REGULAMENTO (UE) 2018/1725 DO PARLAMENTO EUROPEU E DO CONSELHO

de 23 de outubro de 2018

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos 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

(Texto relevante para efeitos do EEE)

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 ([1]),

Deliberando de acordo com o processo legislativo ordinário ([2]),

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 caráter pessoal que lhes digam respeito. Este direito é igualmente garantido pelo artigo 8.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

(2) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho ([3]) 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 dos 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 pelos órgãos da União. Contudo, não se aplica ao tratamento de dados pessoais efetuado no exercício de uma atividade das instituições e dos 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 ([4]) e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ([5]) foram adotados em 27 de abril de 2016. Enquanto o regulamento estabelece regras gerais para proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e para assegurar a livre circulação de dados pessoais na União, a diretiva estabelece as regras específicas para proteger as pessoas singulares no que diz respeito ao tratamento de dados pessoais e para 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 prevê a adaptação do Regulamento (CE) n.º 45/2001, a fim de garantir um regime de proteção de dados sólido e coerente na União e de permitir a sua aplicação em paralelo com o Regulamento (UE) 2016/679.

(5) Uma abordagem coerente da proteção dos dados pessoais e a livre circulação dos mesmos na União implicam uma harmonização, tão ampla quanto possível, das regras de proteção de dados adotadas a nível das instituições, dos órgãos e dos organismos da União com as regras de proteção de dados adotadas para o sector público nos Estados-Membros. Sempre que as disposições do presente regulamento sigam os mesmos princípios que as disposições do

([1]) JO C 288 de 31.8.2017, p. 107.

([2]) Posição do Parlamento Europeu de 13 de setembro de 2018 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 11 de outubro de 2018.

([3]) 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).

([4]) 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) (JO L 119 de 4.5.2016, p. 1).

([5]) 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 do Conselho (JO L 119 de 4.5.2016, p. 89).

Regulamento (UE) 2016/679, de acordo com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça»), esses dois conjuntos de disposições deverão ser interpretados de forma homogénea, sobretudo porque o regime do presente regulamento deverá ser entendido como equivalente ao regime do Regulamento (UE) 2016/679.

(6) As pessoas cujos dados pessoais são tratados por instituições e órgãos da União em qualquer contexto, por exemplo, porque são funcionários dessas instituições e órgãos, deverão ser protegidas. O presente regulamento não deverá aplicar-se 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 evitar graves riscos de ser contornada, a proteção das pessoas singulares deverá ser neutra em termos tecnológicos, e não deverá depender das técnicas utilizadas.

(8) O presente regulamento deverá aplicar-se ao tratamento de dados pessoais por todas as instituições e por todos os órgãos e organismos da União. O presente regulamento deverá aplicar-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios distintos dos meios automatizados de dados pessoais contidos em ficheiros ou a eles destinados. Os ficheiros ou os conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser abrangidos pelo âmbito de aplicação do presente regulamento.

(9) Na Declaração n.º 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, devido à especificidade dos domínios em causa, poderão ser necessárias disposições especiais sobre a proteção de dados pessoais e sobre 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, um capítulo distinto do presente regulamento, consagrado às regras gerais, deverá aplicar-se ao tratamento de dados pessoais operacionais, tais como os dados pessoais tratados para efeitos de investigação criminal pelos órgãos e organismos da União no exercício de atividades nos domínios da cooperação judiciária e penal e da cooperação policial.

(10) A Diretiva (UE) 2016/680 estabelece regras 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 em toda a União, e de evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre os órgãos e os organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE e as autoridades competentes, as regras relativas à proteção e à livre circulação de dados pessoais operacionais tratados por esses órgãos e organismos da União deverão ser coerentes com a Diretiva (UE) 2016/680.

(11) As regras gerais do capítulo do presente regulamento relativo ao tratamento de dados pessoais operacionais deverão ser aplicáveis sem prejuízo das regras específicas aplicáveis ao tratamento de dados pessoais operacionais pelos órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE. Essas regras específicas deverão ser consideradas *lex specialis* relativamente às disposições constantes do capítulo do presente regulamento respeitantes ao tratamento de dados pessoais operacionais (*lex specialis derogat legi generali*). A fim de reduzir a fragmentação jurídica, as regras específicas de proteção de dados aplicáveis ao tratamento de dados pessoais operacionais pelos órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE deverão ser coerentes com os princípios subjacentes ao capítulo do presente regulamento relativo ao tratamento de dados pessoais operacionais, e também com as disposições do presente regulamento relativas ao controlo independente, às vias de recurso, à responsabilidade e às sanções.

(12) O capítulo do presente regulamento relativo ao tratamento de dados pessoais operacionais deverá aplicar-se aos órgãos e aos organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, quer exerçam essas atividades como atribuições principais ou como funções acessórias, para efeitos de prevenção, deteção, investigação ou repressão de infrações penais. No entanto, o presente regulamento não deverá aplicar-se à Europol nem à Procuradoria Europeia até que os atos normativos que criam a Europol e a Procuradoria Europeia sejam alterados a fim de permitir que o capítulo do presente regulamento relativo ao tratamento de dados pessoais operacionais, na sua versão adaptada, lhes seja aplicável.

(13) A Comissão deverá proceder a um reexame do presente regulamento, em especial do capítulo relativo ao tratamento de dados pessoais operacionais. A Comissão deverá também efetuar um reexame de outros atos normativos adotados com base nos Tratados que regulam o tratamento de dados pessoais operacionais pelos órgãos e

organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE. Após esse reexame, a fim de assegurar uma proteção uniforme e coerente das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão deverá poder apresentar as propostas legislativas adequadas, incluindo as adaptações necessárias do capítulo do presente regulamento relativo ao tratamento de dados pessoais operacionais, na perspetiva da sua aplicação à Europol e à Procuradoria Europeia. As adaptações deverão ter em conta as disposições relativas ao controlo independente, às vias de recurso, à responsabilidade e às sanções.

(14) O tratamento de dados pessoais administrativos, tais como os dados relativos ao pessoal, pelos órgãos e organismos da União que exercem atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, deverá ser abrangido pelo presente regulamento.

(15) O presente regulamento deverá aplicar-se ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União que exercem atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do Tratado da União Europeia (TUE). O presente regulamento não deverá aplicar-se ao tratamento de dados pessoais pelas missões referidas no artigo 42.º, n.º 1, e nos artigos 43.º e 44.º do TUE, que aplicam a política comum de segurança e de defesa. Se for caso disso, deverão ser apresentadas propostas adequadas para regulamentar também o tratamento de dados pessoais no domínio da política comum de segurança e de defesa.

(16) Os princípios da proteção de dados deverão aplicar-se a todas as informações relativas 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, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, deverão ser tidos em conta todos os meios que apresentem uma probabilidade razoável de ser 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 existe uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, deverão ser tidos em conta todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta as tecnologias disponíveis à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não deverão, 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 identificável ou já não possa ser identificado. Por conseguinte, o presente regulamento não diz respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.

(17) 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 cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir outras medidas de proteção de dados.

(18) 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), 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 com outras informações recebidas pelos servidores, podem ser utilizados para definir perfis das pessoas singulares e para as identificar.

(19) O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de autorizar 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 o titular dos dados aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado na sequência de um pedido apresentado por via eletrónica, o pedido tem de ser claro e conciso, e não pode perturbar desnecessariamente a utilização do serviço em causa. Além disso, o titular dos dados deverá ter o direito de retirar o seu consentimento a qualquer momento, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado. A fim de assegurar que o consentimento seja dado de livre vontade, este não deverá constituir um fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, em que seja, portanto, improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à

situação específica em causa. Muitas vezes não é possível identificar totalmente a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que sejam respeitados padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.

(20) O tratamento de dados pessoais deverá ser efetuado de forma lícita e leal. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes digam respeito são recolhidos, utilizados, consultados ou sujeitos a outros tipos de tratamento, e em que medida é que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações e as 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 e sobre as finalidades a que o tratamento dos dados se destina, e às informações adicionais destinadas a assegurar que o tratamento dos dados seja efetuado com lealdade e transparência em relação às pessoas singulares em causa e salvaguarde o seu direito a obter a confirmação e a comunicação dos dados pessoais tratados que lhes digam respeito. As pessoas singulares deverão ser alertadas para os riscos, para as regras, para as garantias e para os direitos associados ao tratamento dos seus 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 deverão ser explícitas e legítimas, e determinadas aquando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para as finalidades para as quais são tratados. Para tal, é necessário assegurar, em especial, que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais só deverão ser tratados se a finalidade do seu tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou para a revisão periódica. Deverão ser tomadas todas as medidas razoáveis para que os dados pessoais incorretos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a segurança e a confidencialidade adequadas, designadamente para evitar o acesso aos dados pessoais, a sua utilização e o acesso a equipamentos utilizados para o seu tratamento não autorizados, e para evitar a divulgação não autorizada dos dados pessoais aquando da sua transmissão.

