n.º 3, do RGPD prevê que o responsável pelo tratamento deve garantir que o consentimento pode ser tão fácil de retirar como de dar pelo titular dos dados, a qualquer momento. O RGPD não refere que o ato de dar ou retirar o consentimento deva sempre ser executado pela mesma ação.

Contudo, se o consentimento for obtido por meios eletrónicos unicamente clicando no rato, deslizando o dedo ou pressionando uma tecla, os titulares dos dados devem, na prática, poder retirar esse consentimento de forma igualmente fácil. Se o consentimento for obtido mediante a utilização de uma interface de utilizador para um serviço específico (por exemplo, sítio web, aplicação, conta com senha de acesso, interface de um dispositivo da IdC ou correio eletrónico), não há dúvida de que o titular de dados deve conseguir retirar o consentimento na mesma interface eletrónica, uma vez que mudar para outra interface unicamente para efeitos de retirada do consentimento exigiria um esforço indevido. Além disso, o titular dos dados deve poder retirar o consentimento sem

[49] Ver orientações do GT29 sobre transparência. [Finalizar a citação quando as informações necessárias estiverem disponíveis]

[50] O GT29 abordou este assunto no seu parecer sobre consentimento [ver Parecer 15/2011 sobre a definição de consentimento (WP 187), p. 9, 13, 20, 27 e 32-33] e, entre outros, no seu parecer sobre a utilização dos dados de localização. [ver o Parecer 5/2005 do GT29 sobre a utilização de dados de localização para criar serviços de valor acrescentado (WP 115), p. 7].

prejuízo. Significa isto, entre outras coisas, que o responsável pelo tratamento deve prever a possibilidade de retirar o consentimento de forma gratuita ou sem baixar os níveis do serviço[51].

> [Exemplo 22] Um festival de música vende bilhetes através de uma bilheteira em linha. De cada vez que um bilhete é vendido em linha, solicita-se consentimento para utilizar os contactos fornecidos para fins de comercialização. Para darem indicação sobre o consentimento para esta finalidade, os clientes podem selecionar a resposta Não ou Sim. O responsável pelo tratamento informa os clientes de que têm a possibilidade de retirar o consentimento. Para o fazerem, podem contactar gratuitamente um centro de atendimento nos dias úteis entre as 8h e as 17h. O responsável pelo tratamento neste exemplo não cumpre o disposto no artigo 7.º, n.º 3, do RGPD. Retirar o consentimento neste caso requer uma chamada telefónica durante as horas de expediente, algo que é mais moroso do que o clique no rato necessário para dar o consentimento através da bilheteira em linha, aberta 24 horas por dia, 7 dias por semana.

O requisito relativo à facilidade em retirar o consentimento é descrito como um aspeto necessário para um consentimento válido no RGPD. Se o direito de retirada não cumprir os requisitos do RGPD, o mecanismo de consentimento do responsável pelo tratamento não cumpre o RGPD. Tal como referido no ponto 3.1 sobre a condição do consentimento informado, o responsável pelo tratamento deve informar o titular dos dados acerca do direito de retirar o consentimento antes de este dar efetivamente consentimento, nos termos do artigo 7.º, n.º 3, do RGPD. Além disso, o responsável pelo tratamento deve, no âmbito da obrigação de transparência, informar os titulares dos dados acerca de como podem exercer os seus direitos[52].

Regra geral, se o consentimento for retirado, todas as operações de tratamento de dados baseadas nesse consentimento e que ocorreram antes da retirada do consentimento – e em conformidade com o RGPD – permanecem lícitas. Contudo, o responsável pelo tratamento deve parar as ações de tratamento em causa. Caso não exista qualquer outro fundamento legal que justifique o tratamento (p. ex. continuação da conservação) dos dados, estes devem ser apagados pelo responsável pelo tratamento[53].

Como foi referido anteriormente nas presentes orientações, é muito importante que os responsáveis pelo tratamento avaliem as finalidades para as quais os dados são efetivamente tratados e os fundamentos legais em que se baseia o tratamento antes de recolher os dados. É frequente as empresas precisarem de dados pessoais para várias finalidades, baseando-se o tratamento em mais do que um fundamento legal, por exemplo os dados dos clientes podem basear-se em contrato e consentimento. Como tal, a retirada do consentimento não significa que o responsável pelo tratamento tenha de apagar os dados tratados para uma finalidade que se baseia na execução do contrato celebrado com o titular dos dados. Por conseguinte, os responsáveis pelo tratamento devem

---

[51] Ver o Parecer 4/2010 do GT29 sobre o código de conduta europeu da FEDMA relativo ao uso de dados pessoais no *marketing* direto (WP 174) e o parecer sobre a utilização de dados de localização para criar serviços de valor acrescentado (WP 115).

