



Bruxelas, 10.1.2017  
COM(2017) 8 final

2017/0002 (COD)

Proposta de

**REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE**

## EXPOSIÇÃO DE MOTIVOS

### 1. CONTEXTO DA PROPOSTA

#### • **Justificação e objetivos da proposta**

O artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE), tal como introduzido pelo Tratado de Lisboa, estabelece o princípio de que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. Além disso, no artigo 16.º, n.º 2, do TFUE, o Tratado de Lisboa introduziu uma base jurídica específica para a adoção de normas em matéria de proteção de dados pessoais. O artigo 8.º da Carta dos Direitos Fundamentais da União Europeia consagra a proteção de dados pessoais como um direito fundamental.

O direito à proteção de dados pessoais também se aplica ao tratamento de dados pessoais por parte de instituições, órgãos, organismos e agências da UE. O Regulamento (CE) n.º 45/2001,<sup>1</sup> o ato principal da atual legislação da UE em matéria de proteção de dados nas instituições da UE, foi adotado em 2001 com dois objetivos: assegurar o direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais na União. O referido regulamento foi completado pela Decisão n.º 1247/2002/CE<sup>2</sup>.

Em 27 de abril de 2016, o Parlamento Europeu e o Conselho adotaram o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679], que será aplicável a partir de 25 de maio de 2018. Este regulamento estabelece que o Regulamento (CE) n.º 45/2001 seja adaptado de acordo com os princípios e normas estabelecidos no Regulamento (UE) 2016/679 para fornecer um quadro de proteção de dados sólido e coerente na União e para possibilitar que ambos os instrumentos sejam aplicados em simultâneo<sup>3</sup>.

É considerado consistente com a abordagem coerente da proteção de dados pessoais na União visando alinhar, na medida do possível, as normas de proteção de dados aplicadas pelas instituições, órgãos, organismos e agências da União com as normas de proteção de dados aplicadas a nível dos Estados-Membros. Sempre que as disposições da proposta sejam baseadas no mesmo conceito que as disposições do Regulamento (UE) 2016/679, essas duas disposições devem ser interpretadas homoganeamente, sobretudo porque o sistema da proposta deve ser considerado como equivalente ao sistema do Regulamento (UE) 2016/679<sup>4</sup>.

O reexame do Regulamento (CE) n.º 45/2001 também tem em consideração os resultados dos inquéritos e das consultas às partes interessadas, bem como o estudo de avaliação sobre a sua utilização ao longo dos últimos 15 anos.

Esta iniciativa não se enquadra no programa para a adequação e a eficácia da regulamentação (REFIT).

---

<sup>1</sup> Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados, JO L 8 de 12.1.2001.

<sup>2</sup> Decisão n.º 1247/2002/CE, de 1 de julho de 2002, relativa ao estatuto e às condições gerais de exercício de funções da autoridade europeia para a proteção de dados, JO L 183 de 12.7.2002, p. 1.

<sup>3</sup> Consultar o Regulamento (UE) 2016/679, artigo 98.º e considerando 17.

<sup>4</sup> Consultar TJUE de 9 de março de 2010, *Comissão/Alemanha*, Processo C-518/07, ECLI:EU:C:2010:125, n.ºs 26 e 28.

- **Coerência com as disposições em vigor no mesmo domínio de intervenção**

A proposta visa alinhar as disposições do Regulamento (CE) n.º 45/2001 com os princípios e normas estabelecidos no Regulamento (UE) 2016/679, a fim de estabelecer um quadro de proteção de dados sólido e coerente na União. A proposta também incorpora as normas relevantes estabelecidas no Regulamento (CE) XXXX/XX [Regulamento sobre a privacidade e as comunicações eletrónicas] no que diz respeito à proteção de equipamentos terminais dos utilizadores finais.

- **Coerência com outras políticas da União**

Não aplicável.

## **2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE**

- **Base jurídica**

A proteção de pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais é um direito fundamental estabelecido no artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia.

Esta proposta é baseada no artigo 16.º do TFUE, que constitui a base jurídica para a adoção de normas em matéria de proteção de dados. O referido artigo permite a adoção de normas relacionadas com a proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União no exercício de atividades abrangidas pelo direito da União. Também permite a adoção de normas relativas à livre circulação de dados pessoais tratados por essas instituições, órgãos, organismos e agências.

- **Subsidiariedade (no caso de competência não exclusiva)**

O objeto do presente regulamento enquadra-se no domínio da competência exclusiva da União, dado que apenas a União pode adotar normas relativas ao tratamento de dados pessoais por parte das instituições da União.

- **Proporcionalidade**

De acordo com o princípio da proporcionalidade, para atingir os objetivos básicos que garantem um nível equivalente da proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados na União, é necessário e apropriado estabelecer normas sobre o tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União. O presente regulamento não excede o necessário para atingir os objetivos preconizados, em conformidade com o artigo 5.º, n.º 4, do Tratado da União Europeia.

- **Escolha do instrumento**

Um regulamento é considerado o instrumento jurídico apropriado para definir o quadro de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados. Prevê a concessão às pessoas singulares de direitos suscetíveis de proteção judicial, especifica as obrigações em matéria de tratamento de dados dos responsáveis nesse domínio nas instituições, órgãos, organismos e agências da União. Também prevê uma autoridade independente de controlo, ou seja, a Autoridade Europeia para a Proteção de Dados, que é

responsável pela supervisão do tratamento de dados pessoais por parte das instituições, órgãos, organismos e agências da União.

### **3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS ÀS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO**

A Comissão realizou consultas às partes interessadas em 2010 e 2011, bem como uma avaliação do impacto no contexto da preparação do pacote de reforma legislativa da proteção de dados, que contribuíram para as alterações propostas ao Regulamento (CE) n.º 45/2001. Neste contexto, a Comissão também realizou um inquérito aos coordenadores da proteção de dados da Comissão<sup>5</sup>.

No que diz respeito à aplicação prática do Regulamento (CE) n.º 45/2001 pelas instituições, órgãos, organismos e agências da União, as informações foram recolhidas a partir da Autoridade Europeia para a Proteção de Dados (AEPD), de outras instituições, órgãos, organismos e agências da União, de outras DG da Comissão e de um contratante externo. Foi enviado um questionário à rede de responsáveis pela proteção de dados<sup>6</sup>.

Os responsáveis pela proteção de dados de várias instituições, órgãos, organismos e agências da União organizaram seminários sobre a reforma do Regulamento 45/2001 em 9 de julho de 2015, 22 de outubro de 2015, 19 de janeiro de 2016 e 15 de março de 2016.

Em 2013, a Comissão decidiu realizar um estudo de avaliação sobre a aplicação do Regulamento (CE) n.º 45/2001 até àquele momento, que foi encomendado a um contratante externo. Os resultados finais do estudo de avaliação (relatório final, cinco casos de estudo e análise artigo a artigo) foram submetidos à apreciação da Comissão em 8 de junho de 2015<sup>7</sup>.

A avaliação demonstrou que o sistema de governação estruturado em torno dos responsáveis pela proteção de dados e da AEPD é eficaz. Considerou que a partilha de competências entre os responsáveis pela proteção de dados e a AEPD é clara e equilibrada e que dispõem de um conjunto de competências adequadas. Contudo, podem surgir dificuldades devido a uma falta de autoridade decorrente do apoio insuficiente da hierarquia aos responsáveis pela proteção de dados.

O estudo de avaliação indicou que o Regulamento (CE) n.º 45/2001 podia ser aplicado de forma mais rigorosa através do recurso a sanções por parte da AEPD. Uma utilização mais determinada dos poderes da respetiva autoridade de controlo poderia resultar numa melhor aplicação das normas de proteção de dados. Outra conclusão foi que os responsáveis pelos dados devem adotar um método de gestão dos riscos e efetuar avaliações de riscos antes de realizar operações de tratamento, de forma a aplicar da melhor forma os requisitos de conservação de dados e de segurança.

O estudo também assinalou que as normas do capítulo IV do Regulamento (CE) n.º 45/2001 sobre o sector das telecomunicações estão desatualizadas e que é necessário alinhar esse capítulo com a Diretiva sobre a privacidade e as comunicações eletrónicas. De acordo com o

---

<sup>5</sup> Ver [http://ec.europa.eu/justice/data-protection/reform/index\\_en.htm](http://ec.europa.eu/justice/data-protection/reform/index_en.htm)

<sup>6</sup> Consultar o relatório geral da Autoridade Europeia para a Proteção de Dados sobre «Measuring compliance with Regulation (EC) 45/2001 in EU institutions (‘Survey 2013’)» e Parecer 3/2015 sobre «Europe’s big opportunity: EDPS recommendations on the EU’s options for data protection reform».

<sup>7</sup> «JUST/2013/FRAC/FW/0157/A4 in the context of the multiple framework contract JUST/2011/EVAL/01 (RS 2013/05) - Evaluation Study on Regulation (EC) 45/2001», por Ernst and Young, disponível em [http://ec.europa.eu/newsroom/just/item-detail.cfm?item\\_id=51087](http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=51087)

estudo de avaliação, existe ainda a necessidade de clarificar algumas definições essenciais do Regulamento (CE) n.º 45/2001. Estas definições incluem a identificação dos responsáveis pelos dados nas instituições, órgãos, organismos e agências da União, a definição dos destinatários e a extensão da obrigação de confidencialidade a subcontratantes externos.

O estudo de avaliação também mencionou a necessidade de simplificar o regime de notificações e controlos prévios para aumentar a eficácia e reduzir os encargos administrativos.

O avaliador efetuou um inquérito em linha em 64 instituições, órgãos, organismos e agências da União. Responderam às perguntas do inquérito 422 funcionários responsáveis pelo tratamento de dados, 73 responsáveis pela proteção de dados, 118 coordenadores da proteção de dados e 109 representantes de empresas de tecnologias da informação. O avaliador também efetuou uma série de entrevistas às partes interessadas. Em 26 de março de 2015, o avaliador e a Comissão organizaram uma reunião final na qual participaram vários responsáveis pelos dados, responsáveis pela proteção de dados, coordenadores da proteção de dados, representantes de empresas de tecnologias da informação e representantes da AEPD.

- **Obtenção e utilização de competências especializadas**

Consultar o estudo de avaliação no ponto anterior.

- **Avaliação de impacto**

O impacto da presente proposta incide sobretudo nas instituições, órgãos, organismos e agências da União. Esta situação foi confirmada por informações recolhidas junto da AEPD, de outras instituições, órgãos, organismos e agências da União, das DG da Comissão e do contratante externo. Além disso, o impacto das novas obrigações resultantes do Regulamento (UE) 2016/679, com o qual o presente regulamento deve ser alinhado, foi avaliado no contexto dos trabalhos preliminares respeitantes a este último instrumento. por conseguinte, é desnecessária uma avaliação de impacto específica para o presente regulamento.

- **Adequação e simplificação da legislação**

Não aplicável.

- **Direitos fundamentais**

O direito à proteção de dados pessoais encontra-se estabelecido no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia (Carta), no artigo 16.º do TFUE e no artigo 8.º da Convenção Europeia dos Direitos do Homem. Conforme salientado pelo Tribunal de Justiça da União Europeia<sup>8</sup>, o direito à proteção de dados pessoais não é absoluto, mas deve ser considerado em relação à sua função na sociedade<sup>9</sup>. A proteção de dados também está profundamente relacionada com o respeito pela vida privada e familiar, protegido pelo artigo 7.º da Carta.

---

<sup>8</sup> TJUE, 9 de novembro de 2010, *Volker und Markus Schecke e Eifert*, Processos apensos C-92/09 e C-93/09, ECLI:EU:C:2009:284, n.º 48.

<sup>9</sup> Nos termos do artigo 52.º, n.º 1, da Carta, podem ser impostas restrições ao exercício do direito à proteção de dados desde que sejam previstas por lei, respeitem o conteúdo essencial desse direito e liberdade e, na observância do princípio da proporcionalidade, só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União Europeia, ou à necessidade de proteção dos direitos e liberdades de terceiros.

A presente proposta estabelece normas para a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados.

Outros direitos fundamentais consagrados na Carta suscetíveis de serem afetados são: a liberdade de expressão (artigo 11.º); o direito à propriedade e, em particular, à proteção da propriedade intelectual (artigo 17.º, n.º 2); a proibição de discriminação em razão da raça, origem étnica, características genéticas, religião ou convicções, opiniões políticas ou outras, deficiência ou orientação sexual (artigo 21.º); os direitos da criança (artigo 24.º); o direito a um elevado nível de proteção da saúde humana (artigo 35.º); o direito de acesso aos documentos (artigo 42.º); e o direito à ação e a um tribunal imparcial (artigo 47.º).

#### **4. INCIDÊNCIA ORÇAMENTAL**

Consultar a ficha financeira apresentada em anexo.

#### **5. OUTROS ELEMENTOS**

- **Planos de execução e acompanhamento, avaliação e prestação de informações**

Não aplicável.

- **Documentos explicativos (para as diretivas)**

Não aplicável.

#### **CAPÍTULO I – DISPOSIÇÕES GERAIS**

O artigo 1.º define o objeto do regulamento e, tal como no artigo 1.º do Regulamento (CE) n.º 45/2001, estabelece os dois objetivos do regulamento: a proteção do direito fundamental à proteção de dados e assegurar a livre circulação de dados pessoais na União. Prevê igualmente as principais atribuições da Autoridade Europeia para a Proteção de Dados.

O artigo 2.º determina o âmbito de aplicação do regulamento: deve aplicar-se ao tratamento de dados pessoais por meios automatizados ou outros, por todas as instituições e organismos da União, na medida em que esse tratamento seja efetuado para o exercício de atividades abrangidas total ou parcialmente pelo direito da União. O âmbito de aplicação material do presente regulamento é neutro do ponto de vista tecnológico. A proteção de dados pessoais aplica-se ao seu tratamento por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros.

O artigo 3.º contém as definições dos termos utilizados no regulamento. Para além das definições de «instituições e organismos da União», «responsável pelo tratamento», «utilizador» e «lista», que são específicas do presente regulamento, os termos utilizados no presente regulamento são definidos no Regulamento (UE) 2016/679, no Regulamento (UE) 0000/00 [novo regulamento sobre a privacidade e as comunicações eletrónicas], na Diretiva 00/0000/UE [Diretiva que estabelece o Código Europeu de Comunicações Eletrónicas] e na Diretiva da Comissão 2008/63/CE.

#### **CAPÍTULO II – PRINCÍPIOS**

O artigo 4.º enuncia os princípios relativos ao tratamento de dados pessoais, que correspondem aos previstos no artigo 5.º do Regulamento (UE) 2016/679. Comparativamente ao Regulamento (CE) n.º 45/2001, acrescenta os novos princípios de transparência, de integridade e confidencialidade.

O artigo 5.º é baseado no artigo 6.º do Regulamento (UE) 2016/679 e estabelece os critérios para o tratamento lícito, com a única exceção dos critérios do interesse legítimo do responsável pelo tratamento, que não são aplicáveis ao sector público e, como tal, não se aplicam às instituições e organismos da União. O artigo 5.º retoma os critérios já estabelecidos ao abrigo do artigo 5.º do Regulamento (CE) n.º 45/2001.

O artigo 6.º clarifica as condições que determinam o tratamento para outras finalidades compatíveis, em conformidade com o artigo 6.º, n.º 4, do Regulamento (UE) 2016/679. Comparativamente ao artigo 6.º do Regulamento (CE) n.º 45/2001, esta nova disposição confere mais flexibilidade e segurança jurídica no que se refere ao tratamento posterior para fins de compatibilidade.

O artigo 7.º clarifica, de acordo com o artigo 7.º do Regulamento (UE) 2016/679, as condições para que o consentimento seja válido enquanto fundamento jurídico para o tratamento lícito.

O artigo 8.º estabelece, de acordo com o artigo 8.º do Regulamento (UE) 2016/679, condições suplementares aplicáveis à licitude do tratamento de dados pessoais de crianças em relação aos serviços da sociedade da informação que lhes são diretamente propostos. Estabelece os 13 anos como a idade mínima de uma criança para que o consentimento seja válido.

O artigo 9.º estabelece, de acordo com o artigo 8.º do Regulamento (CE) n.º 45/2001, normas que fornecem um nível específico de proteção na transmissão de dados pessoais a destinatários, diferentes das instituições e organismos da União, estabelecidos na União e sujeitos ao Regulamento (UE) 2016/679 ou à Diretiva (UE) 2016/680. Clarifica que, nos casos em que o responsável pelo tratamento inicia a transmissão, deve demonstrar a necessidade e a proporcionalidade da transmissão.

O artigo 10.º estabelece a proibição geral de tratamento de categorias especiais de dados pessoais e as exceções a esta regra geral, com base no artigo 9.º do Regulamento (UE) 2016/679, e adicionalmente com base no artigo 10.º do Regulamento (CE) n.º 45/2001.

O artigo 11.º estabelece, de acordo com o artigo 10.º do Regulamento (UE) 2016/679 e, em conformidade com o artigo 10.º, n.º 5, do Regulamento (CE) n.º 45/2001, as condições para o tratamento de dados pessoais relacionados com condenações penais e infrações.

O artigo 12.º clarifica as obrigações de informação pelo responsável pelo tratamento para com o titular dos dados, em conformidade com o artigo 11.º do Regulamento (UE) 2016/679, desde que, quando os dados pessoais tratados por um responsável não permitirem a este último identificar uma pessoa singular, esse responsável não deve ser obrigado a obter informações adicionais para identificar os dados com o único objetivo de dar cumprimento a qualquer disposição do presente regulamento. Todavia, o responsável pelo tratamento não deve recusar receber informações suplementares fornecidas pelo titular dos dados no intuito de apoiar o exercício dos seus direitos.

O artigo 13.º estabelece, com base no artigo 89.º, n.º 1, do Regulamento (UE) 2016/679, as normas sobre garantias relativas ao tratamento para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos.

### *CAPÍTULO III - DIREITOS DO TITULAR DOS DADOS*

#### *Secção 1 – Transparência e regras*

O artigo 14.º introduz, com base no artigo 12.º do Regulamento (UE) 2016/679, a obrigação de os responsáveis pelo tratamento fornecerem informações transparentes, de fácil acesso e compreensão, bem como os procedimentos e mecanismos para o exercício dos direitos pelo titular dos dados, incluindo, quando apropriado, meios para pedidos por via eletrónica que

requeiram resposta ao interessado dentro de um prazo fixado, e os motivos da recusa. Dado que as instituições e organismos da União não devem cobrar, em circunstância alguma, taxas relativas a custos administrativos para o fornecimento de informações, esta possibilidade não foi retomada do Regulamento (UE) 2016/679.

## Secção 2 – Informação e acesso aos dados pessoais

O artigo 15.º especifica as obrigações de informação pelo responsável pelo tratamento para com o titular dos dados quando os dados pessoais são recolhidos junto do titular, com base no artigo 13.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 11.º do Regulamento (CE) n.º 45/2001, ao fornecer informações ao titular dos dados, incluindo sobre o período de conservação, o direito de apresentar uma reclamação e em relação a transferências internacionais.

O artigo 16.º especifica mais em pormenor, com base no artigo 14.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 12.º do Regulamento (CE) n.º 45/2001, as obrigações de informação pelo responsável pelo tratamento para com o titular dos dados quando os dados pessoais não foram obtidos do titular dos dados, fornecendo informação à fonte a partir da qual os dados são gerados. Também retoma as derrogações previstas no Regulamento (UE) 2016/679, por exemplo a inexistência de qualquer obrigação caso o titular dos dados já tenha tal informação, a prestação dessa informação se revele impossível ou implique um esforço desproporcionado para o responsável pelo tratamento, nos casos em que os dados pessoais devem manter-se confidenciais em virtude de uma obrigação de sigilo profissional regulada pelo direito da União ou o registo ou a comunicação se encontre expressamente previsto por lei. Tal pode ser aplicado, por exemplo, aos serviços competentes da segurança social ou de saúde.

O artigo 17.º prevê, em conformidade com o artigo 15.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 13.º do Regulamento (CE) n.º 45/2001, o direito de acesso do titular dos dados aos seus dados pessoais, e acrescenta novos elementos, tais como a obrigação de informar os titulares dos dados sobre o período de conservação, os direitos de retificação, de apagamento e de apresentação de reclamação.

## Secção 3 – Retificação e apagamento

O artigo 18.º estabelece o direito do titular dos dados à retificação, com base no artigo 16.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 14.º do Regulamento (CE) n.º 45/2001.

O artigo 19.º estabelece, em conformidade com o artigo 17.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 16.º do Regulamento (CE) n.º 45/2001, o direito do titular dos dados a ser esquecido e ao apagamento. Prevê as condições sobre o direito a ser esquecido, incluindo a obrigação do responsável pelo tratamento que tornou públicos os dados pessoais de informar os terceiros sobre o pedido do interessado de apagamento de quaisquer ligações para esses dados, ou cópias ou reproduções que tenham sido efetuadas.

O artigo 20.º introduz o direito à limitação do tratamento em determinados casos, evitando o termo ambíguo de «bloqueio» utilizado no Regulamento (CE) n.º 45/2001 e garantindo a coerência com a nova terminologia ao abrigo do artigo 18.º do Regulamento (UE) 2016/679.

O artigo 21.º prevê, com base no artigo 19.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 17.º do Regulamento (CE) n.º 45/2001, a obrigação do responsável pelo tratamento de comunicar aos destinatários aos quais os dados pessoais foram divulgados qualquer retificação ou apagamento dos dados pessoais ou limitação, exceto se for considerado impossível ou envolver um esforço desproporcionado. O responsável pelo tratamento também deve informar o titular dos dados sobre esses destinatários, caso o solicite.

O artigo 22.º introduz, em conformidade com o artigo 20.º do Regulamento (UE) 2016/679, o direito do titular dos dados à portabilidade dos dados, ou seja, o direito a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento, ou a que esses dados pessoais sejam transmitidos diretamente a outro responsável pelo tratamento, sempre que seja tecnicamente possível. Como condição prévia, e para melhorar o acesso das pessoas singulares aos dados pessoais que lhe digam respeito, prevê o direito de obter esses dados do responsável pelo tratamento num formato estruturado, de uso corrente e de leitura automática. Este direito só se aplica nos casos em que o tratamento é baseado no consentimento do titular dos dados ou num contrato celebrado por esse titular.

#### Secção 4 - Direito de oposição e decisões individuais automatizadas

O artigo 23.º prevê o direito de oposição do titular dos dados, com base no artigo 21.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 18.º do Regulamento (CE) n.º 45/2001.

O artigo 24.º diz respeito ao direito de o titular dos dados não ser objeto de uma medida com base somente no tratamento automatizado, incluindo definição de perfis, em consonância com o artigo 22.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 19.º do Regulamento (CE) n.º 45/2001.