(21) Em conformidade com o princípio da responsabilidade, quando as instituições e os órgãos da União transmitem dados pessoais no interior da mesma instituição ou do mesmo organismo, e o destinatário não faz parte do responsável pelo tratamento, ou a outras instituições ou a outros órgãos da União, deverão verificar se esses dados pessoais são necessários para o desempenho legítimo de funções da competência do destinatário. Em particular, após o pedido do destinatário para a transmissão dos dados pessoais, o responsável pelo tratamento deverá verificar a existência de um motivo relevante para o tratamento lícito dos dados pessoais e a competência do destinatário. O responsável pelo tratamento deverá efetuar também uma avaliação provisória da necessidade de transmitir esses dados. Em caso de dúvida quanto a essa necessidade, o responsável pelo tratamento deverá solicitar informações complementares ao destinatário. O destinatário deverá certificar-se de que a necessidade da transmissão dos dados pode ser verificada posteriormente.

(22) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base na necessidade de desempenho de uma função efetuada no interesse público pelas instituições e pelos órgãos da União, ou no exercício da sua autoridade pública, na necessidade de conformidade com uma obrigação jurídica a que o responsável pelo tratamento dos dados esteja sujeito, ou com outra base legítima, ao abrigo do presente regulamento, incluindo o consentimento do titular dos dados em causa, a necessidade de executar 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 pelos órgãos da União inclui o tratamento de dados pessoais necessários à gestão e ao funcionamento dessas instituições e órgãos. O tratamento de dados pessoais deverá também ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados, ou de outra pessoa singular. Em princípio, o tratamento de dados pessoais com base no interesse vital de outra pessoa singular só pode ocorrer quando não puder manifestamente ter como base outro fundamento jurídico. Alguns tipos de tratamento de dados podem servir simultaneamente interesses públicos importantes e os interesses vitais do titular dos dados, como, por exemplo, quando o tratamento dos dados é necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação, ou em situações de emergência humanitária, em especial situações de catástrofes naturais e de origem humana.

(23) O direito da União referido no presente regulamento deverá ser claro e rigoroso, e a sua aplicação deverá ser previsível para os seus destinatários, em conformidade com as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

(24) As regras internas referidas no presente regulamento deverão consistir em atos claros e precisos de aplicação geral, destinados a produzir efeitos jurídicos em relação aos titulares dos dados. Essas regras deverão ser adotadas ao mais alto nível de direção das instituições e dos órgãos da União, no âmbito das suas competências e em matérias relacionadas com o seu funcionamento. Essas regras deverão ser publicadas no *Jornal Oficial da União Europeia*. A aplicação dessas normas deverá ser previsível para os seus destinatários, em conformidade com os requisitos estabelecidos na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais. Essas regras internas podem assumir a forma de decisões, em particular quando forem adotadas por instituições da União.

(25) O tratamento de dados pessoais para finalidades distintas daquelas para as quais os dados tenham sido inicialmente recolhidos só deverá 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 daquele que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou para o exercício da autoridade pública de que o responsável pelo tratamento esteja investido, o direito da União pode determinar e definir as tarefas e as finalidades para as quais o tratamento posterior deverá ser considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos deverão ser consideradas como operações de tratamento lícito compatível. O fundamento jurídico previsto no direito da União para o tratamento de dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de um tratamento 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 de licitude do tratamento inicial, deverá 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, com base 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 nas operações de tratamento iniciais como nas operações de tratamento posteriores previstas.

(26) Caso o tratamento tenha por base o consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento a esse tratamento. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir 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 ([1]), deverá ser fornecida uma declaração de consentimento previamente redigida pelo responsável pelo tratamento, inteligível e facilmente acessível, numa linguagem clara e simples, e sem cláusulas abusivas. Para efeitos de um consentimento informado, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades do tratamento para as quais os dados pessoais se destinam. Não deverá considerar-se 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.

(27) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, das consequências e das garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção especial deverá aplicar-se, nomeadamente, à criação de perfis de personalidade; à recolha de dados pessoais relativos às crianças aquando da utilização de serviços disponibilizados diretamente a um menor nos sítios Web das instituições e dos órgãos da União, tais como os serviços de comunicação interpessoal ou de venda de bilhetes em linha; e ao tratamento de dados pessoais com base no consentimento.

(28) Quando os destinatários, que não sejam instituições ou órgãos da União, estejam estabelecidos na União e pretendam que as instituições e os órgãos da União lhes transmitam dados pessoais, deverão demonstrar que a transmissão é necessária para o exercício de funções de interesse público ou para o exercício da autoridade pública de que estejam investidos. Em alternativa, esses destinatários deverão demonstrar que a transmissão é necessária para uma finalidade específica no interesse público e o responsável pelo tratamento deve determinar se existem motivos para pressupor que os interesses legítimos do titular dos dados possam ser prejudicados. Neste caso, o responsável pelo tratamento deverá sopesar, comprovadamente, os diferentes interesses em jogo, a fim de avaliar se o pedido de

([1]) 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).

transmissão de dados pessoais é proporcionado. As finalidades específicas no interesse público podem dizer respeito à transparência das instituições e dos órgãos da União. Além disso, as instituições e os órgãos da União deverão demonstrar essa necessidade quando estão na origem da transmissão, em conformidade com o princípio da transparência e da boa administração. Os requisitos previstos no presente regulamento para a transmissão a destinatários estabelecidos na União, que não sejam instituições ou órgãos da União, deverão ser entendidos como complementares das condições para o tratamento lícito.

(29) Merecem proteção específica os dados pessoais que sejam, 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. Esses dados pessoais só deverão ser tratados se as condições específicas definidas no presente regulamento estiverem reunidas. Deverão 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 deverá ser considerado sistematicamente como um tratamento de categorias especiais de dados pessoais, uma vez que as fotografias só são abrangidas pela definição de dados biométricos quando são processadas por meios técnicos específicos que permitem a identificação inequívoca ou a autenticação de uma pessoa singular. Para além dos requisitos específicos para o tratamento de dados sensíveis, deverão aplicar-se os princípios gerais e outras disposições do presente regulamento, em especial, no que se refere às condições para o tratamento lícito. Deverão ser expressamente previstas derrogações da 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 de dados for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.

(30) As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser tratadas para finalidades relacionadas com a saúde nos casos em que tal se revele necessário para atingir essas finalidades no interesse das pessoas singulares e da sociedade no seu todo, nomeadamente no contexto da gestão dos serviços e sistemas de saúde ou de ação social. Por conseguinte, o presente regulamento deverá estabelecer condições harmonizadas para o tratamento de categorias especiais de dados pessoais relativos à saúde, tendo em conta necessidades específicas, designadamente quando o tratamento desses dados for efetuado para determinadas finalidades ligadas à saúde por pessoas sujeitas a uma obrigação legal de sigilo profissional. O direito da União deverá prever medidas específicas adequadas para defender os direitos fundamentais e para proteger os dados pessoais das pessoas singulares.

(31) 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 deverá 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» deverá ser interpretada segundo a definição constante do Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho ([1]), 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 deverá dar origem a que os dados pessoais sejam tratados para outras finalidades.

(32) Se os dados pessoais tratados pelo responsável pelo tratamento não lhe permitirem identificar uma pessoa singular, o responsável pelo tratamento não deverá ser obrigado a obter informações suplementares para identificar o titular dos dados com o único objetivo de cumprir uma disposição do presente regulamento. Todavia, o responsável pelo tratamento não deverá recusar-se a receber informações suplementares fornecidas pelo titular dos dados para apoiar o exercício dos seus direitos. A identificação deverá 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.

(33) O tratamento de dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos deverá ficar sujeito a garantias adequadas no que respeita aos direitos e às liberdades do titular dos dados, nos termos do presente regulamento. Essas garantias deverão assegurar a 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, para fins de investigação científica

([1]) 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).

ou histórica ou para fins estatísticos deverá 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 os órgãos da União deverão prever, no direito da União e, eventualmente, em regras internas adotadas pelas instituições e pelos órgãos da União em matérias relacionadas com o seu funcionamento, as garantias apropriadas para o tratamento de dados pessoais para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

(34) Deverão ser previstas regras 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, para obter gratuitamente, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento, e o exercício do direito de oposição. O responsável pelo tratamento deverá 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 deverá ser obrigado a responder aos pedidos do titular dos dados sem demora indevida e, o mais tardar, no prazo de um mês, e fundamentar a sua eventual intenção de recusar o pedido.

(35) 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 deverá 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 deverá 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 deverá 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 deverão ser de leitura automática.

(36) As informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser-lhe facultadas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, num prazo razoável, consoante as circunstâncias. Sempre que os dados pessoais possam ser legitimamente comunicados a outro destinatário, o titular dos dados deverá 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, deverá 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, deverão ser-lhe facultadas informações genéricas.

(37) Os titulares dos dados deverão 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 e de verificar a licitude do seu tratamento. 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 deverá, 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 deverá 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 deverão 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, deverá 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.

(38) Os titulares dos dados deverão ter direito a que os seus dados pessoais sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União aplicável ao responsável pelo tratamento. Os titulares dos dados deverão 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 deverá ter a possibilidade de exercer esse direito independentemente do facto de já ser adulto. No entanto, o prolongamento do prazo de conservação dos dados pessoais deverá ser lícito quando se revele necessário para o exercício do direito da liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que o responsável pelo tratamento está investido, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

(39) Para reforçar o «direito a ser esquecido» no ambiente em linha, o direito de apagamento deverá ser 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 as ligações para esses dados pessoais, e as cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá tomar medidas razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar os responsáveis que estejam a tratar esses dados do pedido do titular dos dados pessoais.