[52] O considerando 39 do RGPD, que remete para os artigos 13.º e 14.º do referido regulamento, determina que «*as pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento».*

[53] Ver artigo 17.º, n.º 1, alínea b), e n.º 3, do RGPD.

desde o início ser muito claros quanto à finalidade a que corresponde cada elemento dos dados e em que fundamento legal assenta.

Os responsáveis pelo tratamento devem apagar os dados tratados com base no consentimento assim que o consentimento for retirado, partindo do pressuposto de que não existe outra finalidade que justifique a sua conservação[54].
Para além desta situação, abrangida pelo artigo 17.º, n.º 1, alínea b), o titular dos dados pessoais pode solicitar o apagamento de outros dados que lhe digam respeito e que sejam tratados com outro fundamento legal, por exemplo o artigo 6.º, n.º 1, alínea b)[55]. Os responsáveis pelo tratamento são obrigados a avaliar se continuar com o tratamento dos dados em causa é adequado, mesmo não existindo um pedido de apagamento pelo titular dos dados[56].

Se o titular dos dados retirar o consentimento e o responsável pelo tratamento pretender continuar a tratar os dados pessoais com outro fundamento legal, este último não pode migrar silenciosamente do consentimento (que foi retirado) para esse outro fundamento. Qualquer alteração do fundamento legal do tratamento deve ser notificada ao titular dos dados em conformidade com os deveres de informação previstos nos artigos 13.º e 14.º e nos termos do princípio geral da transparência.

6. Interação entre o consentimento e outros fundamentos de licitude no artigo 6.º do RGPD

O artigo 6.º estabelece as condições do tratamento lícito dos dados pessoais e descreve seis fundamentos legais que o responsável pelo tratamento pode invocar. A aplicação de um desses seis fundamentos deve ser estabelecida antes da atividade de tratamento e em relação a uma finalidade específica[57].

É importante referir aqui que o responsável pelo tratamento, se optar por invocar o consentimento para qualquer parte do tratamento, deve estar preparado para respeitar essa opção e parar essa parte do tratamento se um indivíduo retirar o consentimento. Passar a mensagem de que os dados serão tratados com base no consentimento enquanto, na verdade, esse tratamento assenta noutro fundamento legal, seria fundamentalmente desleal para com as pessoas.

Por outras palavras, o responsável pelo tratamento não pode passar do consentimento para outros fundamentos legais. Por exemplo, não lhe é permitido utilizar retroativamente o fundamento do interesse legítimo para justificar o tratamento, se forem detetados problemas com a validade do consentimento. Por causa do requisito de divulgação do fundamento legal que o responsável pelo tratamento invoca aquando da recolha dos dados pessoais, os responsáveis pelo tratamento devem decidir antes da recolha dos dados qual é o fundamento legal aplicável.

[54] Nesse caso, a outra finalidade que justifica o tratamento deve ter o seu próprio fundamento legal distinto. Isto não significa que o responsável pelo tratamento pode passar do consentimento para outro fundamento legal, ver o ponto 6.
[55] Ver o artigo 17.º, incluindo exceções aplicáveis, e o considerando 65 do RGPD.
[56] Ver também o artigo 5.º, n.º 1, alínea e), do RGPD.
[57] Nos termos dos artigos 13.º, n.º 1, alínea c), e/ou 14.º, n.º 1, alínea c), o responsável pelo tratamento deve informar o titular dos dados acerca dessas questões.

7. Preocupações específicas no RGPD

7.1. Crianças (artigo 8.º)

Comparado com a atual diretiva, o RGPD cria mais um nível de proteção quando os dados pessoais de pessoas singulares vulneráveis, em especial crianças, são tratados. O artigo 8.º introduz obrigações adicionais para assegurar um nível reforçado de proteção dos dados das crianças em relação aos serviços da sociedade da informação. As razões para o reforço da proteção encontram-se especificadas no considerando 38: *«[...] podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. [...]»* O considerando 38 também determina que: «*Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças.*» A expressão «nomeadamente» indica que a proteção específica não se limita à comercialização ou definição de perfis, incluindo também a «recolha de dados pessoais em relação às crianças» mais abrangente.