#### Secção 5 - Limitações

O artigo 25.º permite limitações dos direitos do titular dos dados estabelecidos nos artigos 14.º a 22.º, e nos artigos 34.º e 38.º, e dos princípios estabelecidos no artigo 4.º (na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 14.º a 22.º). Essas limitações devem ser estabelecidas em atos legais adotados com base nos Tratados ou nos regulamentos internos das instituições e organismos da União. Caso não seja fornecida uma possibilidade dessa limitação nos atos jurídicos adotados com base nos Tratados ou nos regulamentos internos das instituições e organismos da União, os últimos poderão impor uma restrição *ad hoc*, desde que respeite a essência dos direitos e liberdades fundamentais, em relação a uma operação de tratamento específica, e seja uma medida necessária e proporcionada numa sociedade democrática para salvaguardar um ou mais objetivos que permitem as restrições aos direitos dos titulares dos dados. Esta abordagem é conforme com o artigo 23.º do Regulamento (UE) 2016/679, mas em contraste com este último artigo e em conformidade com o artigo 20.º do Regulamento (CE) n.º 45/2001, a disposição não confere a possibilidade de restringir o direito de oposição e o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado. Os requisitos das limitações estão em conformidade com a Carta dos Direitos Fundamentais e a Convenção Europeia dos Direitos do Homem, conforme interpretado pelo Tribunal de Justiça da União Europeia e o Tribunal Europeu dos Direitos do Homem, respetivamente.

### CAPÍTULO IV – RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE

#### Secção 1 – Obrigações gerais

O artigo 26.º tem por base o artigo 24.º do Regulamento (UE) 2016/679 e introduz o «princípio da responsabilidade», ao descrever a obrigação de responsabilidade do responsável pelo tratamento para dar cumprimento ao presente regulamento e comprovar a sua observância, incluindo através da adoção de medidas técnicas e organizativas apropriadas e, quando adequado, de políticas e procedimentos internos para garantir essa conformidade. O artigo 24.º, n.º 3, do Regulamento (UE) 2016/679 não foi retomado nesta disposição, dado que as instituições e organismos da União não devem aderir a códigos de conduta ou procedimentos de certificação.

O artigo 27.º estabelece, em conformidade com o artigo 25.º do Regulamento (UE) 2016/679, as obrigações do responsável pelo tratamento decorrentes dos princípios de proteção de dados desde a conceção e por defeito.

O artigo 28.º relativo aos responsáveis conjuntos pelo tratamento tem por base o artigo 26.º do Regulamento (UE) 2016/679 e visa clarificar as responsabilidades dos responsáveis conjuntos pelo tratamento - sejam estes as instituições ou organismos da União - relativamente às relações internas e face ao titular dos dados. Esta disposição regula a situação em que todos os responsáveis conjuntos pelo tratamento são abrangidos pelo mesmo regime jurídico (o presente regulamento) e outros por um instrumento jurídico diferente [Regulamento (UE) 2016/679, Diretiva (UE) 2016/680, Diretiva (UE) 2016/681 e outros regimes específicos de proteção de dados relacionados com as instituições ou organismos da União].

O artigo 29.º tem por base o artigo 28.º do Regulamento (UE) 2016/679 e ainda desenvolve o artigo 23.º do Regulamento (CE) n.º 45/2001, e visa clarificar a posição e as obrigações dos subcontratantes, incluindo a determinação de que um subcontratante que infringe o regulamento ao determinar as finalidades e os meios do tratamento deve ser considerado responsável pelo tratamento em relação a esse tratamento.

O artigo 30.º relativo ao tratamento sob a autoridade do responsável pelo tratamento e do subcontratante é baseado no artigo 29.º do Regulamento (UE) 2016/679, e estabelece uma proibição para o subcontratante ou qualquer pessoa que atua sob a autoridade do responsável pelo tratamento ou do subcontratante, e que tenha acesso a dados pessoais para proceder ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

O artigo 31.º tem por base o artigo 30.º do Regulamento (UE) 2016/679, e introduz a obrigação dos responsáveis pelo tratamento e subcontratantes de manter a documentação das operações de tratamento sob a sua responsabilidade, ao invés de uma notificação prévia da AEPD, conforme exigido pelo artigo 25.º do Regulamento (CE) n.º 45/2001 e do registo do encarregado da proteção de dados. Em contraste com o Regulamento (UE) 2016/679, esta disposição não faz referência aos representantes, uma vez que as instituições da União não têm representantes e terão sempre encarregados da proteção de dados. As referências a transferências com base em derrogações para situações específicas como no Regulamento (UE) 2016/679 não foram mantidas, uma vez que esses tipos de transferências não são previstos no presente regulamento. A obrigação de manter um registo das atividades de tratamento pode ser centralizada ao nível de uma instituição ou organismo da União. Nesse caso, as instituições e organismos da União têm a possibilidade de manter os seus registos de atividades de tratamento na forma de um registo de acesso público.

O artigo 32.º clarifica, com base no artigo 31.º do Regulamento (UE) 2016/679, as obrigações das instituições e organismos da União a nível da cooperação com a AEPD.

## Secção 2 – Segurança dos dados pessoais e confidencialidade das comunicações eletrónicas

O artigo 33.º obriga, em conformidade com o artigo 32.º do Regulamento (UE) 2016/679 e adicionalmente com base no artigo 22.º do Regulamento (CE) n.º 45/2001, o responsável pelo tratamento a aplicar medidas apropriadas para a segurança do tratamento, alargando essa obrigação a subcontratantes, independentemente do contrato com o responsável pelo tratamento.

O artigo 34.º tem por base o artigo 36.º do Regulamento (CE) n.º 45/2001 e garante a confidencialidade das comunicações eletrónicas dentro das instituições e organismos da União.

O artigo 35.º tem por base a prática existente das instituições e organismos da União e protege a informação relacionada com o equipamento terminal dos utilizadores finais que acedem a sítios Web e aplicações móveis acessíveis ao público proporcionados pelas instituições e organismos da União, em conformidade com o Regulamento (UE) XXXX/XX [novo Regulamento sobre a privacidade e as comunicações eletrónicas], sobretudo o artigo 8.º.

O artigo 36.º é baseado no artigo 38.º do Regulamento (CE) n.º 45/2001 e protege os dados pessoais mantidos em listas públicas e privadas das instituições e organismos da União.

Os artigos 37.º e 38.º introduzem uma obrigação de notificar as violações de dados pessoais, em conformidade com os artigos 33.º e 34.º do Regulamento (UE) 2016/679.

### Secção 3 - Avaliação de impacto sobre a proteção de dados e consulta prévia

O artigo 39.º tem por base o artigo 35.º do Regulamento (UE) 2016/679 e introduz a obrigação dos responsáveis pelo tratamento e dos subcontratantes de efetuarem uma avaliação de impacto sobre a proteção de dados antes das operações de tratamento, que são suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares. Esta obrigação é aplicada, em particular, no caso da avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, que são baseados no tratamento automatizado, incluindo a definição de perfis, as operações de tratamento em grande escala de categorias especiais de dados ou o controlo sistemático de zonas acessíveis ao público em grande escala.

O artigo 40.º é baseado no artigo 36.º do Regulamento (UE) 2016/679 e está relacionado com os casos em que a autorização por parte da AEPD e a sua consulta é obrigatória antes do tratamento. Contudo, o n.º 1 do artigo 40.º reproduz o considerando 94 do Regulamento (UE) 2016/679 e visa clarificar o âmbito da obrigação da consulta.

### Secção 4 - Informação e consulta legislativa

O artigo 41.º determina que as instituições e organismos da União devem informar a AEPD ao elaborarem as medidas administrativas e os regulamentos internos respetivos ao tratamento de dados pessoais.

O artigo 42.º prevê que a Comissão deve consultar a AEPD, após a adoção das propostas de um ato legislativo e das recomendações ou propostas ao Conselho, nos termos do artigo 218.º do TFUE, ou durante a preparação de atos delegados ou atos de execução que têm um impacto sobre a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais. Quando esses atos têm uma importância particular para a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão pode também consultar o Comité Europeu para a Proteção de Dados. Nesses casos, ambas as entidades devem coordenar o seu trabalho para emitirem uma opinião conjunta. É estabelecido um limite temporal de oito semanas para a emissão do parecer nos casos supramencionados, com derrogações previstas para casos urgentes e quando for apropriado, por exemplo quando a Comissão está a preparar atos delegados e atos de execução.

### Secção 5 – Dever de resposta a alegações

O artigo 43.º estabelece a obrigação de os responsáveis pelo tratamento e o subcontratante reagirem às alegações após a AEPD ter decidido remeter-lhes uma questão.

### Secção 6 – Encarregado da proteção de dados

O artigo 44.º tem por base o artigo 37.º, n.º 1, alínea a), do Regulamento (UE) 2016/679 e o artigo 24.º do Regulamento (CE) n.º 45/2001, e prevê a designação de um encarregado da proteção de dados obrigatório para as instituições e organismos da União.

O artigo 45.º tem por base o artigo 38.º do Regulamento (UE) 2016/679 e o artigo 24.º do Regulamento (CE) n.º 45/2001, e estabelece a posição do encarregado da proteção de dados.

O artigo 46.º tem por base o artigo 39.º do Regulamento (UE) 2016/679 e o artigo 24.º do Regulamento (CE) n.º 45/2001, bem como e os n.ºs 2 e 3 do anexo deste último regulamento, e prevê as funções principais do encarregado da proteção de dados.

## CAPÍTULO V – TRANSFERÊNCIAS DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

O artigo 47.º tem por base e aprofunda o artigo 9.º do Regulamento (CE) n.º 45/2001, bem como estabelece o princípio geral, em conformidade com o artigo 44.º do Regulamento (UE) 2016/679, de que a conformidade com outras disposições do presente regulamento e as condições estabelecidas no capítulo V são obrigatórias para todas as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo para transferências ulteriores de dados pessoais do país terceiro ou de uma organização internacional para outro país terceiro ou para outra organização internacional.

O artigo 48.º estabelece que uma transferência de dados pessoais para um país terceiro ou organização internacional pode ocorrer quando a Comissão tiver decidido, em conformidade com o artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, que é garantido um nível adequado de proteção no país terceiro, num território ou num ou mais sectores específicos dentro desse país terceiro ou dentro da organização internacional e que os dados pessoais são transferidos unicamente para permitir o desempenho de funções da competência do responsável pelo tratamento. Os n.ºs 2 e 3 deste artigo foram transpostos do artigo 9.º do Regulamento (CE) n.º 45/2001, uma vez que são elementos úteis para o controlo do nível de proteção em países terceiros e organizações internacionais.

O artigo 49.º tem por base o artigo 46.º do Regulamento (UE) 2016/679 e exige, para as transferências para países terceiros quando não tenha sido adotada pela Comissão uma decisão sobre a adequação do nível de proteção, que sejam apresentadas garantias adequadas, em especial cláusulas-tipo de proteção de dados e cláusulas contratuais. Podem ser utilizadas regras vinculativas aplicáveis às empresas, códigos de conduta e procedimentos de certificação, em conformidade com o Regulamento (UE) 2016/679, por subcontratantes diferentes de instituições e organismos da União. O n.º 4 deste artigo prevê a obrigação de instituições e organismos da União informarem a AEPD sobre as categorias de casos em que aplicaram este artigo, correspondendo ao artigo 9.º, n.º 8, do Regulamento (CE) n.º 45/2001, sendo mantido devido à sua especificidade. O n.º 5 tem por base a manutenção das autorizações em vigor estabelecidas no artigo 46.º, n.º 5, do Regulamento (UE) 2016/679.

O artigo 50.º clarifica, em conformidade com o artigo 48.º do Regulamento (UE) 2016/679, que as decisões judiciais ou as decisões de autoridades administrativas de países terceiros que exijam uma transferência ou divulgação de dados pessoais só são reconhecidas ou executadas se tiverem por base um acordo internacional, designadamente um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União, sem prejuízo de outros motivos de transferência nos termos deste capítulo.

O artigo 51.º tem por base o artigo 49.º do Regulamento (UE) 2016/679, e define e clarifica as derrogações para uma transferência de dados. Esta disposição é especialmente aplicável às transferências de dados exigidas e necessárias por razões de proteção de interesses públicos importantes, por exemplo em caso de transferências internacionais de dados que envolvem autoridades da concorrência, fiscais ou aduaneiras, ou entre serviços competentes em matéria de segurança social ou de gestão das atividades da pesca. O n.º 5 prevê a obrigação de

informar a AEPD das categorias de casos nos quais foram invocadas derrogações para uma transferência, correspondendo ao atual artigo 9.º, n.º 8, do Regulamento (CE) n.º 45/2001.

O artigo 52.º tem por base o artigo 50.º do Regulamento (UE) 2016/679, e prevê expressamente os procedimentos de cooperação internacional para a proteção de dados entre a AEPD, em cooperação com a Comissão e o Comité Europeu para a Proteção de Dados, e as autoridades de controlo de países terceiros.

#### *CAPÍTULO VI - AUTORIDADE EUROPEIA PARA A PROTECÇÃO DE DADOS*

O artigo 53.º tem por base o artigo 41.º do Regulamento (CE) n.º 45/2001, e diz respeito ao estabelecimento da AEPD.

O artigo 54.º tem por base o artigo 42.º do Regulamento (CE) n.º 45/2001 e o artigo 3.º da Decisão 1247/2002/CE, e estabelece as normas para a nomeação da AEPD pelo Parlamento Europeu e o Conselho. Também especifica a duração do respetivo mandato, ou seja, cinco anos.

O artigo 55.º tem por base o artigo 43.º do Regulamento (CE) n.º 45/2001 e o artigo 1.º da Decisão 1247/2002/CE, e prevê o estatuto e as condições gerais de exercício das funções da AEPD, bem como diz respeito aos seus colaboradores e recursos financeiros.

O artigo 56.º tem por base o artigo 52.º do Regulamento (UE) 2016/679 e o artigo 44.º do Regulamento (CE) n.º 45/2001, e clarifica as condições que garantem a independência da AEPD, tendo em consideração a jurisprudência do Tribunal de Justiça da União Europeia.

O artigo 57.º estabelece, com base no artigo 45.º do Regulamento (CE) n.º 45/2001, as obrigações de sigilo da AEPD durante e após o mandato, relativamente às informações confidenciais a que tenha tido acesso durante o desempenho das suas funções.

O artigo 58.º tem por base o artigo 57.º do Regulamento (UE) 2016/679 e o artigo 46.º do Regulamento (CE) n.º 45/2001, e estabelece as atribuições da AEPD, incluindo receber e examinar reclamações e sensibilizar o público para os riscos, normas, garantias e direitos existentes.

O artigo 59.º tem por base o artigo 58.º do Regulamento (UE) 2016/679 e o artigo 47.º do Regulamento (CE) n.º 45/2001, e estabelece os poderes da AEPD.

O artigo 60.º tem por base o artigo 59.º do Regulamento (UE) 2016/679 e o artigo 48.º do Regulamento (CE) n.º 45/2001, e estabelece a obrigação de a AEPD elaborar um relatório anual de atividades.

#### *CAPÍTULO VII – COOPERAÇÃO E COERÊNCIA*

O artigo 61.º tem por base o artigo 61.º do Regulamento (UE) 2016/679 e o artigo 46.º, alínea f), do Regulamento (CE) n.º 45/2001, e introduz normas explícitas sobre a cooperação da AEPD com as autoridades nacionais de controlo.

O artigo 62.º prevê as obrigações da AEPD, sempre que outros atos da União remetem para este artigo no quadro de supervisão coordenada com as autoridades nacionais de controlo. Visa aplicar um modelo único de supervisão coordenada. Este modelo pode ser utilizado para uma supervisão coordenada de grandes sistemas informáticos, tais como o Eurodac, o Sistema de Informação de Schengen II, o Sistema de Informação sobre Vistos, o Sistema de Informação Aduaneiro ou o Sistema de Informação do Mercado Interno, mas também para a supervisão de algumas agências da União, nos casos em que é estabelecido um modelo específico de cooperação entre a AEPD e as autoridades nacionais, designadamente a Europol. O Comité Europeu para a Proteção de Dados deve constituir uma instância única para garantir a eficácia do controlo coordenado a todos os níveis.

## CAPÍTULO VIII - VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

O artigo 63.º tem por base o artigo 77.º do Regulamento (UE) 2016/679 e o artigo 32.º do Regulamento (CE) n.º 45/2001, e prevê o direito de qualquer titular dos dados de apresentar uma reclamação à AEPD. Estabelece ainda a obrigação da AEPD de contactar e informar o titular dos dados sobre os progressos e o resultado da reclamação no prazo de três meses, período após o qual a reclamação é considerada indeferida.

O artigo 64.º retoma o artigo 32.º, n.º 1, do Regulamento (CE) n.º 45/2001, que estabelece a competência do Tribunal de Justiça da União Europeia para apreciar todos os litígios relativos a disposições do presente regulamento, incluindo ações de indemnização.

O artigo 65.º estabelece o direito de obter uma indemnização, para danos materiais e não materiais, sob reserva das condições previstas nos Tratados, incluindo em matéria de responsabilidade.

O artigo 66.º tem por base o artigo 83.º do Regulamento (UE) 2016/679, conferindo à AEPD a competência para impor coimas às instituições e organismos da União, como medida de último recurso e apenas nos casos em que as instituições e organismos da União não cumpriram uma ordem da AEPD mencionada no artigo 59.º, n.º 2, alíneas a) a h) e alínea j). Este artigo também especifica os critérios para decidir do montante da coima em cada caso individual, sendo que os montantes anuais máximos se inspiram nos montantes das coimas aplicadas em alguns Estados-Membros.

O artigo 67.º permite, em conformidade com o artigo 80.º, n.º 1, do Regulamento (UE) 2016/679, que determinados organismos, organizações ou associações apresentem uma reclamação em nome do titular dos dados.

O artigo 68.º prevê, em conformidade com o artigo 33.º do Regulamento (CE) n.º 45/2001, normas específicas destinadas a proteger os membros do pessoal da União que apresentam uma reclamação à AEPD relativa a uma alegada violação das disposições do presente regulamento, sem passar pela via oficial.

O artigo 69.º tem por base o artigo 49.º do Regulamento (CE) n.º 45/2001, e prevê as sanções aplicáveis à inobservância de obrigações do presente regulamento por funcionários ou outros agentes da União Europeia.

## *CAPÍTULO IX - ATOS DE EXECUÇÃO*

O artigo 70.º contém a disposição relativa ao procedimento de comité necessário para conferir competências de execução à Comissão sempre que, em conformidade com o artigo 291.º do TFUE, são necessárias condições uniformes para a execução de atos juridicamente vinculativos da União Europeia. Aplica-se o procedimento de exame.

## CAPÍTULO X - DISPOSIÇÕES FINAIS

O artigo 71.º revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE, e prevê que as referências aos dois instrumentos revogados devem entender-se como feitas para o presente regulamento.

O artigo 72.º clarifica que os mandatos atuais da Autoridade Europeia para a Proteção de Dados e da Autoridade-Adjunta não devem ser afetados pelo presente regulamento e que o artigo 54.º, n.ºs 4, 5 e 7 e os artigos 56.º e 57.º do regulamento são aplicáveis à atual Autoridade-Adjunta até ao final do seu mandato, ou seja, 5 de dezembro de 2019.

O artigo 73.º estabelece 25 de maio de 2018 como a data de entrada em vigor do presente regulamento, de forma a garantir a coerência com a data de aplicação do Regulamento (UE) 2016/679.

2017/0002 (COD)

Proposta de

## **REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO**

**relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE**

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 16.º, n.º 2,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu<sup>10</sup>,

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

- (1) A proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito.
- (2) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho<sup>11</sup> confere às pessoas singulares direitos suscetíveis de proteção judicial, especifica as obrigações em matéria de tratamento de dados dos responsáveis pelo tratamento a nível das instituições e órgãos comunitários, e cria uma autoridade de controlo independente, a Autoridade Europeia para a Proteção de Dados, responsável pelo controlo do tratamento de dados pessoais pelas instituições e órgãos da União. Contudo, não se aplica ao tratamento de dados pessoais efetuado no exercício de uma atividade das instituições e órgãos da União que se encontre fora do âmbito de aplicação do direito da União.
- (3) O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho<sup>12</sup> e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho<sup>13</sup> foram adotados em 27 de abril

---

<sup>10</sup> JO C [...] de [...], p. [...].

<sup>11</sup> Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

<sup>12</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação

de 2016. Enquanto o regulamento estabelece normas gerais para proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e assegurar a livre circulação de dados pessoais na União, a diretiva estabelece as normas específicas para proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e assegurar a livre circulação de dados pessoais na União nos domínios da cooperação judiciária em matéria penal e da cooperação policial.

- (4) O Regulamento (UE) 2016/679 salienta que devem ser realizadas as necessárias adaptações do Regulamento (CE) n.º 45/2001, a fim de prever um quadro de proteção de dados sólido e coerente na União e permitir a aplicação em simultâneo com o Regulamento (UE) 2016/679.
- (5) É no interesse de uma abordagem coerente à proteção de dados pessoais em toda a União e da livre circulação de dados pessoais na União, harmonizar o mais possível as normas de proteção de dados adotadas a nível das instituições e organismos da União com as normas de proteção de dados adotadas para o sector público nos Estados-Membros. Sempre que as disposições do presente regulamento sejam baseadas no mesmo conceito que as disposições do Regulamento (UE) 2016/679, essas duas disposições devem ser interpretadas de forma homogénea, sobretudo porque o sistema do presente regulamento deve ser entendido como equivalente ao sistema do Regulamento (UE) 2016/679.
- (6) As pessoas cujos dados pessoais são tratados por instituições e organismos da União, independentemente do contexto, por exemplo porque são funcionários dessas instituições e organismos, devem ser protegidas. O presente regulamento não deve ser aplicado ao tratamento de dados pessoais de pessoas falecidas. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os dados de contacto da pessoa coletiva.
- (7) A fim de se evitar um sério risco de ser contornada, a proteção das pessoas singulares deve ser neutra em termos tecnológicos e não deve depender das técnicas utilizadas. A proteção das pessoas singulares deve aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não devem ser abrangidos pelo âmbito de aplicação do presente regulamento.
- (8) Na Declaração 21 sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial, anexada à Ata Final da Conferência Intergovernamental que adotou o Tratado de Lisboa, a conferência reconheceu que, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições especiais sobre a proteção de dados pessoais e a livre circulação desses dados nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do TFUE. Por conseguinte, o presente

---

desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), JO L 119 de 4.5.2016, pp. 1–88.

<sup>13</sup> Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI, JO L 119 de 4.5.2016, pp. 89–131.

regulamento deve ser aplicado às agências da União que exerçam atividades nos domínios da cooperação judiciária em matéria penal e da cooperação policial, apenas na medida em que o direito da União aplicável a essas agências não contenha normas específicas sobre o tratamento de dados pessoais.

- (9) A Diretiva (UE) 2016/680 prevê normas harmonizadas para a proteção e a livre circulação de dados pessoais tratados para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. A fim de assegurar o mesmo nível de proteção para as pessoas singulares através de direitos suscetíveis de proteção judicial no conjunto da União e evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre as agências da União que exercem atividades nos domínios da cooperação judiciária em matéria penal e da cooperação policial e as autoridades competentes nos Estados-Membros, as normas relativas à proteção e à livre circulação de dados pessoais operacionais tratados por essas agências da União devem basear-se nos princípios subjacentes ao presente regulamento e ser coerentes com a Diretiva (UE) 2016/680.
- (10) Sempre que que o ato que cria uma agência da União que exerce atividades abrangidas pelo âmbito de aplicação dos capítulos 4 e 5 do título V do Tratado estabelece um regime autónomo de proteção de dados para o tratamento de dados pessoais operacionais, esses regimes não devem ser afetados pelo presente regulamento. Contudo, a Comissão deve, nos termos do artigo 62.º da Diretiva (UE) 2016/680, até 6 de maio de 2019, avaliar os atos da União que regulam o tratamento efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública e, quando necessário, apresentar as propostas necessárias à alteração desses atos de forma a assegurar uma abordagem coerente da proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial.
- (11) Os princípios da proteção de dados devem aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, devem ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de serem razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não devem, pois, aplicar-se às informações anónimas, ou seja, às informações que não digam respeito a uma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal modo anónimos que o seu titular não seja ou já não possa ser identificado. O presente regulamento não diz, portanto, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.
- (12) A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares dos dados em questão e ajudar os responsáveis pelo tratamento e os subcontratantes a cumprirem as suas obrigações de proteção de dados. A introdução

explícita da «pseudonimização» no presente regulamento não se destina a excluir outras eventuais medidas de proteção de dados.