(40) Para limitar 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 limitações do tratamento deverão, em princípio, ser asseguradas por meios técnicos, de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma clara no sistema que o tratamento dos dados pessoais se encontra sujeito a limitações.

(41) Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá 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 pelo tratamento. Os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Esse direito deverá 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 deverá ser aplicável quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável pelo tratamento 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 deverá 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 deverá prejudicar os direitos e as liberdades de outros titulares de dados nos termos do presente regulamento. Além disso, esse direito não deverá prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais, nem as limitações desse direito estabelecidas no presente regulamento, nem deverá implicar, nomeadamente, 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 sejam necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deverá ter o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento.

(42) 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 deverá deixar de ter o direito de se opor ao tratamento dos dados pessoais que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento provar que os seus interesses legítimos e imperiosos prevalecem sobre os interesses ou os direitos e as liberdades fundamentais do titular dos dados.

(43) O titular dos dados deverá 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 formas de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e a previsão de aspetos relacionados com o desempenho profissional, a situação económica, a saúde, as

preferências ou os interesses pessoais, a fiabilidade ou o comportamento, a localização ou as deslocações do titular dos dados, quando produza efeitos jurídicos que digam respeito a essa pessoa singular ou a afetem significativamente de forma similar.

Contudo, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se for expressamente autorizada pelo direito da União. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão 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 deverá 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 o contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá 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 sejam corrigidos e que o risco de erros seja minimizado, proteger os dados pessoais de modo a ter em conta os riscos potenciais para os interesses e direitos do titular dos dados, prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opiniões políticas, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou o tratamento que se traduza em medidas que venham a ter tais efeitos. O processo automatizado de tomada de decisões e a definição de perfis baseada em categorias especiais de dados pessoais só deverão ser permitidos em condições específicas.

(44) Os atos normativos adotados com base nos Tratados ou as regras internas adotadas pelas instituições e pelos órgãos da União em matérias relacionadas com o seu funcionamento podem impor limitações 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 dos dados 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 tais limitações sejam necessárias e proporcionadas numa sociedade democrática, para salvaguardar a segurança pública e para a prevenção, a investigação e a repressão de infrações penais, ou para a execução de sanções penais. Tal inclui a salvaguarda e a prevenção de ameaças à segurança pública, a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, a segurança interna das instituições e dos órgãos da União, outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente os objetivos da política externa e de segurança comum da União ou um interesse económico ou financeiro importante da União ou de um Estado-Membro, e a conservação de registos públicos por motivos de interesse público geral ou de defesa do titular dos dados ou dos direitos e das liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários.

(45) A responsabilidade do responsável pelo tratamento deverá ser estabelecida em relação ao tratamento de dados pessoais realizado por si ou por sua conta. Em especial, o responsável pelo tratamento deverá 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 deverão 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 as liberdades das pessoas singulares.

(46) Os riscos para os direitos e as liberdades das pessoas singulares, de probabilidade e gravidade variar, podem resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial: quando o tratamento possa 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.

(47) A probabilidade e a gravidade dos riscos para os direitos e as liberdades do titular dos dados deverão ser determinadas por referência à natureza, ao âmbito, ao contexto e às finalidades do tratamento. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam um risco ou um risco elevado.

(48) A proteção dos direitos e das 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 deverá 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 poderão 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, deverão também ser tomados em consideração no contexto dos contratos públicos.

(49) O Regulamento (UE) 2016/679 prevê que os responsáveis pelo tratamento demonstrem a conformidade mediante o cumprimento de procedimentos de certificação aprovados. Do mesmo modo, as instituições e os órgãos da União deverão poder demonstrar a conformidade com o presente regulamento mediante a obtenção de uma certificação nos termos do artigo 42.º do Regulamento (UE) 2016/679.

(50) A proteção dos direitos e das 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 é efetuada por conta de um responsável pelo tratamento.

(51) 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, deverá 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 que não sejam instituições ou órgãos da União de um código de conduta aprovado ou de um mecanismo de certificação aprovado pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. A realização de operações de tratamento de dados por um subcontratante que não seja uma instituição ou órgão da União deverá ser regulada por um contrato, ou, no caso de instituições e órgãos da União que atuem como subcontratantes, por um contrato ou por outro ato normativo ao abrigo do direito da União 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 funções e as responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e às liberdades do titular dos dados. O responsável pelo tratamento e o subcontratante deverão poder optar por um contrato individual ou por cláusulas contratuais-tipo adotadas diretamente pela Comissão, ou pela Autoridade Europeia para a Proteção de Dados e posteriormente pela Comissão. Uma vez concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deverá devolver ou apagar os dados pessoais, consoante a escolha do responsável pelo tratamento, a não ser que a conservação desses dados pessoais seja exigida ao abrigo do direito da União ou do direito do Estado-Membro a que o subcontratante está sujeito.

(52) A fim de demonstrar a observância do presente regulamento, os responsáveis pelo tratamento deverão conservar um registo das atividades de tratamento sob a sua responsabilidade e os subcontratantes deverão conservar um registo das categorias de atividades de tratamento sob a sua responsabilidade. As instituições e os órgãos da União deverão 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. A não ser que tal não seja adequado devido à dimensão da instituição ou do órgão da União, as instituições e os órgãos da União deverão ter condições para estabelecer um registo central dos registos das suas atividades de tratamento. Por motivos de transparência, as instituições e os órgãos da União deverão poder igualmente tornar esse registo público.

(53) A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão garantir 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, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, a perda e a 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.

(54) As instituições e os órgãos da União deverão garantir a confidencialidade das comunicações eletrónicas prevista no artigo 7.º da Carta. Em especial, as instituições e os órgãos da União deverão garantir a segurança das suas redes de comunicações eletrónicas. As instituições e os órgãos da União deverão proteger as informações relativas ao equipamento terminal dos utilizadores que acedem aos seus sítios Web e às aplicações móveis acessíveis ao público nos termos da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([1]). As instituições e os órgãos da União deverão também proteger os dados pessoais conservados em listas de utilizadores.

(55) 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, deverá notificá-la à Autoridade Europeia para a Proteção de Dados, sem demora indevida e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a não ser 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 as liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, e as informações poderão ser fornecidas por fases, sem demora indevida. Se esse atraso for justificado, as informações menos sensíveis ou menos específicas sobre a violação deverão ser comunicadas o mais cedo possível, em vez de se resolver totalmente o incidente subjacente antes de efetuar a notificação.

(56) O responsável pelo tratamento deverá comunicar a violação de dados pessoais ao titular dos dados sem demora indevida, quando for provável que essa violação implique um elevado risco para os direitos e as liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias. A comunicação deverá descrever a natureza da violação dos dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deverá 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.

(57) 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. A não ser que tal não seja adequado devido à dimensão da instituição ou do órgão da União, o encarregado da proteção de dados deve conservar um registo das operações de tratamento notificadas. Além desta obrigação geral, deverão ser estabelecidos procedimentos e mecanismos eficazes para controlar as operações de tratamento suscetíveis de implicar um risco elevado para os direitos e as liberdades das pessoas singulares, devido à natureza, ao âmbito, ao contexto e às finalidades de tais operações. Esses procedimentos deverão ser também aplicados, nomeadamente, caso os tipos de operações de tratamento envolvam a utilização de novas tecnologias, ou pertençam a um novo tipo em relação ao qual nenhuma avaliação de impacto relativa à proteção de dados tenha sido previamente efetuada pelo responsável pelo tratamento, ou se tenham tornado necessários à luz do período decorrido desde o tratamento inicial. Nesses casos, o responsável pelo tratamento deverá proceder, antes do tratamento, a uma avaliação de impacto relativa à 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 deverá incluir, nomeadamente, as medidas, as garantias e os procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.

(58) Caso uma avaliação de impacto relativa à proteção de dados indique 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 as liberdades das pessoas singulares, e o responsável pelo tratamento considere que o risco não poderá ser atenuado através de medidas razoáveis, tendo em conta as tecnologias disponíveis e os custos de aplicação, a Autoridade Europeia para a Proteção de Dados deverá ser consultada antes de se iniciarem as atividades de tratamento. Esse elevado risco pode resultar de determinados tipos de tratamento, bem como da sua extensão e da sua frequência, os quais podem provocar também danos ou interferências nos direitos e nas liberdades da pessoa singular. A Autoridade Europeia para a Proteção de Dados deverá responder ao pedido de consulta num prazo determinado.

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

Contudo, a falta de reação da Autoridade Europeia para a Proteção de Dados nesse prazo não deverá prejudicar a sua intervenção de acordo com as atribuições e os poderes que lhe são conferidos pelo presente regulamento, incluindo o poder de proibir certas operações de tratamento de dados. No âmbito desse processo de consulta, o resultado de uma avaliação de impacto relativa à proteção de dados efetuada quanto ao tratamento em questão deverá poder ser apresentado à Autoridade Europeia para a Proteção de Dados, em especial as medidas previstas para atenuar o risco para os direitos e as liberdades das pessoas singulares.

(59) A Autoridade Europeia para a Proteção de Dados deverá ser informada das medidas administrativas e consultada sobre as regras internas adotadas pelas instituições e pelos órgãos da União em matérias relacionadas com o seu funcionamento quando preveem o tratamento de dados pessoais, quando estabelecem condições para as limitações dos direitos dos titulares dos dados ou quando 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, no que se refere à atenuação dos riscos para os titulares dos dados.