O artigo 8.º, n.º 1, refere que quando for aplicável o consentimento, no que respeita à oferta direta de serviços da sociedade da informação às crianças, o tratamento dos dados pessoais é lícito se elas tiverem pelo menos 16 anos. Se a criança tiver menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares da responsabilidade parental[58]. Relativamente à idade-limite do consentimento válido, o RGPD prevê flexibilidade. Os Estados-Membros podem dispor no seu direito um limite diferente, que não pode ser inferior a 13 anos.

Tal como referido no ponto 3.1 sobre o consentimento informado, as informações devem ser compreensíveis para o público-alvo do responsável pelo tratamento, com especial atenção para a posição das crianças. Para obter «consentimento informado» de uma criança, o responsável pelo tratamento deve explicar em linguagem clara e simples para crianças de que forma pretende tratar os dados que irá recolher[59]. Caso seja o progenitor quem supostamente deve consentir, então pode ser necessário um conjunto de informações que permita aos adultos tomar uma decisão informada.

O que precede mostra claramente que o artigo 8.º só é aplicável quando estiverem satisfeitas as seguintes condições:

- O tratamento está relacionado com oferta direta de serviços da sociedade da informação a uma criança[60,61].

[58] Sem prejuízo da possibilidade de o direito do Estado-Membro afastar o limite de idade, ver o artigo 8.º, n.º 1.
[59] O considerando 58 do RGPD reafirma esta obrigação quando determina que, se for caso disso, o responsável pelo tratamento deve certificar-se de que as informações fornecidas são compreensíveis para as crianças.
[60] De acordo com o artigo 4.º, n.º 25, do RGPD, um serviço da sociedade da informação significa um serviço na aceção do artigo 1.º, n.º 1, alínea b), da Diretiva 2015/1535: *«b) "Serviço" significa qualquer serviço da sociedade da informação, isto é, qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços; Para efeitos da presente definição, entende-se por: i) "à*

- O tratamento baseia-se no consentimento.

7.1.1. Serviços da sociedade da informação

Para determinar o âmbito da expressão «serviços da sociedade da informação» no RGPD, o seu artigo 4.º, n.º 25, remete para a Diretiva 2015/1535.

Ao avaliar o âmbito desta definição, o GT29 também remete para jurisprudência do TJUE[62]. O TJUE considerou que os *serviços da sociedade da informação* abrangem contratos e outros serviços que sejam celebrados ou transmitidos em linha. Se um serviço tiver duas componentes economicamente independentes, sendo uma a componente em linha, tal como a oferta e aceitação de uma oferta no contexto da celebração de um contrato ou as informações relativas a produtos e serviços, incluindo atividades de comercialização, esta componente é definida como um serviço da sociedade da informação; a outra componente, sendo a entrega ou distribuição dos produtos, não está abrangida pela noção de serviço da sociedade da informação. A prestação de serviços em linha insere-se no âmbito da expressão *serviços da sociedade da informação* que consta do artigo 8.º do RGPD.

7.1.2. Oferecidos diretamente a uma criança

A inclusão da expressão «oferta direta [...] às crianças» indica que o artigo 8.º se destina a ser aplicado a alguns, mas não todos, os serviços da sociedade da informação. A este respeito, se um prestador de serviços da sociedade da informação deixar bem claro aos potenciais utilizadores que só oferece os seus serviços a pessoas com 18 anos ou mais e se este facto não for refutado por outros elementos de prova (tais como o conteúdo do sítio ou planos de comercialização), então o serviço não será considerado como uma «oferta direta às crianças» e o artigo 8.º não é aplicável.

7.1.3. Idade

O RGPD especifica que «*Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos*». O responsável pelo tratamento deve conhecer os diferentes direitos nacionais, tendo em conta o público a que os seus serviços se destinam. Em especial, importa referir que o responsável pelo tratamento que preste um

---

distância": um serviço prestado sem que as partes estejam simultaneamente presentes, ii) "por via eletrónica": um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos, iii) "mediante pedido individual de um destinatário de serviços": um serviço fornecido por transmissão de dados mediante pedido individual;» No anexo I da referida diretiva consta uma lista indicativa dos serviços não incluídos nesta definição. Ver também o considerando 18 da Diretiva 2000/31/CE.

[61] De acordo com o artigo 1.º da Convenção das Nações Unidas sobre os Direitos da Criança, «[...] *criança é todo o ser humano menor de 18 anos, salvo se, nos termos da lei que lhe for aplicável, atingir a maioridade mais cedo.*», ver Assembleia Geral das Nações Unidas, Resolução 44/25 de 20 de novembro de 1989 (Convenção sobre os Direitos da Criança).