- (13) As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.
- (14) O consentimento do titular dos dados deve ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que autoriza o tratamento dos dados que lhe digam respeito, por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio Web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-valorizadas ou a omissão não devem, por conseguinte, constituir um consentimento. O consentimento deve abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deve ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.
- (15) O tratamento de dados pessoais deve ser efetuado de forma lícita e leal. Deve ser transparente para as pessoas singulares que os dados pessoais que lhes digam respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e as finalidades a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com lealdade e transparência em relação às pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes digam respeito que estão a ser tratados. As pessoas singulares a quem os dados digam respeito devem ser alertadas para os riscos, normas, 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. Em especial, as finalidades específicas do tratamento dos dados pessoais devem ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Os dados pessoais devem ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para tal, é necessário assegurar, em especial, que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas devem ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deve fixar os prazos para o apagamento ou a revisão periódica. Devem ser adotadas todas as medidas razoáveis

para que os dados pessoais incorretos sejam retificados ou apagados. Os dados pessoais devem ser tratados de uma forma que garanta a devida segurança e confidencialidade, designadamente para evitar o acesso a dados pessoais e equipamentos utilizados para o seu tratamento ou a sua utilização por pessoas não autorizadas.

- (16) Em conformidade com o princípio da responsabilidade, quando as instituições e organismos da União transmitem dados pessoais internamente ou a outras instituições e organismos da União, devem verificar se esses dados pessoais são necessários para o desempenho legítimo de funções da competência do destinatário, sempre que este não faz parte do responsável pelo tratamento. Em particular, após o pedido do destinatário para a transmissão dos dados pessoais, o responsável pelo tratamento deve verificar a existência de um motivo relevante para o tratamento lícito dos dados pessoais, a competência do destinatário e efetuar uma avaliação provisória da necessidade da transferência desses dados. Em caso de dúvida quanto a essa necessidade, o responsável pelo tratamento deve solicitar informações complementares ao destinatário. O destinatário deve certificar-se que a necessidade da transferência dos dados pode ser posteriormente verificada.
- (17) Para que o tratamento seja lícito, os dados pessoais devem ser tratados com base na necessidade de desempenho de uma função efetuada no interesse público pelas instituições e organismos da União ou no exercício da sua autoridade pública, na necessidade de conformidade com a obrigação jurídica a que o responsável pelo tratamento esteja sujeito ou outra base legítima, conforme mencionado no presente regulamento, incluindo o consentimento do titular dos dados em causa ou a necessidade de ser executado um contrato no qual o titular dos dados seja parte ou para adotar medidas pré-contratuais a pedido do titular dos dados. O tratamento de dados pessoais para o desempenho de funções de interesse público pelas instituições e organismos da União inclui o tratamento de dados pessoais necessários à gestão e ao funcionamento dessas instituições e organismos. O tratamento de dados pessoais também deve ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ocorrer quando tal tratamento não puder manifestamente ter como base outro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação, ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana.
- (18) O direito da União, incluindo as normas internas mencionadas no presente regulamento, deve ser claro e rigoroso e a sua aplicação deve ser previsível para os seus destinatários, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia e do Tribunal Europeu dos Direitos do Homem.
- (19) O tratamento de dados pessoais para outros fins que não aqueles para os quais esses dados tenham sido inicialmente recolhidos apenas deve ser autorizado se for compatível com as finalidades para as quais os dados pessoais tenham sido inicialmente recolhidos. Nesse caso, não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior deve ser

considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, devem ser consideradas tratamento lícito compatível. A base jurídica prevista no direito da União para o tratamento de dados pessoais pode igualmente prever a base jurídica para o tratamento posterior. A fim de apurar se a finalidade de um tratamento de dados posterior é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deve ter em atenção, nomeadamente: a existência de uma ligação entre tais finalidades e a finalidade do tratamento posterior previsto; o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências do tratamento posterior previsto para os titulares dos dados; e a existência de garantias adequadas tanto no tratamento inicial como nas posteriores operações de tratamento previstas.

- (20) Sempre que o tratamento tiver por base o consentimento do titular dos dados, o responsável pelo tratamento deve poder demonstrar que o titular deu o seu consentimento a esse tratamento. Em especial, no contexto de uma declaração escrita relativa a outra matéria, devem existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho<sup>14</sup>, é oportuno prever uma declaração de consentimento previamente redigida pelo responsável pelo tratamento de forma compreensível e facilmente acessível, numa linguagem clara e simples e sem cláusulas abusivas. Para efeitos de um consentimento informado, o titular dos dados deve conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades do tratamento para as quais os dados se destinam. Não se deve considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.
- (21) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção especial deve aplicar-se, nomeadamente, à criação de perfis de personalidade e à recolha de dados pessoais relativos às crianças aquando da utilização de serviços disponibilizados diretamente a um menor nos sítios Web das instituições e organismos da União, tais como os serviços de comunicação interpessoal ou a venda de bilhetes em linha, e aquando do tratamento de dados com base no consentimento.
- (22) Quando os destinatários estabelecidos na União e sujeitos ao disposto no Regulamento (UE) 2016/679 ou na Diretiva (UE) 2016/680, pretendem que lhes sejam transmitidos os seus dados pessoais pelas instituições e organismos da União, devem demonstrar que a transmissão é necessária para a obtenção do seu objetivo, é proporcionada e não excede o necessário para atingir tal objetivo. As instituições e organismos da União devem demonstrar essa necessidade quando estão na origem da transmissão, em conformidade com o princípio da transparência.

---

<sup>14</sup> Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores (JO L 95 de 21.4.1993, p. 29).

- (23) Merecem proteção específica os dados pessoais que são, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e das liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e as liberdades fundamentais. Devem incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso da expressão «origem racial» no presente regulamento que a União aceita teorias que tentam demonstrar a existência de diferentes raças humanas. O tratamento de fotografias não deve ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Para além dos requisitos específicos para o tratamento de dados sensíveis, devem aplicar-se os princípios gerais e outras disposições do presente regulamento, em especial, no que se refere às condições para o tratamento lícito. É oportuno prever expressamente derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.
- (24) O tratamento de categorias especiais de dados pessoais pode ser necessário por razões de interesse público nos domínios da saúde pública sem o consentimento do titular dos dados. Esse tratamento deve ser objeto de medidas adequadas e específicas, a fim de defender os direitos e as liberdades das pessoas singulares. Nesse contexto, a noção de «saúde pública» deve ser interpretada segundo a definição constante do Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho<sup>15</sup>, ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde e as causas de mortalidade. Tal tratamento de dados relativos à saúde efetuado por motivos de interesse público não deve ter por resultado que os dados pessoais sejam tratados para outros fins por terceiros.
- (25) Se os dados pessoais tratados pelo responsável pelo tratamento não lhe permitirem identificar uma pessoa singular, não deve ser obrigado a obter informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento a uma disposição do presente regulamento. Todavia, o responsável pelo tratamento não deve recusar receber informações suplementares fornecidas pelo titular dos dados no intuito de apoiar o exercício dos seus direitos. A identificação deve incluir a identificação digital do titular dos dados, por exemplo com recurso a um procedimento de autenticação com os mesmos dados de identificação usados pelo interessado para aceder (log in) ao serviço em linha do responsável pelo tratamento.
- (26) O tratamento de dados pessoais para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, deve ficar sujeito a garantias adequadas aplicáveis aos direitos e às liberdades do titular dos dados, em conformidade com o presente regulamento. Essas garantias devem assegurar a

---

<sup>15</sup> Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho ([JO L 354 de 31.12.2008, p. 70](#)).

existência de medidas técnicas e organizativas que assegurem, nomeadamente, o princípio da minimização dos dados. O tratamento posterior de dados pessoais para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, deve ser efetuado quando o responsável pelo tratamento tiver avaliado a possibilidade de tais fins serem alcançados por um tipo de tratamento de dados pessoais que não permita ou tenha deixado de permitir a identificação dos titulares dos dados, na condição de existirem as garantias adequadas (como a pseudonimização dos dados pessoais). As instituições e organismos da União devem prever no direito da União, e eventualmente em normas internas, as garantias apropriadas para o tratamento de dados pessoais para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos.

- (27) É oportuno prever modalidades para facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do presente regulamento, incluindo procedimentos para solicitar e, se for o caso, obter gratuitamente, em especial o acesso a dados pessoais, a sua retificação ou apagamento e o exercício do direito de oposição. O responsável pelo tratamento deve fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via. O responsável pelo tratamento deve ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e fundamentar a sua eventual intenção de recusar o pedido.
- (28) Os princípios do tratamento leal e transparente exigem que o titular dos dados seja informado da operação de tratamento de dados e das suas finalidades. O responsável pelo tratamento deve fornecer ao titular as informações adicionais necessárias para assegurar um tratamento leal e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais são tratados. Além disso, o titular dos dados deve ser informado da existência de uma definição de perfis e das suas consequências. Sempre que os dados pessoais forem recolhidos junto do titular dos dados, este deve ser também informado da eventual obrigatoriedade de fornecer os dados pessoais e das consequências de não os facultar. Essas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de modo facilmente visível, inteligível e claramente legível, uma panorâmica útil do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática.
- (29) As informações sobre o tratamento de dados pessoais relativos ao titular dos dados devem ser-lhe facultadas no momento da sua recolha junto do interessado ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias. Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados deve ser informado aquando da primeira comunicação dos dados pessoais a esse destinatário. Sempre que o responsável pelo tratamento tiver a intenção de tratar os dados pessoais para uma finalidade diferente daquela para a qual tenham sido recolhidos, deve facultar ao titular dos dados, antes desse tratamento, informações sobre tal finalidade e outras informações necessárias. Quando não for possível informar o titular dos dados da origem dos dados pessoais por se ter recorrido a várias fontes, devem ser-lhe facultadas informações genéricas.
- (30) Os titulares de dados devem ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude. Tal inclui o direito de acederem a dados sobre a sua saúde, por exemplo os registos médicos contendo informações como diagnósticos, resultados de exames, avaliações dos médicos e

eventuais tratamentos ou intervenções realizados. Cada titular de dados deve, portanto, ter o direito de conhecer e ser informado, em especial das finalidades para as quais os dados pessoais são tratados, quando possível o período durante o qual os dados são tratados, a identidade dos destinatários dos dados pessoais, a lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, as consequências de tal tratamento. Esse direito não deve prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, tais considerações não devem implicar a recusa de fornecer ao titular dos dados todas as informações. Quando o responsável pelo tratamento proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deve poder solicitar que, antes de a informação ser fornecida, o titular especifique a que informações ou a que atividades de tratamento se refere o seu pedido.

- (31) Os titulares dos dados devem ter direito a que os seus dados pessoais sejam retificados e ao «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União aplicável ao responsável pelo tratamento. Um titular dos dados deve ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se já não forem necessários para a finalidade para a qual foram recolhidos ou tratados, se o titular dos dados tiver retirado o seu consentimento ou se se opuser ao tratamento dos seus dados pessoais ou se o tratamento desses dados não respeitar o disposto no presente regulamento. Tal direito assume particular importância sempre que o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos riscos inerentes ao tratamento, e mais tarde pretenda suprimir esses dados pessoais, especialmente na Internet. O titular dos dados deve ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados pessoais deve ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
- (32) Para reforçar o «direito a ser esquecido» no ambiente em linha, é oportuno que o direito de apagamento seja alargado de modo a obrigar o responsável pelo tratamento que tenha tornado públicos os dados pessoais, a informar os responsáveis que estejam a tratar esses dados pessoais de que devem suprimir quaisquer ligações para esses dados pessoais, ou cópias ou reproduções dos mesmos. Ao fazê-lo, é oportuno que esse responsável pelo tratamento adote medidas razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar esses dados.
- (33) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio Web dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento devem, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações

de tratamento e não possam ser alterados. Deve indicar-se de forma clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.

- (34) Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deve ser igualmente autorizado a receber os dados pessoais que lhe digam respeito que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados devem ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Esse direito deve aplicar-se também se o titular dos dados tiver fornecido os dados pessoais com base no seu consentimento ou se o tratamento for necessário para a execução de um contrato. Por conseguinte, esse direito não deve ser aplicável quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de funções de interesse público ou o exercício da autoridade pública de que esteja investido o responsável pelo tratamento. O direito do titular dos dados a transmitir ou receber dados pessoais que lhe digam respeito não deve implicar para os responsáveis pelo tratamento a obrigação de adotar ou manter sistemas de tratamento que sejam tecnicamente compatíveis. Quando um determinado conjunto de dados pessoais diga respeito a mais de um titular, o direito de receber os dados pessoais não deve prejudicar os direitos e as liberdades de outros titulares de dados em conformidade com o presente regulamento. Além disso, esse direito também não deve prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, nomeadamente, não deve implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deve ter o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento.
- (35) No caso de um tratamento de dados pessoais lícito realizado por ser necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento, o titular dos dados não deve deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deve caber ao responsável pelo tratamento provar que os seus interesses legítimos e imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.
- (36) O titular dos dados deve ter o direito de não ficar sujeito a uma decisão, que pode incluir uma medida que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como práticas de recrutamento eletrónico sem intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. Contudo, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deve ser permitida se expressamente autorizada pelo direito da União. Em qualquer dos casos, tal tratamento deve ser acompanhado das garantias adequadas, que devem

incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deve dizer respeito a uma criança. A fim de assegurar um tratamento leal e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deve utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a ter em conta os potenciais riscos para os interesses e direitos do titular dos dados e a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. O processo de tomada de decisão automatizado e a definição de perfis baseada em categorias especiais de dados pessoais só deve ser permitido em condições específicas.

- (37) Os atos jurídicos adotados com base nos Tratados ou normas internas das instituições e organismos da União podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais, ao direito à portabilidade dos dados, à confidencialidade das comunicações eletrónicas, bem como à comunicação de uma violação de dados pessoais ao titular dos dados e a determinadas obrigações conexas dos responsáveis pelo tratamento, desde que necessárias e proporcionais numa sociedade democrática, para salvaguardar a segurança pública, a prevenção, a investigação e repressão de infração penais ou a execução de sanções penais, incluindo a prevenção de ameaças contra a segurança pública e a sua prevenção, a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, a segurança interna das instituições e organismos da União, outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, a conservação de registos públicos por motivos de interesse público geral ou a defesa do titular dos dados ou dos direitos e liberdades de outrem, incluindo a proteção social, a saúde pública e os fins humanitários.

Sempre que uma restrição não esteja prevista nos atos jurídicos adotados com base nos Tratados ou nas suas normas internas, as instituições e organismos da União podem, em casos específicos, impor uma restrição *ad hoc* relativa aos princípios específicos e aos direitos do titular dos dados, se essa restrição respeitar a essência dos direitos e liberdades fundamentais e, em relação a uma operação de tratamento específica, for necessária e proporcionada numa sociedade democrática para salvaguardar um ou mais objetivos mencionados no n.º 1. A restrição deve ser notificada ao encarregado da proteção de dados. Todas as restrições devem respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

- (38) É oportuno estabelecer a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deve ser obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de demonstrar a conformidade das atividades de tratamento com o presente regulamento, incluindo a eficácia das medidas. Essas medidas devem ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o

risco que possa implicar para os direitos e liberdades das pessoas singulares. Os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, podem resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial: quando o tratamento implicar discriminação, usurpação ou roubo da identidade, perdas financeiras, prejuízo para a reputação, perda de confidencialidade dose dados pessoais protegidos por sigilo profissional, decifração não autorizada da pseudonimização, ou qualquer outro prejuízo significativo de natureza económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados devem ser determinadas por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos devem ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam um risco ou um risco elevado.

- (39) A proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder demonstrar a conformidade com o presente regulamento, o responsável pelo tratamento deve adotar orientações internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. Os princípios de proteção de dados desde a conceção e, por defeito, devem também ser tomados em consideração no contexto dos contratos públicos.
- (40) A proteção dos direitos e liberdades dos titulares de dados, bem como a responsabilidade dos responsáveis pelo tratamento e dos subcontratantes, exige uma clara repartição das responsabilidades nos termos do presente regulamento, nomeadamente quando o responsável pelo tratamento determina as finalidades e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento de dados é efetuada por conta de um responsável pelo tratamento.
- (41) Para assegurar o cumprimento do presente regulamento no que se refere ao tratamento a efetuar pelo subcontratante por conta do responsável pelo tratamento, este, quando confiar atividades de tratamento a um subcontratante, deve recorrer exclusivamente a subcontratantes que ofereçam garantias suficientes, especialmente em termos de

conhecimentos especializados, fiabilidade e recursos, quanto à execução de medidas técnicas e organizativas que cumpram os requisitos do presente regulamento, incluindo no que se refere à segurança do tratamento. A aplicação por subcontratantes diferentes de instituições e organismos da União de um código de conduta aprovado ou de um mecanismo de certificação aprovado pode ser utilizada como elemento para demonstrar a conformidade com as obrigações do responsável pelo tratamento. A realização de operações de tratamento de dados por um subcontratante deve ser regulada por um contrato ou outro ato jurídico ao abrigo do direito da União ou dos Estados-Membros que vincule o subcontratante ao responsável pelo tratamento, e em que seja estabelecido o objeto e a duração do contrato, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias de titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e liberdades do titular dos dados. O responsável pelo tratamento e o subcontratante devem poder optar por um contrato individual ou cláusulas contratuais-tipo, que são adotadas quer diretamente pela Comissão ou pela Autoridade Europeia para a Proteção de Dados e posteriormente adotadas pela Comissão. Após concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deve, consoante a escolha do responsável pelo tratamento, restituir ou apagar os dados pessoais, a menos que seja exigida a conservação desses dados pessoais ao abrigo do direito da União ou do Estado-Membro a que o subcontratante está sujeito.

- (42) A fim de demonstrar a observância do presente regulamento, os responsáveis pelo tratamento devem conservar um registo das atividades de tratamento sob a sua responsabilidade e os subcontratantes devem conservar um registo das categorias de atividades de tratamento sob a sua responsabilidade. As instituições e organismos da União devem ser obrigados a cooperar com a Autoridade Europeia para a Proteção de Dados e a facultar-lhe esses registos, mediante pedido, para fiscalização dessas operações de tratamento. As instituições e organismos da União devem ter condições para estabelecer um registo central dos registos das suas atividades de tratamento. Por motivos de transparência, devem poder igualmente tornar esse registo público.
- (43) A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deve avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas devem assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, devem ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.
- (44) As instituições e organismos da União devem garantir a confidencialidade das comunicações eletrónicas, tal como previsto no artigo 7.º da Carta. Em especial, as instituições e organismos da União devem garantir a segurança das suas redes de comunicações eletrónicas, proteger as informações relativas ao equipamento terminal dos utilizadores finais que acedem aos seus sítios Web e aplicações móveis acessíveis ao público em conformidade com o Regulamento (UE) XXXX/XX [novo Regulamento relativo à privacidade e às comunicações eletrónicas] e proteger os dados pessoais em listas de utilizadores.

- (45) Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deve notificá-la à Autoridade Europeia para a Proteção de Dados, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deve ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada. Se esse atraso for justificado, devem ser comunicadas o mais cedo possível as informações menos sensíveis ou menos específicas sobre a violação em vez de resolver totalmente o incidente subjacente antes da notificação.
- (46) O responsável pelo tratamento deve informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias. A comunicação deve descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deve ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a Autoridade Europeia para a Proteção de Dados, e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades com funções coercivas.
- (47) O Regulamento (CE) n.º 45/2001 prevê uma obrigação geral do responsável pelo tratamento de notificar o tratamento dos dados pessoais ao encarregado da proteção de dados, que, por seu turno, deve conservar um registo das operações de tratamento notificadas. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação devem, por isso, ser suprimidas e substituídas por normas e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Esses tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento. Nesses casos, o responsável pelo tratamento deve proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deve incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.
- (48) Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos

de aplicação, a Autoridade Europeia para a Proteção de Dados deve ser consultada antes de as atividades de tratamento terem início. Provavelmente, esse elevado risco decorre de determinados tipos de tratamento e da extensão e frequência do tratamento, que podem originar igualmente danos ou interferir com os direitos e liberdades da pessoa singular. A Autoridade Europeia para a Proteção de Dados deve responder ao pedido de consulta dentro de um determinado prazo. Contudo, a ausência de reação da Autoridade Europeia para a Proteção de Dados no decorrer desse prazo não prejudicará qualquer intervenção que esta autoridade venha a fazer em conformidade com as suas funções e competências, definidas pelo presente regulamento, incluindo a competência para proibir certas operações de tratamento. No âmbito desse processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão pode ser apresentado à Autoridade Europeia para a Proteção de Dados, em especial as medidas previstas para atenuar o risco para os direitos e liberdades das pessoas singulares.

- (49) A Autoridade Europeia para a Proteção de Dados deve ser informada das medidas administrativas e dos regulamentos internos das instituições e organismos da União que preveem o tratamento de dados pessoais, estabelecem condições para as restrições dos direitos dos titulares dos dados ou conferem garantias adequadas para os direitos dos titulares dos dados, de forma a assegurar a conformidade do tratamento previsto com o presente regulamento e, nomeadamente, atenuar os riscos para os titulares dos dados.
- (50) O Regulamento (UE) 2016/679 instituiu o Comité Europeu para a Proteção de Dados como um organismo independente da União com personalidade jurídica. O Comité deve contribuir para a aplicação coerente do Regulamento (UE) 2016/679 e da Diretiva 2016/680 em toda a União, e igualmente o aconselhamento da Comissão. Simultaneamente, a Autoridade Europeia para a Proteção de Dados deve continuar a exercer as suas funções de supervisão e consultivas relativamente a todas as instituições e organismos da União, incluindo por iniciativa própria ou mediante pedido. A fim de garantir a coerência das normas em matéria de proteção de dados em toda a União, deve ser obrigatória uma consulta por parte da Comissão, após a adoção dos atos legislativos ou durante a preparação dos atos delegados e dos atos de execução, conforme definido nos artigos 289.º, 290.º e 291.º do TFUE, e após a adoção de recomendações e propostas relativas aos acordos com países terceiros e organizações internacionais, tal como previsto no artigo 218.º do TFUE, que têm um impacto no direito à proteção de dados pessoais. Nesses casos, a Comissão deve ser obrigada a consultar a Autoridade Europeia para a Proteção de Dados, exceto quando o Regulamento (UE) 2016/679 prevê uma consulta obrigatória do Comité Europeu para a Proteção de Dados, por exemplo, sobre decisões de adequação ou atos delegados relativos a ícones normalizados e a requisitos aplicáveis aos procedimentos de certificação. Sempre que o ato em questão for particularmente importante para a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão deve ainda poder consultar o Comité Europeu para a Proteção de Dados. Nesses casos, a Autoridade Europeia para a Proteção de Dados deve, enquanto membro do Comité Europeu para a Proteção de Dados, coordenar o seu trabalho com este último a fim de emitirem uma opinião conjunta. A Autoridade Europeia para a Proteção de Dados e, se aplicável, o Comité Europeu para a Proteção de Dados, devem emitir o seu parecer por escrito no prazo de oito semanas. Tal prazo deve ser mais curto em caso de urgência, ou sempre que necessário, por exemplo quando a Comissão estiver a preparar atos delegados ou de execução.