(60) O Regulamento (UE) 2016/679 criou o Comité Europeu para a Proteção de Dados como um organismo independente da União com personalidade jurídica. O Comité deverá contribuir para a aplicação coerente do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680 em toda a União, e igualmente o aconselhamento da Comissão. Simultaneamente, a Autoridade Europeia para a Proteção de Dados deverá continuar a exercer as suas funções de supervisão e as suas funções consultivas relativamente a todas as instituições e órgãos da União, por iniciativa própria ou mediante pedido. A fim de assegurar a coerência das regras de proteção de dados em toda a União, quando a Comissão elaborar propostas ou recomendações, deverá esforçar-se por consultar a Autoridade Europeia para a Proteção de Dados. Essa consulta deverá ser obrigatória após a adoção de atos legislativos ou durante a elaboração de atos delegados e de atos de execução, conforme definido nos artigos 289.º, 290.º e 291.º do TFUE, e após a adoção de recomendações e de propostas relativas a acordos com países terceiros e com organizações internacionais, tal como previsto no artigo 218.º do TFUE, com impacto no direito à proteção de dados pessoais. Nesses casos, a Comissão deverá ser obrigada a consultar a Autoridade Europeia para a Proteção de Dados, exceto nos casos em que o Regulamento (UE) 2016/679 preveja a consulta obrigatória do Comité Europeu para a Proteção de Dados, por exemplo, sobre decisões de adequação ou atos delegados relativos a ícones normalizados e requisitos aplicáveis aos procedimentos de certificação. Sempre que o ato em questão for particularmente importante para a proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão deverá ainda poder consultar o Comité Europeu para a Proteção de Dados. Nesses casos, a Autoridade Europeia para a Proteção de Dados, enquanto membro do Comité Europeu para a Proteção de Dados, deverá coordenar o seu trabalho com o Comité tendo em vista a emissão de um parecer comum. A Autoridade Europeia para a Proteção de Dados e, se aplicável, o Comité Europeu para a Proteção de Dados, deverão emitir o seu parecer por escrito no prazo de oito semanas. Tal prazo deverá ser mais curto em casos urgentes, ou sempre que necessário, por exemplo, quando a Comissão estiver a elaborar atos delegados ou de execução.

(61) Nos termos do artigo 75.º do Regulamento (UE) 2016/679, a Autoridade Europeia para a Proteção de Dados deverá assegurar o secretariado do Comité Europeu para a Proteção de Dados.

(62) Em todas as instituições e órgãos da União, um encarregado da proteção de dados deverá assegurar que as disposições do presente regulamento sejam aplicadas, e aconselhar os responsáveis pelo tratamento e os subcontratantes no cumprimento das suas obrigações. Esse encarregado deverá ser uma pessoa com conhecimentos especializados sobre a legislação e as práticas em matéria de proteção de dados, que deverão ser determinados, em particular, em função das operações de tratamento de dados realizadas pelo responsável pelo tratamento ou pelo subcontratante e da proteção exigida para os dados pessoais em causa. Esses encarregados da proteção de dados deverão poder desempenhar as suas funções e cumprir os seus deveres de forma independente.

(63) Quando os dados pessoais são transferidos das instituições e órgãos da União para responsáveis pelo tratamento, subcontratantes ou outros destinatários em países terceiros, ou para organizações internacionais, deverá ser garantido o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento. Deverão aplicar-se as mesmas garantias nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional para responsáveis pelo tratamento ou subcontratantes desse ou de outro país terceiro, ou dessa ou de outra organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento e pelos direitos e liberdades fundamentais consagrados na Carta. Só 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 para organizações internacionais forem cumpridas pelo responsável pelo tratamento ou pelo subcontratante.

(64) A Comissão pode decidir, nos termos do artigo 45.º do Regulamento (UE) 2016/679 ou do artigo 36.º da Diretiva (UE) 2016/680, que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, assegurem um nível adequado de proteção de dados. Nesses casos, as instituições ou os órgãos da União podem realizar transferências de dados pessoais para esse país ou para essa organização internacional sem que para tal seja necessária qualquer outra autorização.

(65) Na falta de uma decisão de adequação, o responsável pelo tratamento ou o subcontratante deverá tomar 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 seja uma instituição ou um órgão 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 deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento dos dados no território da União, incluindo a atribuição de direitos oponíveis ao titular de dados e a existência de vias de recurso eficazes, nomeadamente o direito de recurso administrativo ou judicial e o direito à indemnização, na União ou num país terceiro. As garantias deverão 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 órgãos 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. Deverá ser obtida a autorização da Autoridade Europeia para a Proteção de Dados quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.

(66) A possibilidade de o responsável pelo tratamento ou o subcontratante recorrerem a cláusulas-tipo de proteção de dados adotadas pela Comissão ou pela Autoridade Europeia para a Proteção de Dados não deverá impedi-los de incluir tais cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentar 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 e das liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção de dados.

(67) Alguns países terceiros aprovam leis, regulamentos e outros atos jurídicos destinados a regular diretamente as atividades de tratamento pelas instituições e pelos órgãos 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 o subcontratante transfiram ou divulguem 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 jurídicos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado na União pelo presente regulamento. As transferências só deverão 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.

(68) Deverá 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 procedimento administrativo ou de um procedimento não judicial, incluindo procedimentos junto de organismos de regulação. Deverá também prever-se a possibilidade de efetuar transferências por 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 do público ou de pessoas com um interesse legítimo. Neste último caso, a transferência não deverá abranger a totalidade dos dados pessoais nem categorias completas de dados pessoais contidos nesse registo, a não ser que tal seja autorizado pelo direito da União, e, quando o registo se destinar a ser consultado por pessoas com um interesse legítimo, a transferência só deverá ser efetuada a pedido dessas pessoas ou, caso estas sejam os destinatários, tendo plenamente em conta os interesses e os direitos fundamentais do titular dos dados.

(69) Essas derrogações deverão ser aplicáveis, em especial, às transferências de dados exigidas e necessárias por razões importantes de interesse público, nomeadamente em caso de intercâmbio internacional de dados entre instituições e órgãos 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 por doenças contagiosas ou para reduzir e/ou eliminar a dopagem no desporto. Deverão

igualmente ser consideradas lícitas as transferências de dados pessoais que sejam necessárias 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 estabelecer expressamente, por razões importantes de interesse público, 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 serem do interesse vital do titular dos dados.

(70) Em qualquer caso, se a Comissão não tiver tomado uma decisão relativamente ao nível adequado de proteção de dados num determinado país terceiro, o responsável pelo tratamento ou o subcontratante deverá adotar soluções que confiram aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, que lhes garantam que continuarão a beneficiar dos direitos e das garantias fundamentais.

(71) No caso de transferências transnacionais de dados pessoais para fora do território da União, o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ou da divulgação ilícitas dessas informações, aumenta. Paralelamente, as autoridades nacionais de controlo, incluindo a Autoridade Europeia para a Proteção de Dados, podem não conseguir dar seguimento a reclamações ou realizar investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiriço podem ser também restringidos por poderes preventivos ou de reparação insuficientes, por regimes jurídicos incoerentes e por obstáculos práticos, tais como a limitação de recursos. Por conseguinte, deverá ser promovida uma cooperação mais estreita entre a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo, a fim de facilitar o intercâmbio de informações com as suas homólogas internacionais.

(72) A criação pelo Regulamento (CE) n.º 45/2001 da Autoridade Europeia para a Proteção de Dados, que está 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 deverá reforçar e clarificar o seu papel e a sua independência. A Autoridade Europeia para a Proteção de Dados deverá ser uma pessoa que ofereça todas as garantias de independência e que disponha reconhecidamente da experiência e da competência necessárias para o desempenho das funções de Autoridade Europeia para a Proteção de Dados, por exemplo, por ter pertencido às autoridades de controlo criadas ao abrigo do artigo 51.º do Regulamento (UE) 2016/679.

(73) A fim de assegurar o controlo e a aplicação coerentes das regras de proteção de dados em toda a União, a Autoridade Europeia para a Proteção de Dados tem as mesmas funções e os mesmos poderes efetivos que as autoridades nacionais de controlo, incluindo poderes de investigação, poderes de correção e poderes sancionatórios, e poderes consultivos e de autorização, nomeadamente em caso de reclamações apresentadas por pessoas singulares, poderes para submeter as violações do presente regulamento à apreciação do Tribunal de Justiça e poderes para intentar processos judiciais, em conformidade com o direito primário. Esses poderes deverão incluir o poder de impor uma limitação temporária ou definitiva do tratamento, ou mesmo a sua proibição. A fim de evitar custos supérfluos e inconvenientes excessivos para as pessoas em causa que possam ser prejudicadas, as medidas da Autoridade Europeia para a Proteção de Dados deverão ser adequadas, necessárias e proporcionadas a fim de garantir a conformidade com o presente regulamento, deverão ter em conta as circunstâncias de cada caso concreto e deverão respeitar o direito de todas as pessoas a serem ouvidas antes de serem tomadas. As medidas juridicamente vinculativas da Autoridade Europeia para a Proteção de Dados deverão ser emitidas por escrito, ser claras e inequívocas, indicar a 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.