[62] Ver Tribunal de Justiça da União Europeia, 2 de dezembro de 2010, Processo C-108/09 (*Ker-Optika*), n.os 22 e 28. Em relação a «serviços compósitos», o GT29 também refere o Processo C-434/15 (*Asociacion Profesional Elite Taxi / Uber Systems Spain SL*), n.º 40, onde se determina que o serviço da sociedade da informação que faça parte integrante de um serviço global cujo elemento principal não seja um serviço da sociedade da informação (neste caso, um serviço de transporte) não deve ser considerado «serviço da sociedade da informação».

serviço transfronteiriço não pode invocar sempre o cumprimento apenas do direito do Estado-Membro onde tem o seu estabelecimento principal, pode também necessitar de cumprir o direito nacional de cada Estado-Membro em que oferecer serviços da sociedade da informação. Isto depende se o Estado-Membro escolher utilizar o local do estabelecimento principal do responsável pelo tratamento como ponto de referência no seu direito nacional ou a residência do titular dos dados. Ao fazer a sua escolha, os Estados-Membros devem considerar em primeiro lugar o interesse superior da criança. O Grupo de Trabalho incentiva os Estados-Membros a procurarem uma solução harmonizada nesta matéria.

Quando prestam serviços da sociedade da informação às crianças com base no consentimento, espera-se que os responsáveis pelo tratamento envidem esforços razoáveis para verificar se o utilizador já ultrapassou a idade para o consentimento digital e que essas medidas sejam proporcionais à natureza e aos riscos das atividades de tratamento.

Se os utilizadores afirmarem que já ultrapassaram a idade para o consentimento digital, então o responsável pelo tratamento pode realizar verificações adequadas para comprovar que essa afirmação é verdadeira. Embora a necessidade de envidar esforços razoáveis para verificar a idade não conste explicitamente no RGPD, trata-se de algo implícito porque o facto de a criança consentir sem ter idade suficiente para dar consentimento válido em nome próprio torna o tratamento dos dados ilícito.

Se o utilizador afirmar que não tem idade para dar consentimento digital, então o responsável pelo tratamento pode aceitar esta declaração sem mais verificações, mas precisará de obter autorização parental e verificar se a pessoa que está a dar o consentimento é o titular da responsabilidade parental.

A verificação da idade não deve conduzir a um tratamento de dados excessivo. O mecanismo escolhido para verificar a idade de um titular de dados deve envolver a avaliação do risco do tratamento proposto. Nalgumas situações de baixo risco, pode ser adequado exigir que o novo subscritor do serviço revele o seu ano de nascimento ou preencha um formulário onde declara (não) ser menor[63]. Caso tenha dúvidas, o responsável pelo tratamento deve reavaliar os seus mecanismos de verificação da idade num determinado caso e considerar se são necessárias verificações alternativas[64].

7.1.4. Consentimento dado por crianças e responsabilidade parental

Relativamente à autorização de um titular da responsabilidade parental, o RGPD não especifica formas práticas para obter o consentimento parental nem para determinar se alguém está em posição de realizar essa ação[65]. Por conseguinte, o GT29 recomenda a adoção de uma abordagem proporcionada, em consonância com os artigo 8.º, n.º 2, com 5.º, n.º 1, alínea c), do RGPD

[63] Embora esta solução possa não resultar em todos os casos, é um exemplo de como entender esta disposição.
[64] Ver o Parecer 5/2009 do GT29 sobre as redes sociais em linha (WP 163).
[65] O GT29 refere que nem sempre o titular da responsabilidade parental é o progenitor da criança e que a responsabilidade parental pode caber a várias partes, que podem incluir pessoas singulares e pessoas coletivas.

(minimização dos dados). Uma abordagem proporcionada pode ser dar ênfase à obtenção de uma quantidade limitada de informações, tais como dados de contacto de um dos progenitores ou tutores.

O que é razoável, tanto para verificar se o utilizador tem idade suficiente para dar consentimento, como para verificar se a pessoa que dá o consentimento em nome da criança é o titular da responsabilidade parental, pode depender dos riscos inerentes ao tratamento, bem como à tecnologia disponível. Em casos de baixo risco, a verificação da responsabilidade parental por correio eletrónico pode ser suficiente. Em contrapartida, em casos de alto risco, pode ser adequado solicitar mais provas, para que o responsável pelo tratamento possa verificar e conservar as informações nos termos do artigo 7.º, n.º 1, do RGPD[66]. Alguns serviços de confiança prestados por terceiros de confiança podem oferecer soluções que minimizem a quantidade de dados pessoais que o responsável pelo tratamento tem de tratar ele próprio.