- (51) Um encarregado da proteção de dados deve assegurar, em cada instituição ou organismo da União, que as disposições do presente regulamento são aplicadas e aconselhar os responsáveis pelo tratamento e subcontratantes no exercício das suas obrigações. Esse encarregado deve ser uma pessoa com conhecimentos especializados sobre a legislação e práticas em matéria de proteção de dados que devem ser determinados, em particular, em função do tratamento de dados realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante. Essas pessoas encarregadas da proteção de dados devem poder desempenhar as suas funções e cumprir os seus deveres de forma independente.
- (52) Quando os dados pessoais são transferidos das instituições e organismos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deve continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Apenas poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas às transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.
- (53) A Comissão pode decidir, nos termos do artigo 45.º do Regulamento (UE) 2016/679, que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, assegura um nível adequado de proteção de dados. Nestes casos, uma instituição ou organismo da União pode realizar transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária qualquer outra autorização.
- (54) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deve adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas pela Autoridade Europeia para a Proteção de Dados ou cláusulas contratuais autorizadas por esta autoridade. Nos casos em que o subcontratante não é uma instituição ou organismo da União, essas garantias adequadas podem igualmente consistir em regras vinculativas aplicáveis às empresas, códigos de conduta e mecanismos de certificação utilizados para transferências internacionais ao abrigo do Regulamento (UE) 2016/679. Tais garantias devem assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. Devem estar relacionadas, em especial, com o respeito pelos princípios gerais relativos ao tratamento de dados pessoais e pelos princípios de proteção de dados desde a conceção e por defeito. Também podem ser efetuadas transferências por instituições e organismos da União para autoridades ou organismos públicos em países terceiros ou para organizações internacionais que tenham deveres e funções correspondentes, nomeadamente com base em disposições a

inserir no regime administrativo, por exemplo um memorando de entendimento, que prevejam a existência de direitos efetivos e oponíveis dos titulares dos dados. Deve ser obtida a autorização da Autoridade Europeia para a Proteção de Dados quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.

- (55) A possibilidade de o responsável pelo tratamento ou o subcontratante recorrer a cláusulas-tipo de proteção de dados adotadas pela Comissão ou pela Autoridade Europeia para a Proteção de Dados não os deve impedir de incluírem tais cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais, desde que não colidam, direta ou indiretamente, com as cláusulas contratuais-tipo adotadas pela Comissão ou pela Autoridade Europeia para a Proteção de Dados, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes devem ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção de dados.
- (56) Alguns países terceiros aprovam leis, regulamentos e outros atos normativos destinados a regular diretamente as atividades de tratamento pelas instituições e organismos da União. Pode ser o caso de sentenças de órgãos jurisdicionais ou de decisões de autoridades administrativas de países terceiros que exijam que o responsável pelo tratamento ou subcontratante transfira ou divulgue dados pessoais sem fundamento num acordo internacional em vigor entre o país terceiro em causa e a União. Em virtude da sua aplicabilidade extraterritorial, essas leis, regulamentos e outros atos normativos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado na União Europeia pelo presente regulamento. As transferências só devem ser autorizadas quando estiverem preenchidas as condições estabelecidas pelo presente regulamento para as transferências para países terceiros. Pode ser esse o caso, nomeadamente, sempre que a divulgação for necessária por um motivo importante de interesse público, reconhecido pelo direito da União.
- (57) Deve prever-se a possibilidade de efetuar transferências em situações específicas em que o titular dos dados dê o seu consentimento explícito, em que a transferência seja ocasional e necessária em relação a um contrato ou a um contencioso judicial, independentemente de se tratar de um processo judicial, de um processo administrativo ou de um qualquer procedimento não judicial, incluindo procedimentos junto de organismos de regulação. Deve também estar prevista a possibilidade de efetuar transferências no caso de motivos importantes de interesse público previstos pelo direito da União ou se a transferência for efetuada a partir de um registo criado por lei e destinado à consulta por parte do público ou de pessoas com um interesse legítimo. Neste último caso, a transferência não deve abranger a totalidade dos dados nem categorias completas de dados pessoais contidos nesse registo, a menos que seja autorizada pelo direito da União, e, quando este último se destinar a ser consultado por pessoas com um interesse legítimo, a transferência apenas deve ser efetuada a pedido dessas pessoas ou, caso sejam os seus destinatários, tendo plenamente em conta os interesses e os direitos fundamentais do titular dos dados.
- (58) Essas derrogações devem ser aplicáveis, em especial, às transferências de dados exigidas e necessárias por razões importantes de interesse público, por exemplo em caso de intercâmbio internacional de dados entre instituições e organismos da União e autoridades da concorrência, administrações fiscais ou aduaneiras, autoridades de supervisão financeira e serviços competentes em matéria de segurança social ou de

saúde pública, por exemplo em caso de localização de contactos no que respeita a doenças contagiosas ou para reduzir e/ou eliminar a dopagem no desporto. Deve igualmente ser considerada legal uma transferência de dados pessoais que seja necessária para a proteção de um interesse essencial para os interesses vitais do titular dos dados ou de outra pessoa, nomeadamente a integridade física ou a vida, se o titular dos dados estiver impossibilitado de dar o seu consentimento. Na falta de uma decisão de adequação, o direito da União pode, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. As transferências, para uma organização humanitária internacional, de dados pessoais de um titular que seja física ou legalmente incapaz de dar o seu consentimento, com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por ser do interesse vital do titular dos dados.

- (59) Em qualquer caso, se a Comissão não tiver tomado nenhuma decisão relativamente ao nível de proteção adequado de dados num determinado país terceiro, o responsável pelo tratamento ou o subcontratante deve adotar soluções que confirmem aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, e lhes garantam que continuarão a beneficiar dos direitos e garantias fundamentais.
- (60) Sempre que ocorram transferências transnacionais de dados pessoais para o exterior do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo na União, incluindo a Autoridade Europeia para a Proteção de Dados, podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiras podem ser também restringidos por poderes preventivos ou medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. Por conseguinte, deve ser promovida uma cooperação mais estreita entre a Autoridade Europeia para a Proteção de Dados e outras autoridades de controlo da proteção de dados, a fim de contribuir para o intercâmbio de informações com as suas homólogas internacionais.
- (61) A criação da Autoridade Europeia para a Proteção de Dados pelo Regulamento (CE) n.º 45/2001, habilitada a desempenhar as suas funções e a exercer os seus poderes com total independência, constitui um elemento essencial da proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais. O presente regulamento reforça e clarifica o seu papel e independência.
- (62) A fim de assegurar o controlo e a aplicação coerentes das normas em matéria de proteção de dados em toda a União, a Autoridade Europeia para a Proteção de Dados tem as mesmas funções e poderes efetivos que as autoridades de controlo nos Estados-Membros, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso de reclamações apresentadas por pessoas singulares, bem como submeter as violações ao presente regulamento à apreciação do Tribunal de Justiça da União Europeia e intentar processos judiciais, em conformidade com o direito primário. Essas competências devem incluir o poder de impor uma limitação temporária ou definitiva ao tratamento, ou mesmo a sua proibição. Por forma a evitar custos supérfluos e inconvenientes

excessivos para as pessoas em causa que possam ser prejudicadas, cada medida da Autoridade Europeia para a Proteção de Dados deve ser adequada, necessária e proporcionada, a fim de garantir a conformidade com o presente regulamento, e deve ter em conta as circunstâncias de cada caso concreto e respeitar o direito de todas as pessoas a serem ouvidas antes de ser tomada qualquer medida individual. As medidas juridicamente vinculativas da Autoridade Europeia para a Proteção de Dados devem ser emitidas por escrito, de forma clara e sem ambiguidades, indicar a sua data de emissão, ostentar a assinatura da Autoridade Europeia para a Proteção de Dados, indicar os motivos que as justificam e mencionar o direito de recurso efetivo.

- (63) As decisões da Autoridade Europeia para a Proteção da Dados relacionadas com exceções, garantias, autorizações e condições relativas a certos tratamentos de dados, tal como definidas no regulamento, devem ser publicadas no relatório de atividades. Independentemente da publicação anual de um relatório de atividades, a Autoridade Europeia para a Proteção da Dados poderá publicar relatórios sobre questões específicas.
- (64) As autoridades de controlo nacionais controlam a aplicação das disposições do Regulamento (UE) 2016/679 e contribuem para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados a nível do mercado interno. Para reforçar a coerência na aplicação das normas de proteção de dados que se aplicam nos Estados-Membros e das normas de proteção de dados aplicáveis a instituições e organismos da União, a Autoridade Europeia para a Proteção de Dados deve cooperar eficazmente com as autoridades nacionais de controlo.
- (65) Em determinadas situações, o direito da União prevê um modelo de controlo coordenado, partilhado entre a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo. Além disso, a Autoridade Europeia para a Proteção da Dados é a autoridade de controlo da Europol e, por conseguinte, foi estabelecido um modelo de cooperação específico com as autoridades nacionais de controlo através da criação de um conselho de cooperação com uma função consultiva. Para melhorar o controlo efetivo e a aplicação de normas materiais em matéria de proteção de dados, é oportuno introduzir na União um modelo único e coerente de controlo coordenado. A Comissão deve, portanto, quando apropriado, apresentar propostas legislativas tendo em vista alterar atos jurídicos da União que prevejam um modelo de controlo coordenado, a fim de os alinhar com o modelo de controlo coordenado do presente regulamento. O Comité Europeu para a Proteção de Dados deve constituir uma instância única para garantir a eficácia do controlo coordenado a todos os níveis.
- (66) Os titulares dos dados devem ter o direito a apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados e o direito a um recurso efetivo junto do Tribunal de Justiça da União Europeia, em conformidade com os Tratados, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a Autoridade Europeia para a Proteção de Dados não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as medidas necessárias para proteger os seus direitos. A investigação decorrente de uma reclamação deve ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A Autoridade Europeia para a Proteção de Dados deve informar o titular dos dados da evolução e do resultado da reclamação num prazo razoável. Se o caso exigir a coordenação com outra autoridade nacional de controlo, devem ser fornecidas informações intercalares ao titular dos dados. A Autoridade Europeia para a Proteção de Dados deve tomar medidas para facilitar a apresentação de reclamações,

nomeadamente fornecendo formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.

- (67) Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento deve ter o direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos, nas condições previstas no Tratado.
- (68) A fim de reforçar o papel de controlo da Autoridade Europeia para a Proteção de Dados e a aplicação efetiva do presente regulamento, a referida autoridade deve, como medida de último recurso, ter competência para impor coimas. Tais coimas devem ter por objetivo sancionar a instituição ou organismo – e não pessoas singulares – pela inobservância do presente regulamento, impedir futuras violações do mesmo e promover uma cultura de proteção de dados pessoais no âmbito das instituições e organismos da União. O presente regulamento deve indicar as infrações, bem como os montantes máximos e os critérios para definir as coimas daí decorrentes. A Autoridade Europeia para a Proteção de Dados deve determinar o montante máximo das coimas em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente a natureza, a gravidade e a duração da infração e das suas consequências, bem como as medidas adotadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências dessa infração. Aquando da aplicação de uma coima a um organismo da União, a Autoridade Europeia para a Proteção de Dados deve ter em conta a proporcionalidade do montante da coima. O procedimento administrativo para a aplicação de coimas a instituições e organismos da União deve respeitar os princípios gerais do direito da União, tal como interpretado pelo Tribunal de Justiça da União Europeia.
- (69) Se o titular dos dados considerar que os direitos que lhe são conferidos pelo presente regulamento foram violados, deve ter o direito de mandar um organismo, organização ou associação sem fins lucrativos que seja constituído ao abrigo do direito da União ou de um Estado-Membro, cujos objetivos estatutários sejam de interesse público e que exerça a sua atividade no domínio da proteção dos dados pessoais, para apresentar uma reclamação em seu nome junto da Autoridade Europeia para a Proteção de Dados. Tal organismo, organização ou associação deve também poder exercer o direito a intentar uma ação judicial ou obter uma indemnização em nome dos titulares de dados.
- (70) O funcionário ou outro agente da União que não cumpra as obrigações decorrentes do presente regulamento é passível de sanção disciplinar ou outra medida, nos termos das normas e procedimentos do Estatuto dos Funcionários da União Europeia ou do Regime Aplicável aos Outros Agentes da União Europeia.
- (71) A fim de assegurar condições uniformes para a execução do presente regulamento, devem ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências devem ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho<sup>16</sup>. O procedimento de exame deve ser utilizado para a adoção de cláusulas contratuais-tipo entre os responsáveis pelo tratamento e subcontratantes e entre subcontratantes, para a

---

<sup>16</sup> Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

adoção da lista de operações de tratamento em que é exigida a consulta prévia da Autoridade Europeia para a Proteção de Dados por parte dos responsáveis pelo tratamento para a execução de uma missão de interesse público e para a adoção de cláusulas contratuais-tipo que estabeleçam garantias adequadas para transferências internacionais.

- (72) Devem ser protegidas as informações confidenciais que a União e as autoridades nacionais de estatística recolham para a produção de estatísticas oficiais europeias e nacionais. Devem ser desenvolvidas, elaboradas e divulgadas estatísticas europeias de acordo com os princípios estatísticos enunciados no artigo 338.º, n.º 2, do TFUE. O Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho<sup>17</sup> prevê especificações suplementares em matéria de segredo estatístico aplicável às estatísticas europeias.
- (73) É oportuno revogar o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE. As referências ao regulamento e à decisão revogados devem ser entendidas como referências ao presente regulamento.
- (74) No intuito de garantir a plena independência dos membros da autoridade independente de controlo, os mandatos das atuais Autoridade Europeia para a Proteção de Dados e Autoridade Adjunta não devem ser afetados pelo presente regulamento. A atual Autoridade Adjunta deve permanecer em funções até ao final do seu mandato, a não ser que se verifique uma das condições para a cessação antecipada do mandato da Autoridade Europeia para a Proteção de Dados, estabelecida no presente regulamento. As disposições relevantes do presente regulamento devem aplicar-se à Autoridade Adjunta até ao termo do seu mandato.
- (75) Em conformidade com o princípio da proporcionalidade, para atingir o objetivo fundamental que garanta um nível equivalente de proteção das pessoas singulares e a livre circulação de dados pessoais na União, é necessário e apropriado estabelecer normas sobre o tratamento de dados pessoais nas instituições e organismos da União. O presente regulamento não excede o necessário para atingir tais objetivos, em conformidade com o artigo 5.º, n.º 4, do Tratado da União Europeia.
- (76) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu um parecer em XX/XX/XXXX,

---

<sup>17</sup> Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativo às Estatísticas Europeias e que revoga o Regulamento (CE, Euratom) n.º 1101/2008 relativo à transmissão de informações abrangidas pelo segredo estatístico ao Serviço de Estatística das Comunidades Europeias, o Regulamento (CE) n.º 322/97 do Conselho relativo às estatísticas comunitárias e a Decisão 89/382/CEE, Euratom do Conselho que cria o Comité do Programa Estatístico das Comunidades Europeias ([JO L 87 de 31.3.2009, p. 164](#)).

ADOTARAM O PRESENTE REGULAMENTO:

## CAPÍTULO I

### DISPOSIÇÕES GERAIS

#### *Artigo 1.º*

##### *Objeto e objetivos*

1. O presente regulamento estabelece normas em matéria de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais por instituições, órgãos, organismos e agências, bem como normas sobre a livre circulação de dados pessoais entre eles ou entre eles e destinatários estabelecidos na União e abrangidos pelo Regulamento (UE) 2016/679<sup>18</sup>, ou pelas disposições do direito nacional adotadas de acordo com a Diretiva (UE) 2016/680<sup>19</sup>.
2. O presente regulamento protege os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
3. A Autoridade Europeia para a Proteção de Dados («AEPD») controla a aplicação das disposições do presente regulamento a todas as operações de tratamento efetuadas pelas instituições e organismos da União.

#### *Artigo 2.º*

##### *Âmbito de aplicação*

1. O presente regulamento aplica-se ao tratamento de dados pessoais por todas as instituições e organismos da União, na medida em que esse tratamento for efetuado no exercício de atividades abrangidas total ou parcialmente pelo direito da União.
2. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

#### *Artigo 3.º*

##### *Definições*

1. Para efeitos do presente regulamento, aplicam-se as seguintes definições:
  - (a) As definições constantes do Regulamento (UE) 2016/679, com exceção da definição de «responsável pelo tratamento» no artigo 4.º, ponto 7, do regulamento;

---

<sup>18</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), JO L 119 de 4.5.2016, pp. 1–88.

<sup>19</sup> Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI, JO L 119 de 4.5.2016, pp. 89–131.

- (b) A definição de «comunicação eletrónica» no artigo 4.º, n.º 2, alínea a), do Regulamento (UE) XX/XXXX [Regulamento sobre a privacidade e as comunicações eletrónicas];
- (c) As definições de «rede de comunicações eletrónicas» e «utilizador final» no artigo 2.º, pontos 1 e 14, da Diretiva 00/0000/UE [Diretiva que estabelece o Código Europeu de Comunicações Eletrónicas] respetivamente;
- (d) A definição de «equipamento terminal» no artigo 1.º, ponto 1, da Diretiva 2008/63/CE<sup>20</sup> da Comissão.

2. Para efeitos do presente regulamento, também se aplicam as seguintes definições:

- (a) «Instituições e organismos da União», as instituições, órgãos, organismos e agências da União estabelecidos pelo, ou com base, no Tratado da União Europeia, no Tratado sobre o Funcionamento da União Europeia ou no Tratado Euratom;
- (b) «Responsável pelo tratamento», a instituição, órgão, organismo ou agência, a direção-geral ou qualquer outra entidade organizativa que, individualmente ou em conjunto com outras entidades, determine as finalidades e os meios de tratamento dos dados pessoais; sempre que as finalidades e os meios de tratamento sejam determinados por um ato da União específico, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União.
- (c) «Utilizador», qualquer pessoa singular que utilize uma rede ou um equipamento terminal que opere sob o controlo de uma instituição ou organismo da União;
- (d) «Lista», uma lista acessível ao público de utilizadores ou uma lista interna de utilizadores disponível numa instituição ou organismo da União ou partilhada entre instituições e organismos da União, em formato eletrónico ou impresso.

## CAPÍTULO II

### PRINCÍPIOS

#### *Artigo 4.º*

#### *Princípios relativos ao tratamento de dados pessoais*

- 1. Os dados pessoais devem ser:
  - a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
  - b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 13.º («limitação das finalidades»);

---

<sup>20</sup> Diretiva 2008/63/CE da Comissão, de 20 de junho de 2008, relativa à concorrência nos mercados de terminais de telecomunicações (JO L 162 de 21.6.2008, p. 20).

- c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);
  - d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas razoáveis para que os dados inexatos ou incompletos, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente, sejam apagados ou retificados sem demora («exatidão»);
  - e) Conservados de forma a permitir a identificação dos titulares de dados apenas durante o período necessário para a prossecução das finalidades para que são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 13.º, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
  - f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);
2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e deve poder comprová-lo («responsabilidade»).

#### *Artigo 5.º*

##### *Licitude do tratamento*

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
- a) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investida a instituição ou organismo da União;
  - b) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
  - c) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
  - d) O titular dos dados tiver dado o seu consentimento ao tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
  - e) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.
2. As tarefas referidas no n.º 1, alínea a), devem ser estabelecidas pelo direito da União.

#### *Artigo 6.º*

##### *Tratamento para outras finalidades compatíveis*

Sempre que o tratamento para finalidades diferentes daquelas para as quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União que constituam uma medida necessária e proporcionada numa

sociedade democrática para salvaguardar os objetivos referidos no artigo 25.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outras finalidades é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, deve ter nomeadamente em conta:

- a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
- c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 10.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 11.º;
- d) As eventuais consequências do tratamento posterior pretendido em relação aos titulares dos dados;
- e) A existência de garantias adequadas, que podem ser a cifragem ou a pseudonimização.

#### *Artigo 7.º*

##### *Condições aplicáveis ao consentimento*

1. Sempre que o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o consentimento ao tratamento dos seus dados pessoais.
2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outras matérias, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente dessas outras matérias de modo inteligível, de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. A retirada do consentimento deve ser tão fácil quanto a sua autorização.
4. 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.

#### *Artigo 8.º*

##### *Condições aplicáveis ao consentimento de crianças em relação aos serviços da sociedade da informação*

1. Sempre que for aplicável o artigo 5.º, n.º 1, alínea d), no que respeita à oferta direta de serviços da sociedade da informação às crianças, o tratamento dos dados pessoais de crianças é lícito se tiverem pelo menos 13 anos. Caso a criança tenha menos de 13

anos, o tratamento só é lícito se, e na medida em que, o consentimento seja dado ou autorizado pelos titulares da responsabilidade parental da criança.

2. Nesses casos, o responsável pelo tratamento deve envidar os esforços adequados para verificar se o consentimento foi dado ou autorizado pelo titular da responsabilidade parental da criança, tendo em conta a tecnologia disponível.
3. O disposto no n.º 1 não afeta o direito contratual geral dos Estados-Membros, como as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança.

#### *Artigo 9.º*

*Transmissões de dados pessoais a destinatários diferentes das instituições e organismos da União estabelecidos na União e abrangidos pelo Regulamento (UE) 2016/679 ou pela Diretiva (UE) 2016/680*

1. Sem prejuízo dos artigos 4.º, 5.º, 6.º e 10.º, os dados pessoais só podem ser transferidos para destinatários estabelecidos na União e abrangidos pelo Regulamento (UE) 2016/679, ou pelo direito nacional adotado de acordo com a Diretiva (UE) 2016/680, se o destinatário demonstrar o seguinte:
  - a) Os dados são necessários ao desempenho de funções de interesse público ou inerentes ao exercício da autoridade pública, ou
  - b) É necessário transmitir os dados, a transmissão é proporcionada para as finalidades a que se destinam e não existem motivos para pressupor que os direitos, liberdades e interesses legítimos do titular dos dados possam vir a ser prejudicados.
2. Sempre que a transmissão ocorra, nos termos do presente artigo, por iniciativa do responsável pelo tratamento, este deve demonstrar que a transmissão de dados pessoais é necessária e proporcionada para as finalidades a que se destina, aplicando os critérios referidos nas alíneas a) ou b) do n.º 1.