(74) A competência de controlo da Autoridade Europeia para a Proteção de Dados não deverá abranger o tratamento de dados pessoais efetuado pelo Tribunal de Justiça quando este atue no exercício dos seus poderes jurisdicionais, a fim de assegurar a independência do Tribunal de Justiça no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Em relação a essas operações de tratamento, o Tribunal de Justiça deverá estabelecer um controlo independente, nos termos do artigo 8.º, n.º 3, da Carta, por exemplo, através de um mecanismo interno.

(75) 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 presente regulamento, deverão 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.

(76) A Autoridade Europeia para a Proteção da Dados deverá cumprir o disposto no Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho ([1]).

(77) As autoridades nacionais de controlo 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 regras de proteção de dados aplicáveis nos Estados-Membros e das regras de proteção de dados aplicáveis às instituições e aos órgãos da União, a Autoridade Europeia para a Proteção de Dados deverá cooperar de modo eficaz com as autoridades nacionais de controlo.

(78) 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. A Autoridade Europeia para a Proteção da Dados é igualmente a autoridade de controlo da Europol e, para esse efeito, 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 regras materiais de proteção de dados, deverá ser introduzido na União um modelo único e coerente de controlo coordenado. A Comissão deverá, portanto, apresentar propostas legislativas, quando apropriado, tendo em vista alterar os atos normativos da União que prevejam um modelo de controlo coordenado, a fim de os alinhar pelo modelo de controlo coordenado do presente regulamento. O Comité Europeu para a Proteção de Dados deverá ser uma instância única para garantir a eficácia do controlo coordenado.

(79) Os titulares dos dados deverão ter o direito de apresentar reclamações à Autoridade Europeia para a Proteção de Dados e o direito de intentar uma ação judicial junto do Tribunal de Justiça, nos termos dos 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 a rejeitar, total ou parcialmente, ou não tomar as medidas necessárias para proteger os seus direitos. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A Autoridade Europeia para a Proteção de Dados deverá 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, deverão ser fornecidas informações intercalares ao titular dos dados. A Autoridade Europeia para a Proteção de Dados deverá 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.

(80) As pessoas que tenham sofrido danos materiais ou imateriais devido a uma violação do presente regulamento deverão ter o direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos, nas condições previstas nos Tratados.

(81) 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 deverá, como medida de último recurso, ter competência para impor coimas. Tais coimas deverão ter por objetivo sancionar a instituição ou o órgão da União — 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 dos órgãos da União. O presente regulamento deverá indicar as infrações sujeitas a coimas, bem como os montantes máximos e os critérios para definir as coimas delas decorrentes. A Autoridade Europeia para a Proteção de Dados deverá determinar o montante máximo da coima em cada caso concreto, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente a natureza, a gravidade e a duração da infração e as 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 uma instituição ou a um órgão da União, a Autoridade Europeia para a Proteção de Dados deverá ter em conta a proporcionalidade do montante da coima. O procedimento administrativo para a aplicação de coimas a instituições e órgãos da União deverá respeitar os princípios gerais do direito da União, tal como interpretados pelo Tribunal de Justiça.

(82) Se o titular dos dados considerar que os direitos que lhe são conferidos pelo presente regulamento foram violados, deverá ter o direito de mandatar um organismo, uma organização ou uma associação sem fins lucrativos que seja constituído ao abrigo do direito da União ou do direito de um Estado-Membro, cujos objetivos estatutários sejam de

([1]) Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho, de 30 de maio de 2001, relativo ao acesso do público aos documentos do Parlamento Europeu, do Conselho e da Comissão (JO L 145 de 31.5.2001, p. 43).

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 deverá também poder exercer o direito de intentar ações judiciais ou de obter uma indemnização em nome dos titulares dos dados.

(83) Os funcionários ou outros agentes da União que não cumpram as obrigações decorrentes do presente regulamento deverão ser passíveis de sanções disciplinares ou de outras medidas, nos termos das regras e dos procedimentos estabelecidos no Estatuto dos Funcionários da União Europeia e do Regime Aplicável aos Outros Agentes da União Europeia, constante do Regulamento (CEE, Euratom, CECA) n.º 259/68 do Conselho ([1]) («Estatuto dos Funcionários»).

(84) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho ([2]). O procedimento de exame deverá ser utilizado para a adoção de cláusulas contratuais-tipo entre os responsáveis pelo tratamento e os subcontratantes, e entre os subcontratantes, para a adoção de uma lista das operações de tratamento que requerem a consulta prévia da Autoridade Europeia para a Proteção de Dados pelos responsáveis pelo tratamento de dados pessoais para a execução de uma missão de interesse público e para a adoção de cláusulas contratuais-tipo que estabelecem as garantias adequadas para transferências internacionais.

(85) As informações confidenciais que a União e as autoridades nacionais de estatística recolhem para a produção de estatísticas oficiais europeias e nacionais deverão ser protegidas. Deverão ser concebidas, 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 ([3]) prevê especificações suplementares em matéria de segredo estatístico aplicáveis às estatísticas europeias.

(86) O Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE do Parlamento Europeu, do Conselho e da Comissão ([4]) deverão ser revogados. As referências ao regulamento e à decisão revogados deverão ser entendidas como referências ao presente regulamento.

(87) A fim de garantir a plena independência dos membros da autoridade independente de controlo, os mandatos da atual Autoridade Europeia para a Proteção de Dados e da atual Autoridade Adjunta não deverão ser afetados pelo presente regulamento. A atual Autoridade Adjunta deverá 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 estabelecidas no presente regulamento. As disposições relevantes do presente regulamento deverão aplicar-se à Autoridade Adjunta até ao termo do seu mandato.

(88) De acordo com o princípio da proporcionalidade, para alcançar o objetivo fundamental de garantir um nível equivalente de proteção das pessoas singulares no que respeita à proteção dos dados pessoais e à livre circulação de dados pessoais na União, é necessário e conveniente estabelecer regras sobre o tratamento de dados pessoais nas instituições e nos órgãos da União. O presente regulamento não excede o necessário para alcançar os objetivos previstos, nos termos do artigo 5.º, n.º 4, do TUE.

(89) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 28.º, n.º 2, do Regulamento (CE) n.º 45/2001 e emitiu parecer em 15 de março de 2017 ([5]),

---

([1]) JO L 56 de 4.3.1968, p. 1.

([2]) 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).

([3]) 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).

([4]) Decisão n.º 1247/2002/CE do Parlamento Europeu, do Conselho e da Comissão, 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).

([5]) JO C 164 de 24.5.2017, p. 2.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto e objetivos

1. O presente regulamento estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos da União, e regras sobre a livre circulação de dados pessoais entre essas instituições e órgãos, ou entre essas instituições e órgãos e outros destinatários estabelecidos na União.

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 controla a aplicação das disposições do presente regulamento a todas as operações de tratamento efetuadas pelas instituições e pelos órgãos da União.

Artigo 2.º

Âmbito

1. O presente regulamento aplica-se ao tratamento de dados pessoais por todas as instituições e todos os órgãos da União.

2. Ao tratamento de dados pessoais operacionais pelos órgãos e pelos organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, só se aplicam o artigo 3.º e o capítulo IX do presente regulamento.

3. O presente regulamento não se aplica ao tratamento de dados pessoais operacionais pela Europol e pela Procuradoria Europeia, antes de o Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho ([1]) e o Regulamento (UE) 2017/1939 do Conselho ([2]) serem adaptados de acordo com o artigo 98.º do presente regulamento.

4. O presente regulamento não se aplica ao tratamento de dados pessoais pelas missões referidas no artigo 42.º, n.º 1, e nos artigos 43.º e 44.º do TUE.

5. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, e ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

Artigo 3.º

Definições

Para efeitos do presente regulamento, aplicam-se as seguintes definições:

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

2) «Dados pessoais operacionais», todos os dados pessoais tratados por órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, a fim de cumprir os objetivos e de exercer as funções estabelecidos nos atos normativos que criam esses órgãos ou organismos;

([1]) Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (JO L 135 de 24.5.2016, p. 53).

([2]) Regulamento (UE) 2017/1939 do Conselho, de 12 de outubro de 2017, que dá execução a uma cooperação reforçada para a instituição da Procuradoria Europeia (JO L 283 de 31.10.2017, p. 1).