> [Exemplo 23] Uma plataforma de jogos em linha quer garantir que os clientes menores só conseguem subscrever os seus serviços com o consentimento dos progenitores ou tutores. O responsável pelo tratamento segue os passos seguintes:
> Passo 1: pede ao utilizador que indique se tem menos ou mais de 16 anos (ou idade alternativa para consentimento digital).
> Se o utilizador indicar que a sua idade é inferior à idade para consentimento digital:
> Passo 2: o serviço informa a criança de que um dos progenitores ou tutores deve consentir ou autorizar o tratamento antes de o serviço ser prestado à criança. É pedido ao utilizador que revele o endereço eletrónico de um dos progenitores ou tutores.
> Passo 3: o serviço contacta o progenitor ou tutor e obtém o seu consentimento através de mensagem de correio eletrónico para o tratamento e toma medidas razoáveis para confirmar que o adulto tem responsabilidade parental.
> Passo 4: em caso de queixas, a plataforma toma medidas adicionais para verificar a idade do subscritor.
> Se a plataforma observar os outros requisitos do consentimento, a plataforma pode cumprir os critérios adicionais do artigo 8.º do RGPD seguindo estes passos.

O exemplo mostra que o responsável pelo tratamento pode colocar-se numa posição que revele que envidou esforços razoáveis para assegurar a obtenção de consentimento válido, em relação aos serviços prestados a uma criança. O artigo 8.º, n.º 2, acrescenta em particular que «*o responsável pelo tratamento envida todos os esforços adequados para verificar que o consentimento foi dado ou autorizado pelo titular das responsabilidades parentais da criança, tendo em conta a tecnologia disponível*».

Cabe ao responsável pelo tratamento determinar quais são as medidas adequadas num caso específico. Regra geral, os responsáveis pelo tratamento devem evitar soluções de verificação que envolvam, elas mesmas, uma recolha excessiva de dados pessoais.

[66] Por exemplo, o responsável pelo tratamento pode solicitar a um progenitor ou um tutor o pagamento de 0,01 EUR através de transferência bancária, incluindo uma breve confirmação no espaço para observações da transação que o titular da conta é o titular da responsabilidade parental em relação ao utilizador. Quando adequado, deve ser disponibilizado um método alternativo de verificação para impedir o tratamento discriminatório indevido de pessoas que não tenham conta bancária.

O GT29 reconhece que pode haver casos em que a verificação seja difícil (por exemplo, quando as crianças que estão a dar consentimento ainda não estabeleceram uma «pegada» em termos de identidade ou quando a responsabilidade parental não pode ser verificada facilmente). Esta questão pode ser tida em conta quando for necessário decidir quais são os esforços razoáveis, mas é de esperar que os responsáveis pelo tratamento sujeitem os processos que utilizam e a tecnologia disponível a uma revisão constante.

No que diz respeito à autonomia do titular dos dados para dar consentimento para o tratamento dos seus dados pessoais e ter controlo total sobre o tratamento, o consentimento dado por um titular da responsabilidade parental ou autorizado por um titular da responsabilidade parental para o tratamento dos dados pessoais das crianças pode ser confirmado, modificado ou retirado assim que o titular dos dados atinja a idade para dar consentimento digital.

Na prática, significa isto que, se a criança não agir, o consentimento dado pelo titular da responsabilidade parental ou autorizado por um titular da responsabilidade parental para o tratamento dos dados pessoais antes da idade para o consentimento digital continuará a ser um fundamento válido para o tratamento.

Após alcançar a idade para dar consentimento digital, a criança terá a possibilidade de ela própria retirar o consentimento, em consonância com o artigo 7.º, n.º 3. Em conformidade com os princípios da lealdade e da responsabilização, o responsável pelo tratamento deve informar a criança acerca desta possibilidade[67].

É importante realçar que, em conformidade com o considerando 38, o consentimento dado pelo progenitor ou tutor não é necessário no contexto de serviços de prevenção ou aconselhamento oferecidos diretamente a uma criança. Por exemplo, a prestação de serviços de proteção de crianças oferecidos em linha a uma criança através de um serviço de conversação em linha não exige autorização parental prévia.

Por último, o RGPD determina que as regras relativas aos requisitos de autorização parental em relação a menores não interferem com «o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos do contrato em relação a uma criança». Por conseguinte, os requisitos para obter um consentimento válido para a utilização de dados acerca de crianças fazem parte de um quadro jurídico que deve ser considerado diferente do direito contratual nacional. Assim sendo, as presentes orientações não abordam a questão de saber se é lícito para um menor celebrar contratos em linha. Estes dois regimes jurídicos podem ser aplicáveis em simultâneo e o âmbito do RGPD não inclui a harmonização das disposições nacionais de direito contratual.