#### *Artigo 10.º*

*Tratamento de categorias especiais de dados pessoais*

1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:
  - a) O titular dos dados deu o seu consentimento explícito ao tratamento desses dados para uma ou mais finalidades específicas, exceto se o direito da União prever que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados; ou
  - b) O tratamento é necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União e preveja garantias adequadas aplicáveis aos direitos fundamentais e interesses do titular dos dados; ou

- c) O tratamento é necessário para proteger interesses vitais do titular dos dados ou de outra pessoa, se o titular dos dados estiver física ou legalmente incapacitado de dar o seu consentimento;
  - d) O tratamento é efetuado, no âmbito de atividades lícitas e mediante garantias adequadas, por um organismo sem fins lucrativos que constitua uma entidade integrada numa instituição ou num organismo da União e prossiga fins políticos, filosóficos, religiosos ou sindicais, desde que o tratamento se refira apenas aos membros ou antigos membros desse organismo ou a pessoas que com ele mantenham contactos regulares relacionados com os seus objetivos, e os dados não sejam divulgados a terceiros sem o consentimento dos titulares dos dados;
  - e) O tratamento está relacionado com dados manifestamente tornados públicos pelo seu titular;
  - f) O tratamento é necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que o Tribunal de Justiça da União Europeia atue no exercício da sua função jurisdicional; ou
  - g) O tratamento é necessário por motivos de interesse público importante, com base no direito da União, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
  - h) O tratamento é necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;
  - i) O tratamento é necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;
  - j) O tratamento é necessário para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, com base no direito da União, devendo ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.
3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se forem tratados por, ou sob a responsabilidade, de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União.

### *Artigo 11.º*

#### *Tratamento de dados pessoais relacionados com condenações penais e infrações*

O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas, nos termos do artigo 5.º, n.º 1, só é efetuado se o tratamento for autorizado por disposições do direito da União que prevejam garantias adequadas específicas para os direitos e liberdades dos titulares dos dados.

### *Artigo 12.º*

#### *Tratamento que não exige identificação*

1. Se as finalidades para as quais um responsável efetua o tratamento de dados pessoais não exigirem ou tiverem deixado de exigir a identificação do titular dos dados, esse responsável não é obrigado a manter, obter ou tratar informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento ao presente regulamento.
2. Sempre que, nos casos referidos no n.º 1 do presente artigo, o responsável pelo tratamento possa demonstrar que não está em condições de identificar o titular dos dados, informa-o, se possível, desse facto. Nesses casos, os artigos 17.º a 22.º não são aplicáveis, exceto se o titular dos dados, com a finalidade de exercer os seus direitos ao abrigo dos referidos artigos, fornecer informações adicionais que permitam a sua identificação.

### *Artigo 13.º*

#### *Garantias relativas ao tratamento para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos*

O tratamento para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, aplicáveis aos direitos e liberdades do titular dos dados. Essas garantias devem assegurar que estão criadas as medidas técnicas e organizativas visando respeitar, nomeadamente, o princípio da minimização de dados. Tais medidas podem incluir a pseudonimização, desde que esses fins possam ser alcançados desse modo. Sempre que esses fins possam ser atingidos por tratamentos ulteriores que não permitam ou tenham deixado de permitir a identificação dos titulares dos dados, os referidos fins são atingidos desse modo.

## **CAPÍTULO III**

### **DIREITOS DO TITULAR DOS DADOS**

#### **SECÇÃO 1**

#### **TRANSPARÊNCIA E REGRAS**

### *Artigo 14.º*

#### *Transparência das informações, das comunicações e das regras para o exercício dos direitos dos titulares dos dados*

1. O responsável pelo tratamento deve tomar as medidas adequadas para fornecer ao titular dos dados as informações a que se referem os artigos 15.º e 16.º, e qualquer

comunicação prevista nos artigos 17.º a 24.º e artigo 38.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

2. O responsável pelo tratamento deve facilitar o exercício dos direitos do titular dos dados, nos termos dos artigos 17.º a 24.º. Nos casos a que se refere o artigo 12.º, n.º 2, o responsável pelo tratamento não pode recusar dar seguimento ao pedido do titular no sentido de exercer os seus direitos ao abrigo dos artigos 17.º a 24.º, exceto se demonstrar que não está em condições de identificar o titular dos dados.
3. O responsável pelo tratamento deve fornecer ao titular dos dados informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 17.º a 24.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade e o número de pedidos. O responsável pelo tratamento deve informar o titular dos dados da eventual prorrogação e dos motivos da demora no prazo de um mês a contar da data de receção do pedido. Se o titular dos dados apresentar o pedido por meios eletrónicos, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.
4. Se o responsável pelo tratamento não der seguimento ao pedido apresentado pelo titular dos dados, informa-o sem demora e, o mais tardar, no prazo de um mês a contar da data de receção do pedido, das razões que o levaram a não tomar medidas e da possibilidade de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados e intentar uma ação judicial.
5. As informações fornecidas nos termos dos artigos 15.º e 16.º e quaisquer comunicações e medidas tomadas nos termos dos artigos 17.º a 24.º e artigo 38.º são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu carácter repetitivo, o responsável pelo tratamento pode recusar dar-lhes seguimento.

Cabe ao responsável pelo tratamento demonstrar o carácter manifestamente infundado ou excessivo do pedido.

6. Sem prejuízo do artigo 12.º, quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se referem os artigos 17.º a 23.º, pode solicitar que lhe sejam fornecidas as informações adicionais necessárias para confirmar a identidade do titular dos dados.
7. As informações a fornecer aos titulares dos dados, nos termos dos artigos 15.º e 16.º, podem ser combinadas com ícones normalizados, a fim de dar, de forma facilmente visível, inteligível e claramente legível, uma perspetiva geral e coerente do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática.
8. Se a Comissão adotar atos delegados, em conformidade com o artigo 12.º, n.º 8, do Regulamento (UE) 2016/679, a fim de determinar quais as informações a apresentar por meio de ícones e os procedimentos aplicáveis à comunicação de ícones normalizados, as instituições e organismos da União devem, quando apropriado,

prestar as informações nos termos dos artigos 15.º e 16.º em combinação com esses ícones normalizados.

## SECÇÃO 2

### INFORMAÇÃO E ACESSO AOS DADOS PESSOAIS

#### *Artigo 15.º*

*Informações a facultar quando os dados pessoais são recolhidos junto do titular*

1. Sempre que forem recolhidos dados pessoais junto do interessado, o responsável pelo tratamento deve facultar-lhe, aquando da recolha desses dados pessoais, todas as informações seguintes:
  - a) A identidade e os contactos do responsável pelo tratamento;
  - b) Os contactos do encarregado da proteção de dados;
  - c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
  - d) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
  - e) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas no artigo 49.º, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.
2. Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento deve fornecer ao interessado as seguintes informações adicionais, necessárias para garantir um tratamento leal e transparente:
  - a) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios aplicados para fixar esse prazo;
  - b) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou apagamento, ou a limitação do tratamento no respeitante ao titular dos dados, ou, sempre que aplicável, o direito de se opor ao tratamento ou o direito à portabilidade dos dados;
  - c) Se o tratamento dos dados se basear no artigo 5.º, n.º 1, alínea d), ou no artigo 10.º, n.º 2, alínea a), a existência do direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
  - d) O direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados;
  - e) Se a comunicação de dados pessoais constitui ou não um requisito legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;

- f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 24.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados;
- 3. Sempre que o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para uma finalidade diferente daquela para a qual os dados tenham sido recolhidos, antes desse tratamento o responsável deve fornecer ao titular dos dados informações sobre tal finalidade e qualquer outra informação pertinente referida no n.º 2.
  - 4. Os n.ºs 1, 2 e 3 não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações em causa.

#### *Artigo 16.º*

##### *Informações a facultar quando os dados pessoais não são recolhidos junto do titular*

- 1. Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento deve facultar-lhe as seguintes informações:
  - a) A identidade e os contactos do responsável pelo tratamento;
  - b) Os contactos do encarregado da proteção de dados;
  - c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
  - d) As categorias dos dados pessoais em questão;
  - e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
  - f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um destinatário num país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas no artigo 49.º, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas.
- 2. Para além das informações referidas no n.º 1, o responsável pelo tratamento deve facultar ao titular as seguintes informações adicionais, necessárias para lhe garantir um tratamento leal e transparente:
  - a) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios aplicados para fixar esse prazo;
  - b) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou apagamento, ou a limitação do tratamento no respeitante ao titular dos dados, ou, sempre que aplicável, o direito de se opor ao tratamento ou o direito à portabilidade dos dados;
  - c) Se o tratamento dos dados se basear no artigo 5.º, n.º 1, alínea d), ou no artigo 10.º, n.º 2, alínea a), a existência do direito de retirar o consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;

- d) O direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados;
  - e) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;
  - f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 24.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
3. O responsável pelo tratamento deve facultar as informações referidas nos n.ºs 1 e 2:
- (a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
  - (b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou
  - (c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.
4. Sempre que o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para uma finalidade diferente daquela para a qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável deve facultar ao titular dos dados informações sobre tal finalidade e quaisquer outras informações pertinentes referidas no n.º 2.
5. Os n.ºs 1 a 4 não se aplicam quando e na medida em que:
- a) O titular dos dados já tenha conhecimento das informações;
  - b) Se comprove a impossibilidade de disponibilizar a informação, ou o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, e na medida em que a obrigação referida no n.º 1 do presente artigo seja suscetível de impossibilitar ou prejudicar gravemente a concretização dos objetivos desse tratamento;
  - c) A obtenção ou divulgação dos dados esteja expressamente prevista no direito da União; ou
  - d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União.

#### *Artigo 17.º*

##### *Direito de acesso do titular dos dados*

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são eventualmente objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:
- a) As finalidades do tratamento dos dados;
  - b) As categorias dos dados pessoais em questão;

- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
  - d) Se for possível, o prazo previsto de conservação dos dados pessoais ou, não sendo possível, os critérios usados para fixar esse prazo;
  - e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
  - f) O direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados;
  - g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
  - h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 24.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 49.º relativo à transferência de dados.
  3. O responsável pelo tratamento deve facultar uma cópia dos dados pessoais em fase de tratamento. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário desse titular, a informação é facultada num formato eletrónico de uso corrente.
  4. O direito de obter uma cópia a que se refere o n.º 3 não deve prejudicar os direitos e as liberdades de terceiros.

### **SECÇÃO 3**

## **RETIFICAÇÃO E APAGAMENTO**

#### *Artigo 18.º Direito de retificação*

O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento, o titular dos dados tem direito a que os seus dados pessoais incompletos sejam completados, incluindo por meio de uma declaração adicional.

#### *Artigo 19.º Direito ao apagamento dos dados («direito a ser esquecido»)*

1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais sem demora injustificada, e esse responsável tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:
  - a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

- b) O titular dos dados retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 5.º, n.º 1, alínea d), ou do artigo 10.º, n.º 2, alínea a), e se não existir outro fundamento jurídico para o referido tratamento;
  - c) O titular dos dados opõe-se ao tratamento nos termos do artigo 23.º, n.º 1, e não existem interesses legítimos prevaletentes que justifiquem o tratamento;
  - d) Os dados pessoais foram tratados ilicitamente;
  - e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
  - f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referidos no artigo 8.º, n.º 1.
2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, deve tomar as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.
3. Os n.ºs 1 e 2 não se aplicam na medida em que o tratamento se revele necessário:
- a) Ao exercício da liberdade de expressão e de informação;
  - b) Ao cumprimento de uma obrigação legal a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
  - c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 10.º, n.º 2, alíneas h) e i), bem como do artigo 10.º, n.º 3;
  - d) Para fins de arquivo de interesse público, de investigação científica ou histórica ou para fins estatísticos, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a concretização dos objetivos desse tratamento; ou
  - e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

#### *Artigo 20.º*

##### *Direito à limitação do tratamento*

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, caso se aplique uma das seguintes situações:
- a) A contestação da exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a exatidão dos dados, incluindo a sua exaustividade;
  - b) O tratamento for ilícito e o titular dos dados se opuser ao seu apagamento e solicitar, em contrapartida, a limitação da sua utilização;
  - c) O responsável pelo tratamento já não necessitar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

- d) Se o titular se tiver oposto ao tratamento nos termos do artigo 23.º, n.º 1, até que seja verificado se os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.
2. Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos importantes de interesse público da União ou de um Estado-Membro.
3. O titular dos dados que tiver obtido a limitação do tratamento nos termos do n.º 1, é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.
4. Nos ficheiros automatizados, a limitação do tratamento deve ser, em princípio, assegurada por meios técnicos. O facto de os dados pessoais estarem limitados deve ser indicado no sistema de forma clara de modo a que esses dados não possam ser utilizados.

#### *Artigo 21.º*

##### *Obrigações de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento*

O responsável pelo tratamento deve comunicar a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 18.º, o artigo 19.º, n.º 1, e o artigo 20.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.

#### *Artigo 22.º*

##### *Direito de portabilidade dos dados*

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:
  - a) O tratamento se basear no consentimento dado nos termos do artigo 5.º, n.º 1, alínea d), ou do artigo 10.º, n.º 2, alínea a), ou num contrato referido no artigo 5.º, n.º 1, alínea c); e
  - b) O tratamento for realizado por meios automatizados.
2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.
3. O exercício do direito a que se refere o n.º 1 do presente artigo aplica-se sem prejuízo do artigo 19.º. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.
4. O direito a que se refere o n.º 1 não deve prejudicar os direitos e as liberdades de terceiros.

## SECÇÃO 4

### DIREITO DE OPOSIÇÃO E DECISÕES INDIVIDUAIS AUTOMATIZADAS

#### *Artigo 23.º*

#### *Direito de oposição*

1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 5.º, n.º 1, alínea a), incluindo a definição de perfis com base nessa disposição. O responsável pelo tratamento deve cessar o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se refere os n.º 1 deve ser explicitamente levado à atenção do titular dos dados, sendo apresentado de modo claro e separado de quaisquer outras informações.
3. Sem prejuízo dos artigos 34.º e 35.º, no contexto da utilização dos serviços da sociedade da informação, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.
4. Sempre que os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, o titular dos dados tem o direito de se opor, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito, salvo se tal tratamento for necessário por razões de interesse público.

#### *Artigo 24.º*

#### *Decisões individuais automatizadas incluindo definição de perfis*

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
2. O n.º 1 não se aplica se a decisão:
  - a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e o responsável pelo tratamento;
  - b) For autorizada pelo direito da União, e no qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados; ou
  - c) For baseada no consentimento explícito do titular dos dados.
3. Nos casos referidos no n.º 2, alíneas a) e c), o responsável pelo tratamento deve aplicar medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

4. As decisões referidas o n.º 2 não devem basear-se em categorias especiais de dados pessoais a que se refere o artigo 10.º, n.º 1, salvo se o n.º 2, alínea a) ou g) do mesmo artigo for aplicável e forem aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os interesses legítimos do titular.

## SECÇÃO 5

### LIMITAÇÕES

#### *Artigo 25.º*

#### *Limitações*

1. Os atos jurídicos adotados com base nos Tratados ou, em matérias relacionadas com o funcionamento das instituições e organismos da União, as normas internas estabelecidas por estes últimos podem limitar a aplicação dos artigos 14.º a 22.º, dos artigos 34.º e 38.º, assim como do artigo 4.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 14.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar:
- (a) A segurança nacional, a segurança pública e a defesa dos Estados-Membros;
  - (b) A prevenção, investigação, deteção e repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção contra ameaças à segurança pública;
  - (c) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental e fiscal, da saúde pública e da segurança social;
  - (d) A segurança interna das instituições e organismos da União, incluindo das respetivas redes de comunicação eletrónicas;
  - (e) A defesa da independência judiciária e dos processos judiciais;
  - (f) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;
  - (g) Uma missão de controlo, de inspeção ou de regulamentação associada, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas a) a c).
  - (h) A defesa do titular dos dados ou dos direitos e liberdades de outrem;
  - (i) A execução de ações cíveis.
2. Quando não esteja prevista uma limitação num ato jurídico adotado com base nos Tratados ou numa norma interna, em conformidade com o n.º 1, as instituições e organismos da União podem limitar a aplicação dos artigos 14.º a 22.º, dos artigos 34.º e 38.º, assim como do artigo 4.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 14.º a 22.º, se tal limitação respeitar a essência dos direitos e liberdades fundamentais, relativamente a um tratamento específico, e constituir uma medida necessária e proporcionada numa sociedade democrática para assegurar um ou mais dos objetivos referidos no n.º 1. Tal limitação deve ser notificada ao encarregado da proteção de dados competente.

3. Quando os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos, o direito da União, bem como eventuais normas internas, podem prever derrogações aos direitos a que se referem os artigos 17.º, 18.º, 20.º e 23.º, sob reserva das condições e garantias previstas no artigo 13.º, na medida em que esses direitos sejam suscetíveis de impossibilitar ou prejudicar gravemente a realização de finalidades específicas e tais derrogações sejam necessárias para a prossecução dessas finalidades.
4. Quando os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União, bem como eventuais normas internas, podem prever derrogações aos direitos a que se referem os artigos 17.º, 18.º, 20.º, 21.º, 22.º e 23.º, sob reserva das condições e garantias previstas no artigo 13.º, na medida em que esses direitos sejam suscetíveis de impossibilitar ou prejudicar gravemente a realização de finalidades específicas e tais derrogações sejam necessárias para a prossecução dessas finalidades.
5. As normas internas referidas nos n.ºs 1, 3 e 4 devem ser suficientemente claras, precisas e sujeitas a adequada publicação.
6. Se for imposta uma limitação nos termos dos n.ºs 1 ou 2, o titular dos dados deve ser informado, em conformidade com o direito da União, dos principais motivos de aplicação da limitação e do seu direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados.
7. Se for imposta uma limitação, nos termos dos n.ºs 1 ou 2, para negar o acesso ao titular dos dados, a Autoridade Europeia para a Proteção de Dados deve, ao investigar a reclamação, comunicar-lhe unicamente se os dados foram tratados corretamente e, em caso negativo, se foram introduzidas todas as correções necessárias.
8. A comunicação das informações referidas nos n.ºs 6 e 7, e no artigo 46.º, n.º 2, pode ser adiada, omitida ou recusada se anular o efeito da limitação imposta nos termos dos n.ºs 1 ou 2.

## **CAPÍTULO IV**

### **RESPONSÁVEL PELO TRATAMENTO E SUBCONTRATANTE**

#### **SECÇÃO 1**

#### **OBRIGAÇÕES GERAIS**

##### *Artigo 26.º*

##### *Responsabilidade do responsável pelo tratamento*

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

2. Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

#### *Artigo 27.º*

##### *Proteção de dados desde a conceção e por defeito*

1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento deve aplicar, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento deve aplicar medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

#### *Artigo 28.º*

##### *Responsáveis conjuntos pelo tratamento*

1. Sempre que uma instituição ou organismo da União, juntamente com um ou mais responsáveis pelo tratamento, que podem ou não ser instituições ou organismos da União, determinem conjuntamente as finalidades e os meios desse tratamento, devem ser considerados responsáveis conjuntos pelo tratamento. Devem determinar, por acordo entre si e de modo transparente, as respetivas responsabilidades pelo cumprimento dos deveres em matéria de proteção de dados, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de facultar as informações referidas nos artigos 15.º e 16.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O referido acordo pode designar um ponto de contacto para os titulares dos dados.
2. O acordo a que se refere o n.º 1 deve refletir devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. O conteúdo do acordo deve ser disponibilizado ao titular dos dados.
3. O titular dos dados pode exercer os direitos que lhe confere o presente regulamento em relação ou contra um ou mais responsáveis conjuntos pelo tratamento, tendo em conta as funções respetivas determinadas no acordo referido no n.º 1.

*Artigo 29.º*  
*Subcontratante*

1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento deve recorrer apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.
2. O subcontratante não deve contratar outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante deve informar o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.
3. O tratamento em subcontratação deve ser regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato, ou outro ato normativo, deve estipular, em especial, que o subcontratante:
  - a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados pessoais para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito; nesse caso, o subcontratante informa o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
  - b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
  - c) Adota todas as medidas exigidas nos termos do artigo 33.º;
  - d) Respeita as condições a que se referem os n.ºs 2 e 4 para contratar outro subcontratante;
  - e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III;
  - f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 33.º a 40.º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;
  - g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e

- h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

No que diz respeito à alínea h) do n.º 1, o subcontratante deve informar imediatamente o responsável pelo tratamento se, no seu entender, alguma instrução violar o presente regulamento ou outras disposições do direito da União ou dos Estados-Membros em matéria de proteção de dados.

4. Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no n.º 3, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do presente regulamento. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.
5. Sempre que o subcontratante não é uma instituição ou organismo da União, o facto de cumprir um código de conduta aprovado referido no artigo 40.º, n.º 5, do Regulamento (UE) 2016/679, ou um procedimento de certificação aprovado referido no artigo 42.º do Regulamento (UE) 2016/679, pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os n.ºs 1 e 4 do presente artigo.
6. Sem prejuízo de um eventual contrato individual entre o responsável pelo tratamento e o subcontratante, o contrato ou outro ato normativo referidos nos n.ºs 3 e 4 do presente artigo podem ser baseados, total ou parcialmente, nas cláusulas contratuais-tipo referidas nos n.ºs 7 e 8 do presente artigo, inclusivamente quando fazem parte de uma certificação concedida ao subcontratante que não seja uma instituição ou organismo da União ao abrigo do artigo 42.º do Regulamento (UE) 2016/679.
7. A Comissão pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos n.ºs 3 e 4 do presente artigo em conformidade com o procedimento de exame referido no artigo 70.º, n.º 2.
8. A Autoridade Europeia para a Proteção de Dados pode adotar cláusulas contratuais-tipo para as matérias referidas nos n.ºs 3 e 4.
9. O contrato ou outro ato normativo a que se referem os n.ºs 3 e 4, deve ser redigido por escrito, incluindo em formato eletrónico.
10. Sem prejuízo do disposto nos artigos 65.º e 66.º, o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, deve ser considerado responsável pelo tratamento no que respeita ao tratamento em questão.

### *Artigo 30.º*

#### *Tratamento sob a autoridade do responsável pelo tratamento e do subcontratante*

O subcontratante ou qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não deve proceder ao tratamento desses dados exceto por instrução do responsável pelo tratamento, salvo se tal for exigido pelo direito da União ou dos Estados-Membros.

### *Artigo 31.º*

#### *Registos das atividades de tratamento*

1. Cada responsável pelo tratamento deve conservar um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo devem constar todas as informações seguintes:
  - a) O nome e os contactos do responsável pelo tratamento de dados, do encarregado da proteção de dados e, se for caso disso, do subcontratante e de qualquer responsável conjunto pelo tratamento;
  - b) As finalidades do tratamento dos dados;
  - c) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
  - d) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em Estados-Membros, países terceiros ou organizações internacionais;
  - e) Se for aplicável, as transferências de dados pessoais para um país terceiro ou uma organização internacional, incluindo a identificação desse país terceiro ou dessa organização internacional, e a documentação que comprove a existência das garantias adequadas;
  - f) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;
  - g) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 33.º.
2. Cada subcontratante deve conservar um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constem:
  - a) O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual atua o subcontratante, bem como do encarregado da proteção de dados;
  - b) As categorias de tratamentos efetuados em nome de cada responsável pelo tratamento;
  - c) Se for aplicável, as transferências de dados pessoais para um país terceiro ou uma organização internacional, incluindo a identificação desse país terceiro ou dessa organização internacional, e a documentação que comprove a existência das garantias adequadas;
  - d) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 33.º.

3. Os registos a que se referem os n.ºs 1 e 2 são efetuados por escrito, incluindo em formato eletrónico.
4. As instituições e organismos da União devem disponibilizar, a pedido, os registos à Autoridade Europeia para a Proteção de Dados.
5. As instituições e organismos da União podem decidir conservar os seus registos de atividades de tratamento num registo central. Nesse caso, podem também decidir tornar o registo acessível ao público.