3) «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

4) «Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados a fim de limitar o seu tratamento no futuro;

5) «Definição de perfis», uma forma de tratamento automatizado de dados pessoais que consiste na sua utilização para avaliar certos aspetos pessoais relativos a uma pessoa singular, nomeadamente, para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

6) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sejam sujeitas a medidas técnicas e organizativas destinadas a assegurar que os dados pessoais não sejam atribuídos a uma pessoa singular identificada ou identificável;

7) «Ficheiro», um conjunto estruturado de dados pessoais, acessível segundo critérios específicos, centralizado, descentralizado ou repartido de modo funcional ou geográfico;

8) «Responsável pelo tratamento», a instituição ou o órgão da União, ou a direção-geral ou qualquer outra entidade organizativa que, individualmente ou em conjunto com outras entidades, determina as finalidades e os meios de tratamento dos dados pessoais; caso as finalidades e os meios desse tratamento sejam determinados por um ato específico da União, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União;

9) «Responsáveis pelo tratamento que não sejam instituições ou órgãos da União», os responsáveis pelo tratamento na aceção do artigo 4.º, ponto 7, do Regulamento (UE) 2016/679, e os responsáveis pelo tratamento na aceção do artigo 3.º, ponto 8, da Diretiva (UE) 2016/680;

10) «Instituições e órgãos da União», as instituições, os órgãos e os organismos da União estabelecidos pelo TUE, pelo TFUE ou pelo Tratado Euratom, ou com base nesses tratados;

11) «Autoridade competente», uma autoridade pública de um Estado-Membro competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda da segurança pública e a prevenção de ameaças à segurança pública;

12) «Subcontratante», uma pessoa singular ou coletiva, uma autoridade pública ou outro organismo que tratam dados pessoais por conta do responsável pelo tratamento;

13) «Destinatário», uma pessoa singular ou coletiva, uma autoridade pública ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que podem receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou do direito dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das suas finalidades;

14) «Terceiro», uma pessoa singular ou coletiva, uma autoridade pública, um serviço ou um organismo que não são o titular dos dados, o responsável pelo tratamento, o subcontratante nem as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar dados pessoais;

15) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante uma declaração ou um ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam tratados;

16) «Violação de dados pessoais», uma violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento;

17) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que dão informações únicas sobre a fisiologia ou a saúde dessa pessoa singular, resultantes, designadamente, da análise de uma amostra biológica proveniente da pessoa singular em causa;

18) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitem obter ou confirmar a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

19) «Dados relativos à saúde», dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde;

20) «Serviço da sociedade da informação», um serviço definido no artigo 1.º, n.º 1, alínea b), da Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho ([1]);

21) «Organização internacional», uma organização, e os organismos de direito público internacional por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num tal acordo;

22) «Autoridade nacional de controlo», uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º do Regulamento (UE) 2016/679 ou nos termos do artigo 41.º da Diretiva (UE) 2016/680;

23) «Utilizador», uma pessoa singular que utiliza uma rede ou um equipamento terminal operados sob o controlo de uma instituição ou de um órgão da União;

24) «Lista», uma lista de utilizadores acessível ao público ou uma lista interna de utilizadores disponível numa instituição ou num órgão da União, ou partilhada entre instituições e órgãos da União, em formato eletrónico ou impresso;

25) «Rede de comunicações eletrónicas», um sistema de transmissão, baseado ou não numa infraestrutura permanente ou numa instalação administrativa centralizada, e, se aplicável, os equipamentos de comutação ou de encaminhamento e outros recursos, nomeadamente os elementos da rede não ativos, que permitem o envio de sinais por cabo, por feixes hertzianos, por meios óticos ou por outros meios eletromagnéticos, incluindo as redes de satélites, as redes terrestres fixas (com comutação de circuitos ou de pacotes, incluindo a internet) e móveis, os sistemas de cabos de eletricidade, na medida em que sejam utilizados para a transmissão de sinais, as redes utilizadas para a radiodifusão sonora e televisiva e as redes de televisão por cabo, independentemente do tipo de informações transmitidas;

26) «Equipamento terminal», um equipamento terminal tal como definido no artigo 1.º, ponto 1, da Diretiva 2008/63/CE da Comissão ([2]).

CAPÍTULO II

PRINCÍPIOS GERAIS

Artigo 4.º

Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

a) Tratados de forma lícita, leal e transparente («licitude, lealdade e transparência») em relação ao titular dos dados;

b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não podem ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos não é considerado incompatível com as finalidades iniciais, nos termos do artigo 13.º («limitação das finalidades»);

c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e, se necessário, atualizados; devem ser adotadas todas as medidas adequadas para que os dados pessoais inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora («exatidão»);

([1]) Diretiva (UE) 2015/1535 do Parlamento Europeu e do Conselho, de 9 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação (JO L 241 de 17.9.2015, p. 1).

([2]) Diretiva 2008/63/CE da Comissão, de 20 de junho de 2008, relativa à concorrência nos mercados de equipamentos terminais de telecomunicações (JO L 162 de 21.6.2008, p. 20).

e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 13.º, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e as 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 acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).

2. O responsável pelo tratamento dos dados é responsável pelo cumprimento do n.º 1, e deve poder comprová-lo («responsabilidade»).

Artigo 5.º

Licitude do tratamento

1. O tratamento só é lícito caso, e na medida em que, se verifique pelo menos uma das seguintes situações:

a) O tratamento é necessário para o exercício de funções de interesse público ou para o exercício da autoridade pública de que a instituição ou o órgão da União estão investidos;

b) O tratamento é necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento está sujeito;

c) O tratamento é 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 deu o seu consentimento ao tratamento dos seus dados pessoais para uma ou mais finalidades específicas;

e) O tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.

2. O fundamento para o tratamento referido no n.º 1, alíneas a) e b), é estabelecido no direito da União.

Artigo 6.º

Tratamento para outras finalidades compatíveis

Caso o tratamento para finalidades diferentes daquelas para as quais os dados pessoais foram recolhidos não seja 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 deve ter em conta, a fim de verificar se o tratamento para outras finalidades é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, nomeadamente:

a) As ligações entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior pretendido;

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 para os 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. Caso o tratamento seja 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 e de fácil acesso e numa linguagem clara e simples. Não é vinculativa nenhuma parte dessa declaração que constitua uma 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. Deve ser tão fácil retirar o consentimento quanto dá-lo.

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. Caso seja aplicável o artigo 5.º, n.º 1, alínea d), no que respeita à oferta direta de serviços da sociedade da informação a crianças, o tratamento dos dados pessoais de crianças é lícito se a criança tiver pelo menos 13 anos. Se a criança tiver menos de 13 anos, o tratamento só é lícito caso, 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, nomeadamente as disposições que regulam a validade, a formação ou os efeitos de um contrato em relação a uma criança.

Artigo 9.º

Transmissão de dados pessoais a destinatários estabelecidos na União que não sejam instituições ou órgãos da União

1. Sem prejuízo dos artigos 4.º a 6.º e 10.º, os dados pessoais só podem ser transferidos para destinatários estabelecidos na União que não sejam instituições ou órgãos da União se o destinatário demonstrar que:

a) Os dados são necessários para o desempenho de funções de interesse público ou inerentes ao exercício da autoridade pública de que o destinatário se encontra investido; ou

b) É necessário transmitir os dados para uma finalidade específica no interesse público, e o responsável pelo tratamento estabelecer, caso haja motivos para pressupor que os interesses legítimos do titular dos dados possam vir a ser prejudicados, que a transmissão dos dados pessoais para essa finalidade específica é proporcionada, após ter comprovadamente ponderado os diferentes interesses em jogo.

2. Caso o responsável pelo tratamento dê início à transmissão nos termos do presente artigo, deve demonstrar que a transmissão de dados pessoais é necessária e proporcionada para as finalidades a que se destina, aplicando os critérios referidos no n.º 1, alíneas a) ou b).

3. As instituições e os órgãos da União conciliam o direito à proteção dos dados pessoais com o direito de acesso aos documentos, nos termos do direito da União.

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, e o tratamento de dados genéticos, de dados biométricos para identificar uma pessoa de forma inequívoca, de dados relativos à saúde ou de dados relativos à vida sexual ou à orientação sexual de uma pessoa.

2. O 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 pessoais para uma ou mais finalidades específicas, exceto se o direito da União previr que a proibição a que se refere o n.º 1 não pode ser levantada pelo titular dos dados;

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, que preveja as garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;

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 legítimas e mediante garantias adequadas, por um organismo sem fins lucrativos que constitua uma entidade integrada numa instituição ou num órgão da União e que tenha 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 seus titulares;

e) O tratamento está relacionado com dados pessoais manifestamente tornados públicos pelo seu titular;

f) O tratamento é necessário para a declaração, o exercício ou a defesa de um direito num processo judicial ou caso o Tribunal de Justiça atue no exercício da sua função jurisdicional;

g) O tratamento é necessário por motivos de interesse público importante, com base no direito da União, que deve ser proporcionado em relação ao objetivo visado, deve respeitar a essência do direito à proteção dos dados pessoais e deve 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 a obtenção de 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 as liberdades do titular dos dados, em particular o sigilo profissional; ou

j) O tratamento é necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, com base no direito da União, que deve ser proporcionado em relação ao objetivo visado, deve respeitar a essência do direito à proteção dos dados pessoais e deve prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os 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 ou do direito dos Estados-Membros, ou de regulamentação estabelecida pelas autoridades nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade ao abrigo do direito da União ou do direito dos Estados-Membros, ou de regulamentação estabelecida pelas autoridades nacionais competentes.

Artigo 11.º

Tratamento de dados pessoais relacionados com condenações penais e com infrações

O tratamento de dados pessoais relacionados com condenações penais e com infrações, ou com medidas de segurança conexas, com base no artigo 5.º, n.º 1, só pode ser efetuado sob o controlo de uma autoridade pública, ou se for autorizado por disposições do direito da União que prevejam as garantias adequadas dos direitos e das liberdades dos titulares dos dados.

Artigo 12.º

Tratamento que não exige identificação

1. Se as finalidades para as quais um responsável pelo tratamento 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, a obter ou a tratar informações suplementares para identificar o titular dos dados apenas para 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 este último, se possível, desse facto. Nesses casos, os artigos 17.º a 22.º não são aplicáveis, exceto se o titular dos dados fornecer, a fim de exercer os seus direitos ao abrigo dos referidos artigos, informações adicionais que permitam a sua identificação.