7.2. Investigação científica

A definição de fins de investigação científica tem ramificações consideráveis no âmbito das atividades de tratamento de dados que o responsável pelo tratamento pode realizar. A expressão

[67] Além disso, os titulares dos dados devem conhecer o direito a ser esquecido previsto no artigo 17.º, que é particularmente pertinente no caso do consentimento dado quando o titular dos dados ainda era uma criança, ver considerando 63.

«*investigação científica*» não se encontra definida no RGPD. O considerando 159 determina que: «*[...] Para efeitos do presente regulamento, o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato. [...]*». Contudo, o GT29 considera que a noção não pode estender-se para além do seu significado comum e entende que «*investigação científica*» neste contexto significa um projeto de investigação criado de acordo com as normas metodológicas e éticas aplicáveis em cada setor, em conformidade com as boas práticas.

Se o consentimento for o fundamento jurídico para realizar investigações em conformidade com o RGPD, o referido consentimento para a utilização de dados pessoais deve distinguir-se dos outros requisitos do consentimento que servem de referência ética ou dever processual. É possível encontrar um exemplo de um destes deveres processuais, em que o processo se baseia não no consentimento mas noutra base jurídica, no Regulamento Ensaios Clínicos. No contexto das normas de proteção de dados, esta última forma de consentimento pode ser considerada uma garantia adicional[68]. Ao mesmo tempo, o RGPD não restringe a aplicação do artigo 6.º apenas ao consentimento no que diz respeito ao tratamento de dados para fins de investigação. Desde que existam garantias adequadas, tais como os requisitos do artigo 89.º, n.º 1, e que o tratamento seja leal, lícito, transparente e respeite as normas de minimização de dados e os direitos individuais, podem ser invocados outros fundamentos legais, como o artigo 6.º, n.º 1, alíneas e) ou f)[69]. Algo que também é aplicável às categorias especiais de dados nos termos da exceção prevista no artigo 9.º, n.º 2, alínea j)[70].

O considerando 33 parece introduzir alguma flexibilidade ao grau de especificação e granularidade do consentimento no contexto da investigação científica. O considerando 33 determina: «*Muitas vezes não é possível identificar na totalidade a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.*»

Em primeiro lugar, importa referir que o considerando 33 não exclui a aplicação das obrigações inerentes ao requisito de consentimento específico. Assim, em princípio, os projetos de investigação científica só podem incluir dados pessoais com base no consentimento se tiverem uma finalidade bem definida. Nos casos em que as finalidades do tratamento dos dados no âmbito de um projeto de investigação científica não podem ser especificadas à partida, o considerando 33 permite que, excecionalmente, a finalidade seja descrita a nível mais geral.

[68] Ver também considerando 161 do RGPD.
[69] O artigo 6.º, n.º 1, alínea c), também pode ser aplicável a partes das operações de tratamento especificamente exigidas por lei, tais como a recolha de dados fiáveis e sólidos de acordo com o protocolo aprovado pelo Estado-Membro ao abrigo do Regulamento Ensaios Clínicos.
[70] Os ensaios realizados aos medicamentos podem realizar-se com base no direito da UE ou no direito nacional, nos termos do artigo 9.º, n.º 2, alínea i).

Considerando as condições apertadas do artigo 9.º do RGPD, relativo ao tratamento de categorias especiais de dados, o GT29 refere que, quando as categorias especiais de dados são tratadas com base no consentimento explícito, a aplicação da flexibilidade do considerando 33 ficará sujeita a uma interpretação mais restritiva e exigirá um nível mais elevado de escrutínio.

Quando considerado no seu todo, o RGPD não pode ser interpretado como um ato que permite a um responsável pelo tratamento contornar o princípio-chave da especificação das finalidades em relação às quais solicita o consentimento do titular dos dados.
Quando as finalidades da investigação não podem ser totalmente especificadas, o responsável pelo tratamento deve tentar encontrar outras formas de assegurar que o espírito dos requisitos do consentimento está salvaguardado, permitindo por exemplo, que os titulares dos dados deem o seu consentimento para uma finalidade de investigação em termos mais gerais e para etapas específicas de um projeto de investigação que já se sabe à partida que vão ocorrer. À medida que a investigação avança, o consentimento para etapas subsequentes do projeto pode ser obtido antes do início da etapa seguinte. Porém, este consentimento deve manter-se em consonância com as normas éticas aplicáveis à investigação científica.