*Artigo 32.º*

*Cooperação com a Autoridade Europeia para a Proteção de Dados*

As instituições e organismos da União devem cooperar, a pedido, com a Autoridade Europeia para a Proteção de Dados no exercício das respetivas funções.

## **SECÇÃO 2**

### **SEGURANÇA DOS DADOS PESSOAIS E CONFIDENCIALIDADE DAS COMUNICAÇÕES ELETRÓNICAS**

*Artigo 33.º*

*Segurança do tratamento*

1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante devem aplicar as medidas técnicas e organizativas apropriadas para assegurar um nível de segurança adequado ao risco, incluindo, conforme adequado:
  - (a) A pseudonimização e a cifragem dos dados pessoais;
  - (b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
  - (c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
  - (d) Um processo visando testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
3. O responsável pelo tratamento e o subcontratante devem tomar medidas para assegurar que qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União.

#### *Artigo 34.º*

##### *Confidencialidade das comunicações eletrónicas*

As instituições e organismos da União devem assegurar a confidencialidade das comunicações eletrónicas, em especial garantindo a segurança das respetivas redes de comunicações eletrónicas.

#### *Artigo 35.º*

##### *Proteção de informações relacionadas com o equipamento terminal dos utilizadores finais*

As instituições e organismos da União devem proteger as informações relativas aos equipamentos terminais dos utilizadores finais que acedem aos respetivos sítios Web e aplicações móveis públicos em conformidade com o Regulamento (UE) XXXX/XX [novo regulamento sobre a privacidade e as comunicações eletrónicas], nomeadamente o artigo 8.º.

#### *Artigo 36.º*

##### *Listas de utilizadores*

1. Os dados pessoais inseridos em listas de utilizadores e o acesso a essas listas devem limitar-se ao estritamente necessário para os fins específicos das listas.
2. As instituições e organismos da União devem tomar todas as medidas necessárias para impedir que os dados pessoais incluídos nestas listas, independentemente de serem ou não acessíveis ao público, sejam utilizados para fins de marketing direto.

#### *Artigo 37.º*

##### *Notificação de uma violação de dados pessoais à Autoridade Europeia para a Proteção de Dados*

1. Em caso de violação de dados pessoais, o responsável pelo tratamento deve notificar desse facto a Autoridade Europeia para a Proteção de Dados sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que tal violação não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Sempre que a notificação à Autoridade Europeia para a Proteção de Dados não seja comunicada no prazo de 72 horas, deve ser acompanhada dos motivos do atraso.
2. O subcontratante deve notificar o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.
3. A notificação referida no n.º 1 deve, pelo menos:
  - a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
  - b) Comunicar o nome e contactos do encarregado da proteção de dados;
  - c) Descrever as consequências prováveis da violação de dados pessoais;
  - d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para remediar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;
4. Se, e na medida em que não seja possível comunicar todas as informações ao mesmo tempo, estas podem ser comunicadas por fases, sem demora injustificada.

5. O responsável pelo tratamento deve informar o encarregado da proteção de dados acerca da violação de dados pessoais.
6. O responsável pelo tratamento deve documentar qualquer violação de dados pessoais, compreendendo os factos relacionados com a mesma, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à Autoridade Europeia para a Proteção de Dados verificar o respeito do disposto no presente artigo.

#### *Artigo 38.º*

##### *Comunicação de uma violação de dados pessoais ao titular dos dados*

1. Sempre que a violação de dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento deve comunicar tal violação ao titular dos dados sem demora injustificada.
2. A comunicação ao titular dos dados a que se refere o n.º 1 do presente artigo deve descrever em linguagem clara e simples a natureza da violação dos dados pessoais e facultar, pelo menos, as informações e medidas referidas no artigo 37.º, n.º 3, alíneas b), c) e d).
3. A comunicação ao titular dos dados a que se refere o n.º 1 não é exigida se for preenchida uma das seguintes condições:
  - a) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;
  - b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1 já não é suscetível de se concretizar;
  - c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a Autoridade Europeia para a Proteção de Dados, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições referidas no n.º 3.

### **SECÇÃO 3**

## **AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS E CONSULTA PRÉVIA**

#### *Artigo 39.º*

##### *Avaliação de impacto sobre a proteção de dados*

1. Sempre que um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o

responsável pelo tratamento deve proceder, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento apresentar riscos elevados semelhantes, pode ser objeto de uma única e mesma avaliação.

2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento deve solicitar o parecer do encarregado da proteção de dados.
3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é especialmente obrigatória nos seguintes casos:
  - a) A avaliação sistemática aprofundada dos aspetos pessoais relacionados com pessoas singulares baseada no tratamento automatizado, incluindo a definição de perfis, e com base na qual são adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
  - b) O tratamento em grande escala de categorias especiais de dados referidos no artigo 10.º, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 11.º; ou
  - c) O controlo sistemático em grande escala de uma zona acessível ao público.
4. A Autoridade Europeia para a Proteção de Dados deve elaborar e tornar pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados em conformidade com o n.º 1.
5. A Autoridade Europeia para a Proteção de Dados pode também estabelecer e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados.
6. A avaliação deve incluir, pelo menos:
  - a) Uma descrição sistemática das operações de tratamento previstas e das finalidades do tratamento;
  - b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação às finalidades;
  - c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos direitos em conformidade com o n.º 1; e
  - d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os interesses legítimos dos titulares dos dados e de outros interessados afetados.
7. Ao avaliar o impacto das operações de tratamento efetuadas pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, deve ser tido em devida conta o respeito dos códigos de conduta aprovados a que se refere o artigo 40.º do Regulamento (UE) 2016/679 por parte dos subcontratantes que não sejam instituições e organismos da União.
8. Se for adequado, o responsável pelo tratamento deve solicitar a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses públicos ou da segurança das operações de tratamento.

9. Se o tratamento efetuado por força do artigo 5.º, n.º 1, alínea a) ou b), tiver por fundamento jurídico um ato jurídico adotado com base nos Tratados, e esse ato regular a operação ou conjuntos de operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto geral da proteção dos dados antes da adoção desse ato jurídico, não são aplicáveis os n.ºs 1 a 6, salvo disposição em contrário prevista no direito da União.
10. Se necessário, o responsável pelo tratamento deve proceder a um controlo para examinar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração do risco que as operações de tratamento representam.

*Artigo 40.º*  
*Consulta prévia*

1. O responsável pelo tratamento deve consultar a Autoridade Europeia para a Proteção de Dados antes do tratamento sempre que uma avaliação de impacto relativa à proteção de dados, nos termos do artigo 39.º, indicar que o tratamento, na falta de garantias, de medidas e de procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação. O responsável pelo tratamento deve solicitar o parecer do encarregado da proteção de dados sobre a necessidade da consulta prévia.
2. Sempre que a Autoridade Europeia para a Proteção de Dados considerar que o tratamento previsto referido no n.º 1 violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a referida autoridade, no prazo máximo de oito semanas a contar da receção do pedido de consulta, deve emitir orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante, e pode recorrer a todos os seus poderes referidos no artigo 59.º. Esse prazo pode ser prorrogado até seis semanas, tendo em conta a complexidade do tratamento previsto. A Autoridade Europeia para a Proteção de Dados deve informar da eventual prorrogação o responsável pelo tratamento e, se o houver, o subcontratante, no prazo de um mês a contar da data de receção do pedido de consulta, juntamente com os motivos do atraso. Esses prazos podem ser suspensos até que a Autoridade Europeia para a Proteção de Dados tenha obtido as informações solicitadas para efeitos da consulta.
3. Quando consultar a Autoridade Europeia para a Proteção de Dados nos termos do n.º 1, o responsável pelo tratamento deve comunicar-lhe os seguintes elementos:
  - a) Se for aplicável, a repartição de responsabilidades entre o responsável pelo tratamento, os responsáveis conjuntos pelo tratamento e os subcontratantes envolvidos no tratamento;
  - b) As finalidades e os meios do tratamento previsto;
  - c) As medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados nos termos do presente regulamento;
  - d) Os contactos do encarregado da proteção de dados;
  - e) A avaliação de impacto sobre a proteção de dados prevista no artigo 39.º; e

- f) Quaisquer outras informações solicitadas pela Autoridade Europeia para a Proteção de Dados.
4. A Comissão pode, mediante um ato de execução, determinar uma lista de casos em que os responsáveis pelo tratamento consultem a Autoridade Europeia para a Proteção de Dados e dela obtenham a autorização prévia no que diz respeito ao tratamento efetuado no exercício de uma missão de interesse público por um responsável pelo tratamento, incluindo o tratamento desses dados por motivos de proteção social e de saúde pública.

## SECÇÃO 4

### INFORMAÇÃO E CONSULTA LEGISLATIVA

#### *Artigo 41.º* *Informação*

As instituições e os organismos da União devem informar a Autoridade Europeia para a Proteção de Dados da elaboração de medidas administrativas e de normas internas relativas ao tratamento de dados pessoais que envolvam uma instituição ou organismo da União, individualmente ou em conjunto com outros.

#### *Artigo 42.º* *Consulta legislativa*

1. Após a adoção das propostas de ato legislativo e de recomendações ou de propostas ao Conselho, nos termos do artigo 218.º do TFUE, ou durante a elaboração de atos delegados ou de atos de execução que têm um impacto sobre a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão deve consultar a Autoridade Europeia para a Proteção de Dados.
2. Sempre que um ato referido no n.º 1 tem uma importância particular para a proteção dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão pode consultar igualmente o Comité Europeu para a Proteção de Dados. Nesses casos, a Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados devem coordenar o seu trabalho para emitirem um parecer conjunto.
3. O parecer referido nos n.ºs 1 e 2 é emitido por escrito no prazo de oito semanas a contar da receção do pedido de consulta mencionado nos n.ºs 1 e 2. Em casos urgentes, ou sempre que necessário, a Comissão pode reduzir tal prazo.
4. O presente artigo não se aplica quando a Comissão é obrigada, por força do Regulamento (UE) 2016/679, a consultar o Comité Europeu para a Proteção de Dados.

## SECÇÃO 5

### DEVER DE RESPOSTA A ALEGAÇÕES

#### *Artigo 43.º*

##### *Dever de resposta a alegações*

Sempre que a Autoridade Europeia para a Proteção de Dados exerce os poderes previstos no artigo 59.º, n.º 2, alíneas a), b) e c), o responsável pelo tratamento ou o subcontratante em questão deve comunicar-lhe a sua opinião, num prazo razoável que aquela autoridade fixará, tendo em conta as circunstâncias de cada caso. Essa resposta inclui igualmente uma descrição das medidas eventualmente adotadas na sequência das observações da Autoridade Europeia para a Proteção de Dados.

## SECÇÃO 6

### ENCARREGADO DA PROTEÇÃO DE DADOS

#### *Artigo 44.º*

##### *Designação do encarregado da proteção de dados*

1. Cada instituição ou organismo da União deve designar um encarregado da proteção de dados.
2. As instituições e organismos da União podem designar um único e mesmo encarregado da proteção de dados, tendo em conta a sua dimensão e estrutura organizativa.
3. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas em matéria de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 46.º.
4. O encarregado da proteção de dados pode ser um elemento do pessoal da instituição ou organismo da União, ou exercer as suas funções com base num contrato de prestação de serviços.
5. As instituições e organismos da União devem publicar os contactos do encarregado da proteção de dados e comunicam-nos à Autoridade Europeia para a Proteção de Dados.

#### *Artigo 45.º*

##### *Posição do encarregado da proteção de dados*

1. As instituições e organismos da União devem assegurar que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, em todas as matérias relacionadas com a proteção de dados pessoais.
2. As instituições e organismos da União devem apoiar o encarregado da proteção de dados no exercício das funções referidas no artigo 46.º, fornecendo-lhe os recursos necessários ao desempenho dessas funções, bem como o acesso aos dados pessoais e às operações de tratamento, permitindo-lhe a manutenção dos seus conhecimentos especializados.

3. As instituições e organismos da União devem assegurar que o encarregado da proteção de dados não recebe qualquer instrução no que diz respeito ao exercício das suas funções. O encarregado não pode ser demitido nem penalizado pelo responsável pelo tratamento ou pelo subcontratante devido ao facto de exercer as suas funções. O encarregado da proteção de dados tem o dever de informar diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.
4. Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas matérias relacionadas com o tratamento dos seus dados pessoais e o exercício dos direitos que lhes são conferidos pelo presente regulamento.
5. O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União.
6. O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante devem assegurar que essas funções e atribuições não resultam num conflito de interesses.
7. O encarregado da proteção de dados pode ser consultado diretamente, sem necessidade de recorrer à via oficial, sobre qualquer questão relativa à interpretação ou aplicação do presente regulamento pelo responsável pelo tratamento e pelo subcontratante, pelo Comité do Pessoal ou por qualquer outra pessoa singular. Nenhuma pessoa pode ser prejudicada por ter levado ao conhecimento do encarregado da proteção de dados competente uma alegada violação das disposições do presente regulamento.
8. O encarregado da proteção de dados é designado por um período de três a cinco anos e o seu mandato é renovável. O encarregado da proteção de dados pode ser demitido das suas funções pela instituição ou organismo da União que o nomeou unicamente com o acordo da Autoridade Europeia para a Proteção de Dados se deixar de preencher as condições exigidas para o exercício das suas funções.
9. Após a nomeação do encarregado da proteção de dados, o seu nome é comunicado à Autoridade Europeia para a Proteção de Dados pela instituição ou organismo da União que o tenha nomeado.

#### *Artigo 46.º*

##### *Funções do encarregado da proteção de dados*

1. O encarregado da proteção de dados tem as seguintes funções:
  - (a) Informar e aconselhar o responsável pelo tratamento ou o subcontratante, bem como os membros do pessoal que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União;
  - (b) Garantir de forma independente a aplicação interna do presente regulamento e controlar o respeito do presente regulamento, de outras disposições de proteção de dados do direito da União aplicáveis e das regras internas do responsável pelo tratamento ou do subcontratante em matéria de proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e a formação do pessoal envolvido nas operações de tratamento de dados, e as auditorias correspondentes;

- (c) Garantir que os titulares dos dados são informados dos seus direitos e deveres nos termos do presente regulamento;
  - (d) Prestar aconselhamento, quando tal lhe for solicitado, sobre a necessidade de notificar ou comunicar uma violação de dados pessoais, em conformidade com os artigos 37.º e 38.º;
  - (e) Prestar aconselhamento, quando tal lhe for solicitado, no que diz respeito à avaliação de impacto sobre a proteção de dados e ao controlo da sua aplicação nos termos do artigo 39.º, e consultar a Autoridade Europeia para a Proteção de Dados em caso de dúvida quanto à necessidade de uma avaliação de impacto sobre a proteção de dados;
  - (f) Prestar aconselhamento, quando tal lhe for solicitado, sobre necessidade de consulta prévia da Autoridade Europeia para a Proteção de Dados nos termos do artigo 40.º, e consultar esta autoridade em caso de dúvida quanto à necessidade de a consultar previamente;
  - (g) Responder aos pedidos da Autoridade Europeia para a Proteção de Dados, e dentro do âmbito da sua esfera de competência, cooperar e consultar a referida autoridade a pedido desta ou por sua própria iniciativa;
2. O encarregado da proteção de dados pode emitir recomendações, a fim de melhorar concretamente a proteção de dados, dirigidas ao responsável pelo tratamento e ao subcontratante, bem como aconselhá-los sobre matérias relativas à aplicação das disposições relativas à proteção de dados. Além disso, por sua própria iniciativa ou a pedido do responsável pelo tratamento ou do subcontratante, do Comité de Pessoal ou de qualquer pessoa singular, pode investigar questões e factos diretamente relacionados com as suas funções e de que tenha tido conhecimento, e prestar informações à pessoa que solicitou essa investigação ou ao responsável pelo tratamento ou ao subcontratante.
3. Serão adotadas disposições de execução complementares respeitantes ao encarregado da proteção de dados por cada instituição ou organismo da União. Essas normas incidirão sobre as funções e competências do encarregado da proteção de dados.

## **CAPÍTULO V**

### **Transferências de dados pessoais para países terceiros ou organizações internacionais**

#### *Artigo 47.º*

#### *Princípio geral das transferências*

Qualquer transferência de dados pessoais, que sejam ou venham a ser objeto de tratamento após a transferência para um país terceiro ou uma organização internacional, só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento e pelo subcontratante, inclusivamente no que diz respeito às transferências ulteriores de dados pessoais do país terceiro ou da organização internacional para outro país terceiro ou outra organização internacional. Todas as disposições do presente capítulo devem ser aplicadas de forma a assegurar que não é comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.

#### *Artigo 48.º*

##### *Transferências com base numa decisão de adequação*

1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido, por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, que é garantido um nível de proteção adequado no país terceiro, num território ou num ou mais sectores específicos desse país terceiro ou dessa organização internacional, e se os dados pessoais forem transferidos exclusivamente para o desempenho de funções da competência do responsável pelo tratamento.
2. As instituições e os organismos da União devem informar a Comissão e a Autoridade Europeia para a Proteção de Dados dos casos em que consideram que o país terceiro ou a organização internacional em questão não assegura um nível de proteção adequado nos termos do n.º 1.
3. As instituições e organismos da União devem tomar as medidas necessárias para se conformar com as decisões adotadas pela Comissão, verificando, por força do artigo 45.º, n.ºs 3 e 5, do Regulamento (UE) 2016/679, se determinado país terceiro ou organização internacional assegura ou deixou de assegurar um nível de proteção adequado.

#### *Artigo 49.º*

##### *Transferências sujeitas a garantias adequadas*

1. Não tendo sido tomada qualquer decisão por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, os responsáveis pelo tratamento ou os subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.
2. Podem ser previstas as garantias adequadas referidas no n.º 1, sem requerer nenhuma autorização específica da Autoridade Europeia para a Proteção de Dados, por meio de:
  - (a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
  - (b) Cláusulas-tipo de proteção de dados adotadas pela Comissão mediante o procedimento de exame referido no artigo 70.º, n.º 2;
  - (c) Cláusulas-tipo de proteção de dados adotadas pela Autoridade Europeia para a Proteção de Dados e aprovadas pela Comissão mediante o procedimento de exame referido no artigo 70.º, n.º 2;
  - (d) Regras vinculativas aplicáveis às empresas, códigos de conduta e procedimentos de certificação, em conformidade com o artigo 46.º, n.º 2, alíneas b), e) e f), do Regulamento (UE) 2016/679, nos casos em que o subcontratante não é uma instituição ou organismo da União.
3. Sob reserva de autorização da Autoridade Europeia para a Proteção de Dados, podem também ser previstas as garantias adequadas referidas no n.º 1, nomeadamente por meio de:

- (a) Cláusulas contratuais entre o responsável pelo tratamento ou o subcontratante e o responsável pelo tratamento, o subcontratante ou o destinatário dos dados pessoais no país terceiro ou na organização internacional; ou
  - (b) Disposições a inserir nos acordos administrativos entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.
4. As instituições e os organismos da União devem informar a Autoridade Europeia para a Proteção de Dados das categorias de casos em que se aplicou o presente artigo.
5. As autorizações concedidas pela Autoridade Europeia para a Proteção de Dado, com base no artigo 9.º, n.º 7, do Regulamento (CE) n.º 45/2001, continuam válidas até à sua alteração, substituição ou revogação, se necessário, pela mesma autoridade.

#### *Artigo 50.º*

##### *Transferências ou divulgações não autorizadas pelo direito da União*

As decisões judiciais e as decisões de autoridades administrativas de um país terceiro exigindo que o responsável pelo tratamento ou o subcontratante transfira ou divulgue dados pessoais só são reconhecidas ou executadas se tiverem por base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União, sem prejuízo de outros motivos de transferência em conformidade com o presente capítulo.

#### *Artigo 51.º*

##### *Derrogações em situações específicas*

1. Na falta de uma decisão por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, ou de garantias adequadas em conformidade com o artigo 49.º, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições:
- (a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
  - (b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
  - (c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;
  - (d) A transferência for necessária por razões importantes de interesse público;
  - (e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial; ou
  - (f) A transferência for necessária para proteger os interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento; ou

- (g) A transferência for realizada a partir de um registo que, nos termos do direito da União, se destine à informação do público e se encontre aberto à consulta do público ou de qualquer pessoa que possa provar um interesse legítimo, mas apenas na medida em que as condições estabelecidas para a consulta no direito da União sejam cumpridas no caso concreto.
2. Uma transferência efetuada nos termos do n.º 1, alínea g), não deve envolver a totalidade dos dados pessoais nem categorias completas de dados pessoais constantes do registo, a não ser que seja autorizada pelo direito da União. Quando o registo se destinar a ser consultado por pessoas com um interesse legítimo, as transferências só podem ser efetuadas a pedido dessas pessoas ou se forem elas os seus destinatários.
  3. O interesse público referido na alínea d) do n.º 1 deve ser reconhecido no direito da União.
  4. Na falta de uma decisão de adequação, o direito da União pode, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados pessoais para países terceiros ou organizações internacionais.
  5. As instituições e os organismos da União devem informar a Autoridade Europeia para a Proteção de Dados das categorias de casos em que se aplicou o presente artigo.

#### *Artigo 52.º*

##### *Cooperação internacional no domínio da proteção de dados pessoais*

Em relação a países terceiros e a organizações internacionais, a Autoridade Europeia para a Proteção de Dados, em cooperação com a Comissão e o Comité Europeu para a Proteção de Dados, deve tomar as medidas necessárias para:

- (a) Estabelecer normas internacionais de cooperação destinadas a facilitar a aplicação efetiva da legislação em matéria de proteção de dados pessoais;
- (b) Prestar assistência mútua a nível internacional no domínio da aplicação da legislação relativa à proteção de dados pessoais, nomeadamente através da notificação, comunicação de reclamações, assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;
- (c) Associar as partes interessadas aos debates e atividades que visem intensificar a cooperação internacional no âmbito da aplicação da legislação relativa à proteção de dados pessoais;
- (d) Promover o intercâmbio e a documentação da legislação e das práticas em matéria de proteção de dados pessoais, incluindo no que diz respeito a conflitos de competência com países terceiros.

## CAPÍTULO VI

### AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

#### *Artigo 53.º*

##### *Autoridade Europeia para a Proteção de Dados*

1. É instituída a Autoridade Europeia para a Proteção de Dados.
2. No que diz respeito ao tratamento de dados pessoais, a Autoridade Europeia para a Proteção de Dados é encarregada de assegurar que os direitos e liberdades fundamentais das pessoas singulares, especialmente o direito à proteção de dados, são respeitados pelas instituições e organismos da União.
3. A Autoridade Europeia para a Proteção de Dados é encarregada do controlo e da aplicação das disposições do presente regulamento e de qualquer outro ato da União relativo à proteção dos direitos e liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais por uma instituição ou organismo da União, bem como do aconselhamento das instituições e organismos da União e dos titulares dos dados sobre todas as questões relativas ao tratamento de dados pessoais. Para esses fins, a Autoridade Europeia para a Proteção de Dados exerce as atribuições previstas no artigo 58.º e os poderes conferidos pelo artigo 59.º.