Artigo 13.º

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

O tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos está sujeito às garantias adequadas, nos termos do presente regulamento, dos direitos e das liberdades do titular dos dados. Essas garantias devem assegurar a existência de medidas técnicas e organizativas destinadas a garantir, nomeadamente, o respeito do princípio da minimização de dados. Essas medidas podem incluir a pseudonimização, desde que esses fins possam ser alcançados desse modo. Caso esses fins possam ser atingidos por tratamentos ulteriores que não permitam ou que 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 e das comunicações e 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 as comunicações previstas nos artigos 17.º a 24.º e no artigo 35.º relativas ao tratamento dos dados, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial no que diz respeito às informações dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, nomeadamente, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, as informações podem ser prestadas 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-se a dar seguimento ao pedido do titular dos dados para 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 na sequência de um pedido apresentado nos termos dos artigos 17.º a 24.º, sem demora indevida e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado por 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 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 de intentar uma ação judicial.

5. As informações prestadas nos termos dos artigos 15.º e 16.º e as comunicações e as medidas tomadas nos termos dos artigos 17.º a 24.º e do artigo 35.º são fornecidas gratuitamente. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter recorrente, o responsável pelo tratamento pode recusar-se a dar-lhes seguimento. Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

6. Sem prejuízo do artigo 12.º, caso o responsável pelo tratamento tenha 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 prestar 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 os ícones forem apresentados por via eletrónica, devem ser de leitura automática.

8. Caso a Comissão adote atos delegados, nos termos do artigo 12.º, n.º 8, do Regulamento (UE) 2016/679, a fim de determinar as informações que devem ser apresentadas por meio de ícones e os procedimentos aplicáveis à apresentação de ícones normalizados, as instituições e os órgãos da União devem prestar, se apropriado, as informações previstas nos artigos 15.º e 16.º do presente regulamento, em combinação com esses ícones normalizados.

SECÇÃO 2

Informação e acesso aos dados pessoais

Artigo 15.º

Informações a prestar caso os dados pessoais sejam recolhidos junto do titular dos dados

1. Caso os dados pessoais sejam recolhidos junto do titular dos dados, o responsável pelo tratamento deve prestar-lhe, aquando da recolha dos 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 dos dados;

d) Os destinatários ou as categorias de destinatários dos dados pessoais, se os houver;

e) Se for caso disso, a intenção do responsável pelo tratamento de transferir dados pessoais para um país terceiro ou para uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências referidas no artigo 48.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 titular dos dados as seguintes informações adicionais, necessárias para garantir um tratamento dos dados leal e transparente:

a) O prazo de conservação dos dados pessoais ou, se isso 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 digam respeito ao titular dos dados, bem como a sua retificação ou o seu apagamento, ou a limitação do tratamento no que respeita ao titular dos dados, ou, se 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, e se o titular dos dados 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 desse tratamento para o titular dos dados.

3. Caso o responsável pelo tratamento tenha a intenção de proceder ao tratamento posterior dos dados pessoais para uma finalidade diferente daquela para a qual os dados foram recolhidos, antes de proceder a esse tratamento posterior, deve prestar ao titular dos dados informações sobre essa finalidade diferente e outras informações pertinentes referidas no n.º 2.

4. Os n.ºs 1, 2 e 3 não se aplicam caso, e na medida em que, o titular dos dados já tenha conhecimento das informações em causa.

Artigo 16.º

Informações a prestar caso os dados pessoais não sejam recolhidos junto do titular dos dados

1. Caso os dados pessoais não sejam recolhidos junto do titular dos dados, o responsável pelo tratamento deve prestar-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 dos dados;

d) As categorias dos dados pessoais em questão;

e) Os destinatários ou as categorias de destinatários dos dados pessoais, se os houver;

f) Se for caso disso, a intenção do responsável pelo tratamento de transferir dados pessoais para um destinatário num país terceiro ou para uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências referidas no artigo 48.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 prestar ao titular dos dados as seguintes informações adicionais, necessárias para garantir um tratamento leal e transparente:

a) O prazo de conservação dos dados pessoais ou, se isso 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 digam respeito ao titular dos dados, bem como a sua retificação ou o seu apagamento, ou a limitação do tratamento no que respeita ao titular dos dados, ou, se 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 desse tratamento para o titular dos dados.

3. O responsável pelo tratamento deve prestar 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 foram 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. Caso o responsável pelo tratamento tenha a intenção de proceder ao tratamento posterior dos dados pessoais para uma finalidade diferente daquela para a qual os dados pessoais foram obtidos, antes de proceder a esse tratamento posterior, deve prestar ao titular dos dados informações sobre essa finalidade diferente, e outras informações pertinentes referidas no n.º 2.

5. Os n.ºs 1 a 4 não se aplicam caso, e na medida em que:

a) O titular dos dados já tenha conhecimento das informações;

b) Se comprove a impossibilidade de disponibilizar as informações, ou o esforço envolvido seja desproporcionado, nomeadamente para o tratamento dos dados para fins de arquivo de interesse público, para fins 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 de prejudicar gravemente a concretização dos objetivos desse tratamento;

c) A obtenção ou a divulgação dos dados esteja expressamente prevista no direito da União, que preveja medidas adequadas para proteger os interesses legítimos do titular dos dados; ou

d) Os dados pessoais devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União, inclusive uma obrigação legal de confidencialidade.

6. Nos casos referidos no n.º 5, alínea b), o responsável pelo tratamento toma as medidas adequadas para defender os direitos, as liberdades e os interesses legítimos do titular dos dados, incluindo a divulgação pública das informações.

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 do facto de estarem ou não a ser tratados dados pessoais que lhe dizem respeito, e, em caso afirmativo, 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 aos quais os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

d) Se possível, o prazo previsto de conservação dos dados pessoais ou, se não for 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 dos dados, 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 desse tratamento para o titular dos dados.

2. Caso os dados pessoais sejam transferidos para um país terceiro ou para uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 48.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 seu em contrário, as informações são facultadas num formato eletrónico de uso corrente.

4. O direito de obter uma cópia a que se refere o n.º 3 não pode 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 indevida, 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, inclusive por meio de uma declaração adicional.

Artigo 19.º

Direito ao apagamento dos dados («direito a ser esquecido»)

1. O titular dos dados tem o direito de obter, sem demora indevida, do responsável pelo tratamento o apagamento dos seus dados pessoais, e o responsável pelo tratamento tem a obrigação de apagar os dados pessoais, sem demora indevida, caso 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 não existe 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 prevalecentes que justifiquem o tratamento dos dados;

d) Os dados pessoais foram tratados ilicitamente;

e) Os dados pessoais têm de ser apagados a fim de dar cumprimento a uma obrigação jurídica a que o responsável pelo tratamento está 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. Caso o responsável pelo tratamento tenha tornado públicos os dados pessoais e seja obrigado a apagá-los nos termos do n.º 1, deve tomar as medidas que sejam razoáveis, nomeadamente de caráter técnico, tendo em consideração as tecnologias disponíveis e os custos da sua aplicação, para informar os responsáveis pelo tratamento, ou os responsáveis pelo tratamento que não sejam instituições ou órgãos da União, que efetuam o tratamento dos dados pessoais, de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, ou das cópias ou reproduções dos mesmos.

3. Os n.os 1 e 2 não se aplicam na medida em que o tratamento dos dados seja necessário:

a) Para o exercício da liberdade de expressão e de informação;

b) Para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que o responsável pelo tratamento esteja investido;

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 10.º, n.º 2, alíneas h) e i), e do artigo 10.º, n.º 3;

d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, na medida em que o direito referido no n.º 1 seja suscetível de impossibilitar ou de prejudicar gravemente a concretização dos objetivos desse tratamento; ou

e) Para efeitos de declaração, de exercício ou de 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 verifique uma das seguintes situações:

a) A exatidão dos dados pessoais é contestada pelo titular dos dados, durante um período que permita ao responsável pelo tratamento verificar a exatidão dos dados pessoais, incluindo a sua exaustividade;

b) O tratamento é ilícito e o titular dos dados opõe-se ao apagamento dos dados pessoais e solicita, em contrapartida, a limitação da sua utilização;

c) O responsável pelo tratamento já não necessita dos dados pessoais para fins de tratamento, mas os dados são requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;

d) O titular opôs-se ao tratamento dos dados nos termos do artigo 23.º, n.º 1, até que se verifique se os motivos legítimos do responsável pelo tratamento prevalecem sobre os motivos do titular dos dados.

2. Caso o tratamento tenha sido limitado nos termos do n.º 1, os dados pessoais só podem ser tratados, com exceção da conservação, com o consentimento do titular, ou para efeitos de declaração, de exercício ou de 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 tenha obtido a limitação do tratamento dos dados nos termos do n.º 1 é informado pelo responsável pelo tratamento antes de a limitação do referido tratamento ser levantada.

4. Nos ficheiros automatizados, a limitação do tratamento deve ser, em princípio, assegurada por meios técnicos. O facto de os dados pessoais estarem sujeitos a limitações deve ser indicado no sistema de forma que seja bem claro que os dados pessoais não podem ser utilizados.