Além disso, o responsável pelo tratamento pode aplicar outras garantias nestes casos. O artigo 89.º, n.º 1, por exemplo, realça a necessidade de haver garantias nas atividades de tratamento de dados com finalidades científicas, históricas ou estatísticas. Estas finalidades estão sujeitas «*a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados*». A minimização, anonimização e segurança dos dados são referidas como possíveis garantias[71]. A anonimização é a solução preferida quando a finalidade da investigação pode ser alcançada sem o tratamento de dados pessoais.

A transparência é uma garantia adicional quando as circunstâncias da investigação não permitem a obtenção de consentimento específico. A inexistência de especificação da finalidade pode ser compensada pelo fornecimento regular de informações sobre a evolução da finalidade, por parte dos responsáveis pelo tratamento, à medida que o projeto de investigação avança, para que, com o tempo, o consentimento possa ser o mais específico possível. Nestes casos, o titular dos dados consegue pelo menos compreender em termos básicos a situação, podendo assim avaliar se quer ou não exercer, por exemplo, o direito de retirada do consentimento nos termos do artigo 7.º, n.º 3[72].

---

[71] Ver, por exemplo, o considerando 156. O tratamento de dados pessoais para fins científicos também deve cumprir outra legislação aplicável, nomeadamente em matéria de ensaios clínicos, ver o considerando 156, que refere o Regulamento (UE) n.º 536/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos ensaios clínicos de medicamentos para uso humano. Ver também o Parecer 15/2011 do GT29 sobre a definição de consentimento (WP 187), p. 7: *«Para além do mais, a obtenção de consentimento não exonera o responsável pelo tratamento das obrigações estabelecidas no artigo 6.º relativas à lealdade, necessidade e proporcionalidade, assim como à qualidade dos dados. «Por exemplo, mesmo que o tratamento de dados seja baseado no consentimento da pessoa em causa, este consentimento não legitimaria uma recolha de dados excessiva em relação ao fim em causa.» […] Por princípio, o consentimento não devia ser visto como uma derrogação aos outros princípios de proteção de dados, mas sim como uma salvaguarda. O consentimento é, antes de mais, um fundamento de licitude, não afastando a aplicação de outros princípios.»*

[72] Podem ser também pertinentes outras medidas em matéria de transparência. Quando os responsáveis pelo tratamento realizam atividades de tratamento de dados para fins científicos, ainda que não possam fornecer todas as informações à partida, podem designar uma pessoa de contacto a quem os titulares dos dados possam recorrer quando têm dúvidas.

Além disso, a existência de um plano de investigação exaustivo que esteja à disposição dos titulares dos dados para referência antes de estes darem o consentimento pode ajudar a compensar a inexistência de especificação da finalidade[73]. Este plano de investigação deve especificar o mais claramente possível as questões a que a investigação pretende dar resposta e os métodos de trabalho previstos. O plano de investigação deve também contribuir para o cumprimento das disposições do artigo 7.º, n.º 1, uma vez que os responsáveis pelo tratamento necessitam de demonstrar quais as informações disponibilizadas aos titulares dos dados aquando do consentimento, por forma a comprovar que o consentimento é válido.

É importante relembrar que, quando o consentimento está a ser utilizado como fundamento legal para o tratamento, deve existir a possibilidade de o titular dos dados o retirar. O GT29 refere que a retirada do consentimento pode prejudicar alguns tipos de investigação científica que exijam que os dados estejam associados a certas pessoas. Contudo, o RGPD é claro quanto a esta matéria, o consentimento pode ser retirado e os responsáveis pelo tratamento devem agir em conformidade. Não existe exceção a este requisito para fins científicos. Se receber um pedido de retirada de consentimento, o responsável pelo tratamento deve em princípio apagar imediatamente os dados pessoais se quiser continuar a utilizar os dados para fins de investigação[74].

7.3. Direitos dos titulares dos dados

Se a atividade de tratamento de dados se basear no consentimento do titular, este facto afetará os respetivos direitos. Os titulares têm direito à portabilidade dos dados (artigo 20.º) se o tratamento se basear no consentimento. Ao mesmo tempo, o direito de oposição (artigo 21.º) não é aplicável se o tratamento se basear no consentimento, embora o direito de retirar o consentimento a qualquer momento possa ter resultado semelhante.

Os artigos 16.º a 20.º do RGPD indicam que (se o tratamento dos dados se basear no consentimento) os titulares dos dados têm o direito de apagamento quando o consentimento for retirado e os direitos de limitação, retificação e acesso[75].