#### *Artigo 54.º*

##### *Nomeação da Autoridade Europeia para a Proteção de Dados*

1. O Parlamento Europeu e o Conselho nomeiam, de comum acordo, a Autoridade Europeia para a Proteção de Dados por um período de cinco anos, com base numa lista estabelecida pela Comissão na sequência de um convite público à apresentação de candidaturas. Esse convite público à apresentação de candidaturas permite a todas as pessoas interessadas na União apresentarem as suas candidaturas. A lista de candidatos estabelecida pela Comissão é pública. A comissão competente do Parlamento Europeu, com base na lista elaborada pela Comissão, pode decidir realizar uma audição de forma a poder exprimir a sua preferência.
2. A lista elaborada pela Comissão, a partir da qual a Autoridade Europeia para a Proteção de Dados é escolhida, deve ser constituída por pessoas que ofereçam todas as garantias de independência e disponham da experiência e competência requeridas para o desempenho das funções de Autoridade Europeia para a Proteção de Dados, por exemplo porque pertencem ou pertenceram às autoridades de controlo instituídas ao abrigo do artigo 41.º do Regulamento (UE) 2016/679.
3. O mandato da Autoridade Europeia para a Proteção de Dados é renovável uma vez.
4. As funções da Autoridade Europeia para a Proteção de Dados cessam nas seguintes circunstâncias:
  - (a) Em caso de substituição da Autoridade Europeia para a Proteção de Dados;
  - (b) Em caso de renúncia da Autoridade Europeia para a Proteção de Dados;
  - (c) Em caso de demissão ou de aposentação compulsiva da Autoridade Europeia para a Proteção de Dados.

5. A Autoridade Europeia para a Proteção de Dados pode ser declarada demissionária ou privada do seu direito à pensão ou a outros benefícios equivalentes por decisão do Tribunal de Justiça da União Europeia, a pedido do Parlamento Europeu, do Conselho ou da Comissão, se deixar de preencher os requisitos necessários ao exercício das suas funções ou tiver cometido uma falta grave.
6. Nos casos de substituição regular ou de demissão voluntária, a Autoridade Europeia para a Proteção de Dados permanece, no entanto, em funções até que se proceda à sua substituição.
7. Os artigos 11.º a 14.º e 17.º do Protocolo relativo aos Privilégios e Imunidades da União Europeia são igualmente aplicáveis à Autoridade Europeia para a Proteção de Dados.

#### *Artigo 55.º*

#### *Estatuto e condições gerais de exercício das funções da Autoridade Europeia para a Proteção de Dados, recursos humanos e financeiros*

1. A Autoridade Europeia para a Proteção de Dados é considerada equiparada a um juiz do Tribunal de Justiça da União Europeia no que se refere à determinação da sua remuneração, subsídios, pensão de reforma e qualquer outro benefício equivalente à remuneração.
2. A autoridade orçamental deve assegurar que a Autoridade Europeia para a Proteção de Dados dispõe dos recursos humanos e financeiros necessários ao desempenho das suas funções.
3. O orçamento da Autoridade Europeia para a Proteção de Dados deve figurar numa rubrica específica da secção IX do orçamento geral da União Europeia.
4. A Autoridade Europeia para a Proteção de Dados é assistida por um secretariado. Os funcionários e outros agentes do secretariado são nomeados pela Autoridade Europeia para a Proteção de Dados, que é o seu superior hierárquico e de quem dependem exclusivamente. O seu número é aprovado anualmente no âmbito do exercício orçamental.
5. Os funcionários e outros agentes do secretariado da Autoridade Europeia para a Proteção de Dados estão sujeitos às normas e regulamentação aplicáveis aos funcionários e outros agentes da União Europeia.
6. A Autoridade Europeia para a Proteção de Dados tem sede em Bruxelas.

#### *Artigo 56.º*

#### *Independência*

1. A Autoridade Europeia para a Proteção de Dados deve exercer com total independência as atribuições e poderes que lhe são conferidos em conformidade com o presente regulamento.
2. A Autoridade Europeia para a Proteção de Dados não está sujeita a influências externas, diretas ou indiretas, no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicita nem recebe instruções de outrem.

3. A Autoridade Europeia para a Proteção de Dados deve abster-se de qualquer ato incompatível com as suas atribuições e, durante o seu mandato, não pode desempenhar qualquer outra atividade profissional, remunerada ou não.
4. Cessadas as suas funções, a Autoridade Europeia para a Proteção de Dados deve agir com integridade e discrição relativamente à aceitação de determinadas funções e benefícios.

*Artigo 57.º*  
*Sigilo profissional*

A Autoridade Europeia para a Proteção de Dados e o seu pessoal ficam, durante o respetivo mandato e após a cessação deste, sujeitos à obrigação de sigilo profissional quanto às informações confidenciais a que tenham tido acesso no desempenho das suas funções.

*Artigo 58.º*  
*Atribuições*

1. Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, a Autoridade Europeia para a Proteção de Dados:
  - (a) Controla e garante a aplicação do presente regulamento e de qualquer outro ato da União relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais por qualquer instituição ou organismo da União, com exceção do tratamento de dados pessoais pelo Tribunal de Justiça da União Europeia no exercício das suas funções jurisdicionais;
  - (b) Promove a sensibilização do público e a sua compreensão dos riscos, normas, garantias e direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser objeto de uma atenção especial;
  - (c) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento;
  - (d) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito;
  - (e) Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação em conformidade com o artigo 67.º, e investiga, na medida do necessário, o conteúdo da reclamação e informa o interessado do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares em conjunto com outra autoridade de controlo;
  - (f) Conduz investigações sobre a aplicação do presente regulamento, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;
  - (g) Presta aconselhamento a todas as instituições e organismos da União quanto a medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades de pessoas singulares no que diz respeito ao tratamento de dados pessoais;

- (h) Acompanha factos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações;
  - (i) Adota as cláusulas contratuais-tipo previstas no artigo 29.º, n.º 8, e no artigo 49.º, n.º 2, alínea c);
  - (j) Elabora e conserva uma lista associada à exigência de realizar uma avaliação de impacto sobre a proteção de dados, em conformidade com o artigo 39.º, n.º 4;
  - (k) Participa nas atividades do Comité Europeu para a Proteção de Dados instituído pelo artigo 68.º do Regulamento (UE) 2016/679;
  - (l) Assegura o secretariado do Comité Europeu para a Proteção de Dados, em conformidade com o artigo 75.º do Regulamento (UE) 2016/679;
  - (m) Presta aconselhamento sobre o tratamento referido no artigo 40.º, n.º 2;
  - (n) Autoriza as cláusulas contratuais e as disposições referidas no artigo 49.º, n.º 3;
  - (o) Conserva registos internos de violações do presente regulamento e das medidas tomadas em conformidade com o artigo 59.º, n.º 2;
  - (p) Desempenha qualquer outra atribuição relacionada com a proteção de dados pessoais; e
  - (q) Elabora o seu regulamento interno.
2. A Autoridade Europeia para a Proteção de Dados deve facilitar a apresentação das reclamações previstas no n.º 1, alínea e), disponibilizando o formulário de reclamação que possa ser igualmente preenchido eletronicamente, sem excluir outros meios de comunicação.
3. O exercício das atribuições da Autoridade Europeia para a Proteção de Dados é gratuito para o titular dos dados.
4. Sempre que os pedidos são manifestamente infundados ou excessivos, nomeadamente devido ao seu carácter repetitivo, a Autoridade Europeia para a Proteção de Dados pode recusar-se a dar-lhes seguimento. Cabe à Autoridade Europeia para a Proteção de Dados demonstrar o carácter manifestamente infundado ou excessivo de um pedido.

*Artigo 59.º*  
*Poderes*

1. A Autoridade Europeia para a Proteção de Dados dispõe dos seguintes poderes de investigação:
- (a) Ordenar que o responsável pelo tratamento e o subcontratante lhe forneçam as informações de que necessita para o desempenho das suas funções;
  - (b) Realizar investigações sob a forma de auditorias sobre a proteção de dados;
  - (c) Notificar o responsável pelo tratamento ou o subcontratante de alegadas violações do presente regulamento;
  - (d) Obter, da parte do responsável pelo tratamento e do subcontratante, acesso a todos os dados pessoais e a todas as informações necessárias ao exercício das suas funções;

- (e) Obter acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União ou dos Estados-Membros;
2. A Autoridade Europeia para a Proteção de Dados dispõe dos seguintes poderes de correção:
- (a) Advertir o responsável pelo tratamento ou o subcontratante de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento;
  - (b) Repreender o responsável pelo tratamento ou o subcontratante sempre que operações de tratamento tenham violado as disposições do presente regulamento;
  - (c) Submeter a questão ao responsável pelo tratamento ou ao subcontratante em causa e, se necessário, ao Parlamento Europeu, ao Conselho e à Comissão;
  - (d) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos apresentados pelo titular dos dados tendo em vista exercer os seus direitos em conformidade com o presente regulamento;
  - (e) Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um determinado prazo;
  - (f) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais;
  - (g) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;
  - (h) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 18.º, 19.º e 20.º, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 19.º, n.º 2, e do artigo 21.º;
  - (i) Impor uma coima nos termos do artigo 66.º, caso a instituição ou organismo da União não respeite alguma das medidas referidas no presente número e em função das circunstâncias de cada caso;
  - (j) Ordenar a suspensão dos fluxos de dados para um destinatário num Estado-Membro, num país terceiro ou uma organização internacional.
3. A Autoridade Europeia para a Proteção de Dados dispõe dos seguintes poderes de autorização e consultivos:
- (a) Aconselhar os titulares de dados sobre o exercício dos seus direitos;
  - (b) Aconselhar o responsável pelo tratamento, em conformidade com o procedimento de consulta prévia referido no artigo 40.º;
  - (c) Emitir, por iniciativa própria ou a pedido, pareceres dirigidos a instituições e organismos da União, bem como ao público, sobre qualquer matéria relacionada com a proteção de dados pessoais;
  - (d) Adotar as cláusulas-tipo de proteção de dados previstas no artigo 29.º, n.º 8, e no artigo 49.º, n.º 2, alínea c);

- (e) Autorizar as cláusulas contratuais referidas no artigo 49.º, n.º 3, alínea a);
  - (f) Autorizar os acordos administrativos referidos no artigo 49.º, n.º 3, alínea b).
4. O exercício dos poderes conferidos à Autoridade Europeia para a Proteção de Dados nos termos do presente artigo está subordinado a garantias adequadas, incluindo o direito a uma ação judicial efetiva e a um processo equitativo, previsto no direito da União.
  5. A Autoridade Europeia para a Proteção de Dados dispõe do poder de submeter uma questão à apreciação do Tribunal de Justiça da União Europeia nas condições previstas no Tratado e de intervir em processos judiciais no Tribunal de Justiça da União Europeia.

#### *Artigo 60.º*

##### *Relatório de atividades*

1. A Autoridade Europeia para a Proteção de Dados deve apresentar ao Parlamento Europeu, ao Conselho e à Comissão um relatório anual de atividades, que publica em paralelo.
2. A Autoridade Europeia para a Proteção de Dados transmite o relatório de atividades aos demais organismos e instituições da União, que podem apresentar observações tendo em vista um eventual exame do relatório pelo Parlamento Europeu.

## **CAPÍTULO VII**

### **COOPERAÇÃO E COERÊNCIA**

#### *Artigo 61.º*

##### *Cooperação com as autoridades nacionais de controlo*

A Autoridade Europeia para a Proteção de Dados deve cooperar com as autoridades de controlo instituídas a título do artigo 41.º do Regulamento (UE) 2016/679 e do artigo 51.º da Diretiva (UE) 2016/680 (doravante «autoridades nacionais de controlo»), bem como com a Autoridade Comum de Controlo, instituída a título do artigo 25.º da Decisão 2009/917/JAI do Conselho<sup>21</sup>, na medida necessária ao cumprimento das suas obrigações respetivas, em especial partilhando informações relevantes, solicitando às autoridades de controlo nacionais que exerçam os seus poderes ou respondendo a pedidos destas autoridades.

#### *Artigo 62.º*

##### *Supervisão coordenada pela Autoridade Europeia para a Proteção de Dados e pelas autoridades de controlo nacionais*

1. Sempre que um ato da União faça referência ao presente artigo, a Autoridade Europeia para a Proteção de Dados deve cooperar ativamente com as autoridades nacionais de controlo, a fim de assegurar uma supervisão eficaz dos sistemas informáticos de grande escala ou das agências da União.

---

<sup>21</sup> Decisão 2009/917/JAI do Conselho, de 30 de novembro de 2009, relativa à utilização da informática no domínio aduaneiro, JO L 323 de 10.12.2009, pp. 20–30.

2. A Autoridade Europeia para a Proteção de Dados, agindo no âmbito das suas competências e responsabilidades, deve partilhar informações relevantes, prestar assistência na realização de auditorias e inspeções, examinar as dificuldades de interpretação ou de aplicação do presente regulamento e de outros atos aplicáveis da União, examinar problemas suscetíveis de resultar do exercício de um controlo independente ou do exercício dos direitos dos titulares dos dados, elaborar propostas harmonizadas para resolver eventuais problemas e sensibilizar o público para os direitos de proteção de dados, se necessário em conjunto com as autoridades nacionais de controlo.
3. Para os efeitos referidos no n.º 2, a Autoridade Europeia para a Proteção de Dados deve reunir-se com as autoridades nacionais de controlo pelo menos duas vezes por ano no quadro do Comité Europeu para a Proteção de Dados. Os custos e a organização dessas reuniões são suportados pelo Comité Europeu para a Proteção de Dados. O regulamento interno é aprovado na primeira reunião. Outros métodos de trabalho são definidos conjuntamente, em função das necessidades.
4. O Comité Europeu para a Proteção de Dados apresenta, de dois em dois anos, ao Parlamento Europeu, ao Conselho e à Comissão um relatório de atividades conjunto relativo aos controlos realizados.

## **CAPÍTULO VIII**

### **VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES**

#### *Artigo 63.º*

##### *Direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados*

1. Sem prejuízo de qualquer outra via de recurso judicial, administrativo ou extrajudicial, cada titular de dados tem o direito de apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados se considerar que o tratamento dos seus dados pessoais constitui uma violação do presente regulamento.
2. A Autoridade Europeia para a Proteção de Dados deve informar o titular dos dados do andamento e do resultado da reclamação apresentada, nomeadamente da possibilidade de intentar uma ação judicial ao abrigo do artigo 64.º.
3. Se a Autoridade Europeia para a Proteção de Dados não tratar uma reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da referida reclamação, considera-se que a mesma foi indeferida.

#### *Artigo 64.º*

##### *Direito à ação judicial*

O Tribunal de Justiça da União Europeia é competente para apreciar todos os litígios relacionados com o disposto no presente regulamento, incluindo as ações de indemnização.

#### *Artigo 65.º*

##### *Direito de indemnização*

Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem o direito a receber uma indemnização do responsável pelo

tratamento ou do subcontratante pelos danos causados, sob reserva das condições previstas nos Tratados.

*Artigo 66.º*  
*Coimas*

1. A Autoridade Europeia para a Proteção de Dados pode impor coimas a instituições e organismos da União, em função das circunstâncias de cada caso, se uma instituição ou organismo da União não cumprir uma ordem da Autoridade Europeia para a Proteção de Dados em conformidade com o artigo 59.º, n.º 2, alíneas d) a h) e j). Ao decidir sobre a eventual imposição de uma coima e o seu montante, deve ter em conta, em cada caso individual, os seguintes elementos:
  - (a) A natureza, a gravidade e a duração da infração, tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos sofridos;
  - (b) Qualquer medida tomada pela instituição ou organismo da União para atenuar os danos sofridos pelos titulares;
  - (c) O grau de responsabilidade da instituição ou organismo da União, tendo em conta as medidas técnicas e organizativas que aplicaram por força dos artigos 27.º e 33.º;
  - (d) Qualquer violação similar anteriormente cometida pela instituição ou organismo da União;
  - (e) O grau de cooperação com a Autoridade Europeia para a Proteção de Dados tendo em vista sanar a violação e atenuar os seus eventuais efeitos negativos;
  - (f) As categorias de dados pessoais específicas afetadas pela violação;
  - (g) A forma como a Autoridade Europeia para a Proteção de Dados tomou conhecimento da infração, em especial se a instituição ou organismo da União a notificou e, em caso afirmativo, em que medida o fez;
  - (h) O cumprimento das medidas a que se refere o artigo 59.º, caso tenham sido previamente impostas à instituição ou organismo da União em causa relativamente à mesma matéria;

Os procedimentos que levam à imposição de coimas devem ser executados num prazo razoável, em função das circunstâncias de cada caso, e tendo em conta as ações e procedimentos aplicáveis referidos no artigo 69.º.

2. A violação das obrigações pela instituição ou organismo da União, em conformidade com os artigos 8.º, 12.º, 27.º, 28.º, 29.º, 30.º, 31.º, 32.º, 33.º, 37.º, 38.º, 39.º, 40.º, 44.º, 45.º e 46.º deve, em conformidade com o n.º 1, ser sujeita a coimas até um total de 25 000 EUR por infração e até um total de 250 000 EUR por ano.
3. A violação das disposições seguintes pela instituição ou organismo da União deve, em conformidade com o n.º 1, ser sujeita a coimas até um total de 50 000 EUR por infração e até um total de 500 000 EUR por ano:
  - (a) Os princípios básicos do tratamento, incluindo as condições aplicáveis ao consentimento, por força dos artigos 4.º, 5.º, 7.º e 10.º;
  - (b) Os direitos dos titulares dos dados, por força dos artigos 14.º a 24.º;

- (c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional, por força dos artigos 47.º a 51.º.
4. Se uma instituição ou organismo da União violar, no âmbito da mesma operação de tratamento ou de operações de tratamento ligadas ou contínuas, várias disposições do presente regulamento ou várias vezes a mesma disposição, o montante total da coima não pode exceder o montante fixado para a infração mais grave.
  5. Antes de tomar uma decisão por força do presente artigo, a Autoridade Europeia para a Proteção de Dados deve conceder à instituição ou organismo da União objeto dos procedimentos conduzidos por essa autoridade, a oportunidade de se pronunciar sobre as objeções apresentadas. A Autoridade Europeia para a Proteção de Dados deve basear as suas decisões unicamente nas objeções relativamente às quais as partes em causa puderam apresentar as suas observações. Os queixosos devem ser estreitamente associados ao procedimento.
  6. Os direitos de defesa das partes interessadas devem ser plenamente respeitados durante o procedimento. As partes interessadas devem ter o direito de aceder ao processo da Autoridade Europeia para a Proteção de Dados, sob reserva do interesse legítimo dos indivíduos ou das empresas relativamente à proteção dos seus dados pessoais ou dos seus segredos comerciais.
  7. Os fundos recolhidos em resultado da imposição das coimas por força do presente artigo devem integrar as receitas do orçamento geral da União Europeia.

#### *Artigo 67.º*

##### *Representação dos titulares dos dados*

O titular dos dados tem o direito de mandar um organismo, organização ou associação sem fins lucrativos, que foi devidamente constituído em conformidade com o direito da União ou de um Estado-Membro, cujos objetivos estatutários são de interesse público e cuja atividade incide sobre a proteção dos direitos e liberdades dos titulares de dados no que diz respeito à proteção dos seus dados pessoais para apresentar, em seu nome, uma reclamação à Autoridade Europeia para a Proteção de Dados, para exercer, em seu nome, os direitos referidos no artigo 63.º, e para exercer, em seu nome, o direito de receber uma indemnização referido no artigo 65.º.

#### *Artigo 68.º*

##### *Reclamações apresentadas pelos funcionários da União*

Qualquer pessoa ao serviço de uma instituição ou organismo da União pode apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados relativa a uma alegada violação das disposições do presente artigo, sem passar pela via oficial. Ninguém pode ser prejudicado por ter apresentado à Autoridade Europeia para a Proteção de Dados uma reclamação alegando tal violação.

#### *Artigo 69.º*

##### *Sanções*

O incumprimento das obrigações estabelecidas no presente regulamento, intencional ou negligente, por parte de um funcionário ou outro agente da União Europeia, é passível de sanção disciplinar ou outra sanção, em conformidade com o Estatuto dos Funcionários da União Europeia ou o Regime aplicável aos Outros Agentes da União Europeia.

# CAPÍTULO IX

## ATOS DE EXECUÇÃO

### *Artigo 70.º*

#### *Procedimento de comité*

1. A Comissão é assistida pelo comité criado pelo artigo 93.º do Regulamento (UE) 2016/679. Esse comité é um comité na aceção do Regulamento (UE) n.º 182/2011.
2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

# CAPÍTULO X

## DISPOSIÇÕES FINAIS

### *Artigo 71.º*

#### *Revogação do Regulamento (CE) n.º 45/2001 e da Decisão n.º 1247/2002/CE.*

O Regulamento (CE) n.º 45/2001<sup>22</sup> e a Decisão n.º 1247/2002/CE<sup>23</sup> são revogados com efeitos a partir de 25 de maio de 2018. As remissões para o regulamento e para a decisão revogados devem entender-se como sendo feitas para o presente regulamento.

### *Artigo 72.º*

#### *Medidas transitórias*

1. O presente regulamento não obsta à aplicação da Decisão 2014/886/UE do Parlamento Europeu e do Conselho<sup>24</sup> e aos mandatos atuais da Autoridade Europeia para a Proteção de Dados e da Autoridade Adjunta.
2. A Autoridade Adjunta é considerada equiparada ao Secretário do Tribunal de Justiça da União Europeia no que se refere à determinação da sua remuneração, subsídios, pensão de reforma e quaisquer outros benefícios equivalentes à remuneração.
3. O artigo 54.º, n.ºs 4, 5 e 7, e os artigos 56.º e 57.º do presente regulamento, são aplicáveis à atual Autoridade Adjunta até ao termo do seu mandato em 5 de dezembro de 2019.
4. A Autoridade Adjunta assiste a Autoridade Europeia para a Proteção de Dados em todas as suas funções e substitui-a em caso de ausência ou impedimento até ao termo do mandato da Autoridade Adjunta em 5 de dezembro de 2019.

---

<sup>22</sup> Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos organismos comunitários e à livre circulação desses dados, JO L 8 de 12.1.2001.

<sup>23</sup> Decisão n.º 1247/2002/CE, de 1 de julho de 2002, relativa ao estatuto e às condições gerais de exercício de funções da Autoridade Europeia para a Proteção de Dados, JO L 183 de 12.7.2002, p. 1.

<sup>24</sup> Decisão 2014/886/UE do Parlamento Europeu e do Conselho, de 4 de dezembro de 2014, relativa à nomeação da Autoridade Europeia para a Proteção de Dados e da Autoridade Adjunta, JO L 351 de 9.12.2014, p. 9.

*Artigo 73.º*

*Entrada em vigor e aplicação*

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.
2. O presente regulamento é aplicável a partir de 25 de maio de 2018.