8. Consentimento obtido nos termos da Diretiva 95/46/CE

Os responsáveis pelo tratamento que procedem atualmente ao tratamento de dados com base no consentimento em conformidade com as normas nacionais de proteção de dados não são automaticamente obrigados a renovar totalmente todas as relações de consentimento existentes com os titulares dos dados em preparação para o RGPD. O consentimento que foi obtido até à data continua válido na medida em que esteja em consonância com as condições do RGPD.

É importante que, antes de 25 de maio de 2018, os responsáveis pelo tratamento revejam pormenorizadamente os processos de trabalho e registos atuais, para garantirem que os

[73] Esta possibilidade pode ser encontrada no artigo 14.º, n.º 1, da atual lei finlandesa da proteção de dados (*Henkilötietolaki*, 523/1999).
[74] Ver também o Parecer 05/2014 do GT29 sobre técnicas de anonimização (WP 216).
[75] Nos casos em que determinadas atividades de tratamento de dados são limitadas em conformidade com o artigo 18.º do RGPD, pode ser necessário obter o consentimento do titular para anular as restrições.

consentimentos existentes cumprem os critérios do RGPD (ver o considerando 171 do RGPD[76]). Na prática, o RGPD eleva o nível de exigência no que toca à aplicação de mecanismos de consentimento e introduz vários novos requisitos que exigem que os responsáveis pelo tratamento alterem os mecanismos de consentimento, em vez de apenas reescreverem as políticas de privacidade[77].

Por exemplo, uma vez que o RGPD exige que um responsável pelo tratamento demonstre que obteve um consentimento válido, todos os presumíveis consentimentos em relação aos quais não tenham sido conservadas referências estarão automaticamente abaixo dos níveis de exigência do RGPD em matéria de consentimento e terão de ser renovados. De igual modo, uma vez que o RGPD exige uma «declaração ou ato positivo inequívoco», todos os presumíveis consentimentos que se tiverem baseado numa forma mais implícita de ação por parte do titular dos dados (p. ex. uma opção pré-assinalada de aceitação) também não cumprem o disposto no RGPD em matéria de consentimento.

Além disso, por forma a ser possível demonstrar que o consentimento foi obtido ou permitir manifestações de vontade mais granulares por parte dos titulares dos dados, pode haver necessidade de rever as operações e os sistemas de TI. Também devem estar disponíveis mecanismos que permitam aos titulares dos dados retirar facilmente o seu consentimento e devem ser fornecidas informações sobre como fazê-lo. Se os procedimentos existentes para obtenção e gestão do consentimento não cumprirem as normas do RGPD, os responsáveis pelo tratamento terão de obter novos consentimentos que estejam em conformidade com o RGPD.

Por outro lado, uma vez que nem todos os elementos referidos nos artigos 13.º e 14.º devem estar presentes como condição para um consentimento informado, os deveres de informação alargados previstos no RGPD não se opõem necessariamente à continuidade do consentimento que foi concedido antes da entrada em vigor do RGPD (ver página 15 acima). Nos termos da Diretiva 95/46/CE, não existia requisito de informar os titulares dos dados acerca do fundamento para efetuar o tratamento.

Se o responsável pelo tratamento verificar que o consentimento dado anteriormente nos termos da antiga legislação não cumpre as normas de consentimento do RGPD, os responsáveis pelo tratamento devem tomar medidas para cumprir essas normas, por exemplo revalidando o

[76] O considerando 171 do RGPD determina: «*A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento. Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor. «Se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento. As decisões da Comissão que tenham sido adotadas e as autorizações que tenham sido emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que forem alteradas, substituídas ou revogadas.*»

[77] Como foi mencionado na introdução, o RGPD clarifica e especifica mais pormenorizadamente os requisitos necessários para obter e comprovar o consentimento válido. Muitos dos novos requisitos assentam no Parecer 15/2011 relativo ao consentimento.

consentimento de forma a cumprir o RGPD. Nos termos do RGPD, não é possível mudar de um fundamento legal para outro. Se o responsável pelo tratamento não conseguir renovar o consentimento em conformidade com as novas normas e também não conseguir – em situação excecional – fazer a transição para uma situação conforme com o RGPD, baseando o tratamento dos dados num fundamento legal diferente, garantindo ao mesmo tempo que o tratamento continua a ser leal e responsável, as atividades de tratamento devem cessar. Em todo o caso, importa que o responsável pelo tratamento observe os princípios da licitude, lealdade e transparência aplicáveis ao tratamento.

-*-*-*-*-*-*-*-*-*-*-*-* FIM DO DOCUMENTO *-*