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

Feito em Bruxelas, em

*Pelo Parlamento Europeu*  
*O Presidente*

*Pelo Conselho*  
*O Presidente*

## **FICHA FINANCEIRA LEGISLATIVA**

### **1. CONTEXTO DA PROPOSTA/INICIATIVA**

- 1.1. Denominação da proposta/iniciativa
- 1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB
- 1.3. Natureza da proposta/iniciativa
- 1.4. Objetivo(s)
- 1.5. Justificação da proposta/iniciativa
- 1.6. Duração da ação e impacto financeiro
- 1.7. Modalidade(s) de gestão planeada(s)

### **2. MEDIDAS DE GESTÃO**

- 2.1. Disposições em matéria de acompanhamento e prestação de informações
- 2.2. Sistema de gestão e de controlo
- 2.3. Medidas de prevenção de fraudes e irregularidades

### **3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA**

- 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)
- 3.2. Impacto estimado nas despesas
  - 3.2.1. *Síntese do impacto estimado nas despesas*
  - 3.2.2. *Impacto estimado nas dotações operacionais*
  - 3.2.3. *Impacto estimado nas dotações de natureza administrativa*
  - 3.2.4. *Compatibilidade com o atual quadro financeiro plurianual*
  - 3.2.5. *Participação de terceiros no financiamento*
- 3.3. Impacto estimado nas receitas

# FICHA FINANCEIRA LEGISLATIVA

## 1. CONTEXTO DA PROPOSTA/INICIATIVA

### 1.1. Denominação da proposta/iniciativa

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais por parte das instituições, órgãos, organismos e agências da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE.

### 1.2. Domínio(s) de intervenção abrangido(s) segundo a estrutura ABM/ABB<sup>25</sup>

Justiça – Proteção de dados pessoais

### 1.3. Natureza da proposta/iniciativa

- A proposta/iniciativa refere-se a **uma nova ação**
- A proposta/iniciativa refere-se a **uma nova ação na sequência de um projeto-piloto/ação preparatória**<sup>26</sup>
  - A proposta/iniciativa refere-se à **prorrogação de uma ação existente**
- A proposta/iniciativa refere-se a **uma ação reorientada para uma nova ação**

### 1.4. Objetivo(s)

#### 1.4.1. *Objetivo(s) estratégico(s) plurianual(is) da Comissão visado(s) pela proposta/iniciativa*

A entrada em vigor do Tratado de Lisboa e, particularmente, a introdução de uma nova base jurídica (artigo 16.º do TFUE), constitui a oportunidade de criar um quadro global de proteção de dados abrangendo todos os domínios.

Em 27 de abril de 2016, a União adotou o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (Texto relevante para efeitos do EEE), JO L 119 de 4.5.2016, p. 1–88.

No mesmo dia, a União adotou a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI, JO L 119 de 4.5.2016, p. 89–131.

A presente proposta visa concluir o estabelecimento de um quadro abrangente para a proteção de dados na União, harmonizando as normas de proteção de dados aplicáveis às instituições e organismos da União com as normas de proteção de dados

<sup>25</sup> ABM: Activity Based Management (gestão por atividades); ABB: Activity Based Budgeting (orçamentação por atividades).

<sup>26</sup> Conforme referido no artigo 54.º, n.º 2, alíneas a) e b), do Regulamento Financeiro.

do Regulamento (UE) 2016/679. Por razões de consistência e de coerência, as instituições e organismos da União devem aplicar um conjunto de normas de proteção de dados semelhante ao do setor público nos Estados-Membros.

1.4.2. *Objetivo(s) específico(s) e atividade(s) ABM/ABB em causa*

Objetivo específico n.º 1:

Garantir a aplicação coerente das normas de proteção de dados em toda a União.

Objetivo específico n.º 2:

Racionalizar o atual modelo de governação da proteção de dados nas instituições e organismos da União.

Objetivo específico n.º 3:

Garantir um maior respeito e aplicação das normas de proteção de dados nas instituições e organismos da União.

### 1.4.3. Resultados e impacto esperados

*Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada*

Na sua qualidade de responsáveis pelo tratamento de dados, as instituições e organismos da União devem beneficiar da mudança dos atuais procedimentos administrativos (abordagem *ex ante*) associados à proteção de dados para um respeito efetivo e uma aplicação reforçada das normas materiais de proteção de dados e dos novos princípios e conceitos de proteção de dados introduzidos pelo Regulamento (UE) 2016/679 (abordagem *ex post*) que serão aplicáveis em toda a União.

As pessoas singulares cujos dados são objeto de tratamento por instituições e organismos da União beneficiarão de um melhor controlo sobre os seus dados pessoais, aumentando a sua confiança no ambiente digital. Beneficiarão igualmente de uma responsabilidade reforçada por parte das instituições e organismos da União.

A Autoridade Europeia para a Proteção de Dados poderá centrar-se mais na sua função de controlo. A repartição da missão de aconselhamento à Comissão entre o Comité Europeu para a Proteção de Dado, instituído pelo Regulamento (UE) 2016/679, e a Autoridade Europeia para a Proteção de Dados, será clarificada evitando-se a sobreposição de tarefas.

### 1.4.4. Indicadores de resultados e de impacto

*Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa*

Os indicadores incluem os seguintes elementos:

Número de pareceres emitidos pelo Comité Europeu para a Proteção de Dados e pela Autoridade Europeia para a Proteção de Dados;

Discriminação das atividades dos encarregados da proteção de dados;

Utilização feita das avaliações de impacto sobre a proteção de dados;

Número de reclamações apresentadas pelos titulares dos dados;

Coimas aplicadas aos responsáveis pelo tratamento de dados por violações da proteção dos dados que lhes sejam imputadas.

## 1.5. Justificação da proposta/iniciativa

### 1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo

No Regulamento (UE) 2016/679 (artigo 2.º, n.º 3, artigo 98.º, considerando 17), os legisladores solicitaram a adaptação do Regulamento (CE) n.º 45/2001 aos princípios e normas estabelecidos no Regulamento (UE) 2016/679, a fim de criar um quadro de proteção de dados sólido e coerente na União e permitir a aplicação de ambos os instrumentos em simultâneo, ou seja, em 25 de maio de 2018.

### 1.5.2. Valor acrescentado da participação da UE

As normas de proteção de dados aplicáveis às instituições e organismos da União apenas podem ser introduzidas através de um ato da UE.

1.5.3. *Lições tiradas de experiências anteriores semelhantes*

A presente proposta baseia-se na experiência com o Regulamento (CE) n.º 45/2001 e na avaliação da respetiva aplicação, realizada por um estudo de avaliação (a cargo de um contratante externo entre setembro de 2014 e junho de 2015)<sup>27</sup>.

1.5.4. *Compatibilidade e eventual sinergia com outros instrumentos adequados*

A presente proposta baseia-se no Regulamento (UE) 2016/679 e finaliza o estabelecimento de um quadro de proteção de dados sólido, coerente e moderno a nível da União, neutro do ponto de vista tecnológico e resistente à prova do tempo.

---

<sup>27</sup> JUST/2013/FRAC/FW/0157/A4 no contexto do contrato-quadro múltiplo JUST/2011/EVAL/01 (RS 2013/05) - Estudo de avaliação sobre o Regulamento (CE) n.º 45/2001, de Ernst & Young.

## 1.6. Duração da ação e impacto financeiro

Proposta/iniciativa de **duração limitada**

- Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA
- Impacto financeiro no período compreendido entre AAAA e AAAA

- Proposta/iniciativa **de duração ilimitada**

- Aplicação com um período de arranque progressivo entre [2017] e 25 de maio de 2018, seguido de um período de aplicação a um ritmo de cruzeiro.

## 1.7. Modalidade(s) de gestão planeada(s)<sup>28</sup>

- Gestão direta pela Comissão

- pelos seus departamentos, incluindo pelos seus efetivos nas delegações da União;
- pelas agências executivas

**Gestão partilhada** com os Estados-Membros

**Gestão indireta**, confiando tarefas de execução orçamental:

- a países terceiros ou aos organismos por eles designados;
- às organizações internacionais e respetivas agências (a especificar);
- ao BEI e ao Fundo Europeu de Investimento;
- a organismos referidos nos artigos 208.º e 209.º do Regulamento Financeiro;
- aos organismos de direito público;
- aos organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;
- aos organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;
- a pessoas responsáveis pela execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

– *Se assinalar mais de uma modalidade de gestão, queira especificar na secção «Observações».*

### Observações

A presente proposta é limitada às instituições e organismos da União e diz respeito a todos eles.

<sup>28</sup>

As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

## **2. MEDIDAS DE GESTÃO**

### **2.1. Disposições em matéria de acompanhamento e prestação de informações**

*Especificar a periodicidade e as condições*

A presente proposta está limitada à aplicação de normas de proteção de dados pelas instituições e organismos da União. Dado que o controlo e a aplicação dessas normas é uma atribuição da Autoridade Europeia para a Proteção de Dados, cabe-lhe assegurar o acompanhamento e a prestação de informações na matéria. Em especial, por força do artigo 60.º da presente proposta, a Autoridade Europeia para a Proteção de Dados tem a obrigação de apresentar ao Parlamento Europeu, ao Conselho e à Comissão um relatório anual sobre as atividades da sua esfera de competência, que deve simultaneamente tornar público.

### **2.2. Sistema de gestão e de controlo**

#### **2.2.1. Risco(s) identificado(s)**

Foi realizado um estudo de avaliação da aplicação do Regulamento (CE) n.º 45/2001 por um contratante externo entre setembro de 2014 e junho de 2015. O estudo também analisa o impacto da introdução dos principais conceitos e princípios do Regulamento (UE) n.º 2016/679 nas instituições e organismos da União.

O novo modelo de proteção de dados centrar-se-á no respeito efetivo das normas da proteção de dados, bem como no controlo e aplicação efetivos dessas normas. Tal exigirá uma mudança da cultura da proteção de dados nas instituições e organismos da União, passando da abordagem administrativa *ex ante* para uma abordagem efetiva *ex post*.

#### **2.2.2. Informações sobre o sistema de controlo interno criado**

Métodos de controlo existentes aplicados pelas instituições e organismos da União.

#### **2.2.3. Estimativa dos custos e benefícios dos controlos e avaliação do nível previsto de risco de erro**

Métodos de controlo existentes aplicados pelas instituições e organismos da União.

### **2.3. Medidas de prevenção de fraudes e irregularidades**

*Especificar as medidas de prevenção e de proteção existentes ou previstas*

Métodos existentes de prevenção de fraudes aplicados pelas instituições e organismos da União.

### 3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

#### 3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(is) de despesas envolvida(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual:	Rubrica orçamental	Tipo de despesa	Contribuição			
	Número [...][Rubrica.....] .....]	DD/DND <sup>29</sup>	dos países EFTA <sup>30</sup>	dos países candidatos <sup>31</sup>	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
[...][XX.YY.YY.YY]	DD/DND	SIM/NÃO	SIM/NÃO	SIM/NÃO	SIM/NÃO	

- Novas rubricas orçamentais, cuja criação é solicitada

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual:	Rubrica orçamental	Tipo de despesa	Contribuição			
	Número [...][Rubrica.....] .....]	DD/DND	dos países EFTA	dos países candidatos	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
[...][XX.YY.YY.YY]		SIM/NÃO	SIM/NÃO	SIM/NÃO	SIM/NÃO	

<sup>29</sup> DD = dotações diferenciadas/DND = dotações não diferenciadas.

<sup>30</sup> EFTA: Associação Europeia de Comércio Livre.

<sup>31</sup> Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

### 3.2. Impacto estimado nas despesas

O impacto da presente proposta nas despesas está limitado às despesas das instituições e organismos da União. Contudo, a avaliação dos custos associada à presente proposta demonstra que esta não cria despesas adicionais significativas para as instituições e organismos da União.

No que diz respeito aos responsáveis pelo tratamento dos dados em instituições e organismos da União, o estudo de avaliação relativo à aplicação do Regulamento (CE) n.º 45/2001 demonstra que as suas atividades de proteção de dados correspondem a cerca de 70 equivalentes a tempo completo (ETC), ou seja, cerca de 9,3 milhões de EUR por ano. Cerca de 20 % das suas atividades de proteção de dados atuais correspondem a notificações de tratamento de dados. Esta atividade é suprimida no presente regulamento, o que corresponde a uma poupança anual de 1,922 milhões de EUR para responsáveis pelo tratamento de dados em instituições e organismos da União. Prevê-se que esta poupança seja compensada pelo envolvimento acrescido dos responsáveis pelo tratamento de dados na aplicação dos novos princípios e conceitos introduzidos pelo presente regulamento.

Mais especificamente, o inquérito realizado no âmbito do estudo de avaliação salientava que:

- a) A introdução do princípio da minimização de dados resultaria num impacto mínimo ou inexistente nas instituições e organismos da União;
- b) A introdução do princípio da transparência não teria um impacto significativo nas instituições e organismos da União;
- c) As crescentes obrigações de informação aumentariam a carga de trabalho dos responsáveis pelo tratamento de dados e dos encarregados da proteção de dados;
- d) O direito a ser esquecido não teria um impacto significativo nas instituições e organismos da União;
- e) O direito de portabilidade dos dados resultaria num impacto mínimo ou inexistente nas instituições e organismos da União;
- f) A introdução das avaliações de impacto relativas à proteção de dados teria uma importância moderadamente significativa na carga de trabalho dos responsáveis pelo tratamento de dados e nos encarregados da proteção de dados, uma vez que determinadas instituições e organismos da União já as realizam tais e os casos em que essas avaliações serão necessárias são limitados;
- g) A introdução de notificações de violações de dados pessoais aumentaria a carga de trabalho dos responsáveis pelo tratamento de dados, mas tais violações são raras;
- h) A proteção de dados desde a conceção e a proteção de dados por defeito já se encontram em vigor em várias instituições e organismos da União.

Além do mais, a avaliação de impacto realizada antes da adoção da proposta de reforma da proteção de dados concluiu que a introdução do princípio da proteção de dados desde a conceção não implicaria encargos administrativos para as autoridades públicas ou responsáveis pelo tratamento de dados<sup>32</sup>.

No que se refere aos encarregados da proteção de dados, o estudo de avaliação estimou o custo da rede atual de encarregados da proteção de dados (EPD) e dos coordenadores da proteção de dados (CPD) nas instituições e organismos da União em 82,9 ETC ou 10,9 milhões de EUR por ano. Consagram 26 % do tempo relacionado com a proteção de dados a atividades suprimidas pelo presente regulamento, ou seja, redação de notificações (em vez dos responsáveis pelo tratamento de dados), avaliação das notificações recebidas, manutenção dos respetivos registos e realização de controlos prévios. Essas supressões de atividades resultam numa poupança adicional de 2,834 milhões de EUR por ano para as instituições e organismos da União. Além disso, o presente regulamento favorece potenciais poupanças adicionais ao permitir que as instituições e organismos da União subcontratem atividades dos EPD, em vez de recorrerem aos seus próprios funcionários.

As poupanças no que diz respeito a atividades dos EPD serão contrabalançadas pelo seu envolvimento nas crescentes obrigações de informação, nas avaliações de impacto da proteção de dados (em circunstâncias limitadas quando forem necessárias) e na consulta prévia da Autoridade Europeia para a Proteção de Dados (cujo âmbito será muito mais limitado do que a atual obrigação de controlo prévio).

No que diz respeito à Autoridade Europeia para a Proteção de Dados, o seu orçamento anual é relativamente estável desde 2011 e ronda os 8 milhões de EUR. Atualmente, a sua unidade «Controlo e aplicação» e a sua unidade «Política e consulta» têm números de funcionários semelhantes, estáveis desde 2008. A maior ênfase do presente regulamento na função de controlo da Autoridade Europeia para a Proteção de Dados será compensada pelo papel consultivo mais direcionado e a eliminação da duplicação de funções com o Comité Europeu para a Proteção de Dados. Com efeito, a Autoridade Europeia para a Proteção de Dados pode, portanto, proceder a uma reafetação interna do seu pessoal.

A presente proposta prevê a possibilidade de a Autoridade Europeia para a Proteção de Dados impor coimas a instituições e organismos da União. Cada instituição ou organismo da União pode ser multado até um montante máximo de 250 000 EUR por ano (25 000 EUR por infração) ou até um máximo de 500 000 EUR por ano (50 000 EUR por infração) para as infrações mais graves ao presente regulamento. Essas coimas devem ser aplicadas apenas nos casos mais graves, e após a inobservância pela instituição ou organismo da União de outras medidas corretivas adotadas pela Autoridade Europeia para a Proteção de Dados. Desta forma, é esperado que o impacto financeiro dessas coimas seja limitado.

---

<sup>32</sup>

Documento de trabalho dos serviços da Comissão, Avaliação de impacto, SEC (2012) 72 final, p. 110.

3.2.1. Síntese do impacto estimado nas despesas

Em milhões de EUR (três casas decimais)

<b>Rubrica do quadro financeiro plurianual</b>	Número	[...][Rubrica..... .....]
--	--------	------------------------------

DG: <.....>			Ano N <sup>33</sup>	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)			<b>TOTAL</b>
• Dotações operacionais										
Número da rubrica orçamental	Autorizações	(1)								
	Pagamentos	(2)								
Número da rubrica orçamental	Autorizações	(1A)								
	Pagamentos	(2A)								
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos <sup>34</sup>										
Número da rubrica orçamental		(3)								
<b>TOTAL das dotações para a DG &lt;.....&gt;</b>	Autorizações	=1+1a +3								
	Pagamentos	=2+2A +3								

<sup>33</sup> O ano N é o do início da aplicação da proposta/iniciativa.

<sup>34</sup> Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

• TOTAL das dotações operacionais	Autorizações	(4)								
	Pagamentos	(5)								
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)								
<b>TOTAL das dotações ao abrigo da RUBRICA &lt;....&gt; do quadro financeiro plurianual</b>	Autorizações	=4+ 6								
	Pagamentos	=5+ 6								

**Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica:**

• TOTAL das dotações operacionais	Autorizações	(4)								
	Pagamentos	(5)								
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)								
<b>TOTAL das dotações no âmbito das RUBRICAS 1 a 4 do quadro financeiro plurianual (quantia de referência)</b>	Autorizações	=4+ 6								
	Pagamentos	=5+ 6								

<b>Rubrica do quadro financeiro plurianual</b>	<b>5</b>	«Despesas administrativas»
--	----------	----------------------------

Em milhões de EUR (três casas decimais)

	Ano N	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)	TOTAL
DG: <.....>						
• Recursos humanos						
• Outras despesas administrativas						

<b>TOTAL DG &lt;.....&gt;</b>	Dotações								
-------------------------------	----------	--	--	--	--	--	--	--	--

<b>TOTAL das dotações no âmbito da RUBRICA 5 do quadro financeiro plurianual</b>	(Total das autorizações = total dos pagamentos)								
--	---	--	--	--	--	--	--	--	--

Em milhões de EUR (três casas decimais)

		Ano N <sup>35</sup>	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)			TOTAL
<b>TOTAL das dotações no âmbito das RUBRICAS 1 a 5 do quadro financeiro plurianual</b>	Autorizações								
	Pagamentos								

<sup>35</sup> O ano N é o do início da aplicação da proposta/iniciativa.

3.2.2. *Impacto estimado nas dotações operacionais*

- A proposta/iniciativa não acarreta a utilização de dotações operacionais

A proposta/iniciativa acarreta a utilização de dotações operacionais tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e as realizações  ↓			Ano N	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)									TOTAL				
	REALIZAÇÕES																			
	Tipo <sup>36</sup>	Custo médio	º Z	Custo	º Z	Custo	º Z	Custo	º Z	Custo	º Z	Custo	º Z	Custo	º Z	Custo	º Z	Custo	Total n.º	Custo total
OBJETIVO ESPECÍFICO N.º 1 <sup>37</sup> ...																				
- Realização																				
- Realização																				
- Realização																				
Subtotal objetivo específico n.º 1																				
OBJETIVO ESPECÍFICO N.º 2...																				
- Realização																				
Subtotal objetivo específico n.º 2																				
<b>CUSTO TOTAL</b>																				

<sup>36</sup> As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

<sup>37</sup> Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)...».

### 3.2.3. Impacto estimado nas dotações de natureza administrativa

#### 3.2.3.1 Síntese

- A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

	Ano N <sup>38</sup>	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)	TOTAL
--	---------------------	---------	---------	---------	---	-------

<b>RUBRICA 5 do quadro financeiro plurianual</b>								
Recursos humanos								
Outras despesas administrativas								
<b>Subtotal RUBRICA 5 do quadro financeiro plurianual</b>								

<b>Com exclusão da RUBRICA 5<sup>39</sup> do quadro financeiro plurianual</b>								
Recursos humanos								
Outras despesas de natureza administrativa								
<b>Subtotal com exclusão da RUBRICA 5 do quadro financeiro plurianual</b>								

<b>TOTAL</b>								
--------------	--	--	--	--	--	--	--	--

As dotações necessárias para recursos humanos e outras despesas de natureza administrativa serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas internamente a nível da DG, complementadas, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

<sup>38</sup> O ano N é o do início da aplicação da proposta/iniciativa.

<sup>39</sup> Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

### 3.2.3.2 Necessidades estimadas de recursos humanos

- A proposta/iniciativa não acarreta a utilização de recursos humanos.
- A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

*As estimativas devem ser expressas em termos de equivalente a tempo completo*

	Ano N	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)		
<b>• Lugares do quadro do pessoal (postos de funcionários e de agentes temporários)</b>							
XX 01 01 01 (na sede e nos gabinetes de representação da Comissão)							
XX 01 01 02 (nas delegações)							
XX 01 05 01 (investigação indireta)							
10 01 05 01 (investigação direta)							
<b>• Pessoal externo (em equivalente a tempo completo: ETC)<sup>40</sup></b>							
XX 01 02 01 (AC, PND e TT da dotação global)							
XX 01 02 02 (AC, AL, PND, TT e JPD nas delegações)							
<b>XX 01 04 yy<sup>41</sup></b>	- na sede						
	- nas delegações						
XX 01 05 02 (AC, PND e TT - Investigação indireta)							
10 01 05 02 (AC, PND e TT - Investigação direta)							
Outras rubricas orçamentais (especificar)							
<b>TOTAL</b>							

**XX** constitui o domínio de intervenção ou título em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	
Pessoal externo	

<sup>40</sup> AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

<sup>41</sup> Sublimite máximo para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

### 3.2.4. *Compatibilidade com o atual quadro financeiro plurianual*

- A proposta/iniciativa é compatível com o atual quadro financeiro plurianual.

A proposta/iniciativa requer uma reprogramação da rubrica relevante do quadro financeiro plurianual.

Explicitar a reprogramação necessária, especificando as rubricas orçamentais em causa e as quantias correspondentes.

A proposta/iniciativa requer a mobilização do instrumento de flexibilidade ou a revisão do quadro financeiro plurianual.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes.

### 3.2.5. *Participação de terceiros no financiamento*

- A proposta/iniciativa não prevê o cofinanciamento por terceiros

A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

Dotações em milhões de EUR (três casas decimais)

	Ano N	Ano N+1	Ano N+2	Ano N+3	Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)			Total
Especificar o organismo de cofinanciamento								
TOTAL das dotações cofinanciadas								

### 3.3. Impacto estimado nas receitas

- A proposta/iniciativa não tem impacto financeiro nas receitas.
- A proposta/iniciativa tem o impacto financeiro a seguir descrito:
  - nos recursos próprios
  - nas receitas diversas

Em milhões de EUR (três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o atual exercício	Impacto da proposta/iniciativa <sup>42</sup>					Inserir os anos necessários para mostrar a duração do impacto (ver ponto 1.6)	
		Ano N	Ano N+1	Ano N+2	Ano N+3			
Artigo .....								

Relativamente às diversas receitas «afetadas», especificar a(s) rubrica(s) orçamental(is) de despesas envolvida(s).

Especificar o método de cálculo do impacto nas receitas.

<sup>42</sup>

No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 25 % a título de despesas de cobrança.