Artigo 21.º

Obrigação de notificação da retificação ou do apagamento dos dados pessoais e da limitação do tratamento

O responsável pelo tratamento deve comunicar a cada destinatário ao qual os dados pessoais tenham sido transmitidos a retificação ou o apagamento dos dados pessoais ou a limitação do tratamento realizada nos termos do artigo 18.º, do artigo 19.º, n.º 1, e do artigo 20.º, salvo se essa 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 os transmitir a outro responsável pelo tratamento sem que o responsável ao qual os dados pessoais foram fornecidos possa impedi-lo de o fazer, caso o tratamento:

a) Se baseie 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 nos termos do artigo 5.º, n.º 1, alínea c); e

b) Seja 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 de um responsável pelo tratamento para outro, ou para responsáveis pelo tratamento que não sejam instituições ou órgãos da União, caso 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 nem ao exercício da autoridade pública de que o responsável pelo tratamento esteja investido.

4. O direito a que se refere o n.º 1 não pode 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, salvo se apresentar razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, os direitos e as liberdades do titular dos dados, ou para efeitos de declaração, de exercício ou de 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 o n.º 1 deve ser-lhe explicitamente comunicado, e apresentado de modo claro e destacado de outras informações.

3. Sem prejuízo dos artigos 36.º e 37.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. Caso os dados pessoais sejam 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 o tratamento for necessário por razões de interesse público.

Artigo 24.º

Decisões individuais automatizadas, incluindo a definição de perfis

1. O titular dos dados tem o direito de não ficar sujeito a decisões tomadas exclusivamente com base no tratamento automatizado de dados, incluindo a definição de perfis, que produzam efeitos na sua esfera jurídica ou que o afetem significativamente de forma similar.

2. O n.º 1 não se aplica se a decisão:

a) For necessária para a celebração ou para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento;

b) For autorizada pelo direito da União, o qual prevê também medidas adequadas para salvaguardar os direitos, as liberdades e os interesses legítimos do titular dos dados; ou

c) Se basear 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, as liberdades e os interesses legítimos do titular dos dados, pelo menos o direito de obter a intervenção humana do responsável pelo tratamento, de manifestar o seu ponto de vista e de contestar a decisão.

4. As decisões referidas o n.º 2 do presente artigo não podem basear-se nas categorias especiais de dados pessoais a que se refere o artigo 10.º, n.º 1, salvo caso se aplique o n.º 2, alínea a) ou g), desse artigo, e existam medidas adequadas para salvaguardar os direitos, as liberdades e os interesses legítimos do titular.

SECÇÃO 5

Limitações

Artigo 25.º

Limitações

1. Os atos normativos adotados com base nos tratados ou, em matérias relacionadas com o funcionamento das instituições e dos órgãos da União, as regras internas estabelecidas por estes últimos podem limitar a aplicação dos artigos 14.º a 22.º, dos artigos 35.º e 36.º, e do artigo 4.º, na medida em que as disposições deste artigo correspondam aos direitos e às obrigações previstos nos artigos 14.º a 22.º, desde que tal limitação respeite a essência dos direitos e das liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para salvaguardar:

a) A segurança nacional, a segurança pública e a defesa dos Estados-Membros;

b) A prevenção, a investigação, a deteção e a repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda da segurança pública e a prevenção de ameaças à segurança pública;

c) Outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente os objetivos da política externa e de segurança comum da União, ou um interesse económico ou financeiro importante da União ou de um Estado-Membro, inclusive de ordem monetária, orçamental e fiscal, de saúde pública e de segurança social;

d) A segurança interna das instituições e dos órgãos da União, incluindo as suas redes de comunicações eletrónicas;

e) A defesa da independência judiciária e dos processos judiciais;

f) A prevenção, a investigação, a deteção e a repressão de violações da deontologia das 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 terceiros;

i) A execução de ações cíveis.

2. Em especial, os atos normativos e as regras internas a que se refere o n.º 1 incluem disposições explícitas, se tal for relevante, relativas:

a) Às finalidades do tratamento ou às diferentes categorias de tratamento;

b) Às categorias de dados pessoais;

c) Ao alcance das limitações impostas;

d) Às garantias para evitar o abuso ou o acesso ou transferência ilícitos;

e) À especificação do responsável pelo tratamento ou às categorias de responsáveis pelo tratamento;

f) Aos prazos de conservação e às garantias aplicáveis, tendo em conta a natureza, o âmbito e os objetivos do tratamento ou das categorias de tratamento; e

g) Aos riscos para os direitos e para as liberdades dos titulares dos dados.

3. Caso os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos, o direito da União, que pode incluir regras internas adotadas pelas instituições e pelos órgãos da União em matérias relacionadas com o seu funcionamento, pode prever derrogações dos direitos a que se referem os artigos 17.º, 18.º, 20.º e 23.º, sob reserva das condições e das garantias previstas no artigo 13.º, na medida em que esses direitos sejam suscetíveis de impossibilitar ou de prejudicar gravemente a consecução de finalidades específicas, e essas derrogações sejam necessárias para a consecução dessas finalidades.

4. Caso os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União, que pode incluir regras internas adotadas pelas instituições e pelos órgãos da União em matérias relacionadas com o seu funcionamento, pode prever derrogações dos 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 das garantias previstas no artigo 13.º, na medida em que esses direitos sejam suscetíveis de impossibilitar ou de prejudicar gravemente a consecução de finalidades específicas, e essas derrogações sejam necessárias para a consecução dessas finalidades.

5. As regras internas referidas nos n.os 1, 3 e 4 devem constituir atos claros e precisos de aplicação geral, destinados a produzir efeitos jurídicos em relação aos titulares dos dados, adotados ao mais alto nível de direção das instituições e dos órgãos da União e sujeitos a publicação no *Jornal Oficial da União Europeia*.

6. Se for imposta uma limitação nos termos do n.º 1, o titular dos dados deve ser informado, nos termos do 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. Caso seja invocada uma limitação imposta nos termos do n.º 1 para recusar o acesso ao titular dos dados, a Autoridade Europeia para a Proteção de Dados, ao investigar a reclamação, comunica-lhe unicamente se os dados foram tratados corretamente e, em caso negativo, se as correções necessárias foram introduzidas.

8. A comunicação das informações referida nos n.os 6 e 7 do presente artigo e no artigo 45.º, n.º 2, pode ser adiada, omitida ou recusada caso se presuma que anule o efeito da limitação imposta nos termos do n.º 1 do presente artigo.

CAPÍTULO IV

RESPONSÁVEIS PELO TRATAMENTO E SUBCONTRATANTES

SECÇÃO 1

Obrigações gerais

Artigo 26.º

Responsabilidade dos responsáveis pelo tratamento

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos, de probabilidade e gravidade variáveis, para os direitos e as liberdades das pessoas singulares, o responsável pelo tratamento deve aplicar as medidas técnicas e organizativas adequadas para assegurar e para 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 medidas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.

3. O cumprimento de procedimentos de certificação aprovados a que se refere o artigo 42.º do Regulamento (UE) 2016/679 pode ser utilizado como um elemento demonstrativo do cumprimento das obrigações do 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 as liberdades das pessoas singulares, de probabilidade e gravidade variáveis, o responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios de tratamento como durante o próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a pôr efetivamente em prática os princípios da proteção de dados, como a minimização, e a integrar as garantias necessárias no tratamento a fim de cumprir os requisitos do presente regulamento e de proteger os direitos dos titulares dos dados.

2. O responsável pelo tratamento deve aplicar medidas técnicas e organizativas adequadas 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.

3. O cumprimento de procedimentos de certificação aprovados nos termos do artigo 42.º do Regulamento (UE) 2016/679 pode ser utilizado como um elemento demonstrativo do cumprimento das obrigações estabelecidas nos n.os 1 e 2 do presente artigo.

Artigo 28.º

Responsáveis conjuntos pelo tratamento

1. Caso dois ou mais responsáveis pelo tratamento, ou um ou mais responsáveis pelo tratamento juntamente com um ou mais responsáveis pelo tratamento que não sejam instituições ou órgãos da União, determinem em conjunto as finalidades e os meios do tratamento, são considerados responsáveis conjuntos pelo tratamento. Os responsáveis conjuntos pelo tratamento determinam, por acordo entre si e de modo transparente, as respetivas responsabilidades pelo cumprimento das suas obrigações em matéria de proteção de dados, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos seus deveres de prestar as informações referidas nos artigos 15.º e 16.º, a não ser e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou pelo direito do Estado-Membro a que estão sujeitos. No referido acordo, pode ser designado 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 as relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. O teor do acordo deve ser disponibilizado ao titular dos dados.

3. Independentemente dos termos do acordo a que se refere o n.º 1, o titular dos dados pode exercer os direitos que o presente regulamento lhe confere em relação a, e contra, cada um dos responsáveis pelo tratamento.

Artigo 29.º

Subcontratantes

1. Caso o tratamento dos dados seja 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 tal forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.

2. O subcontratante não pode contratar outro subcontratante sem autorização escrita prévia, específica ou geral, do responsável pelo tratamento. Em caso de autorização geral por escrito, o subcontratante deve informar o responsável pelo tratamento das 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 essas alterações.

3. O tratamento por subcontratação é regulado por contrato ou por outro ato normativo ao abrigo do direito da União ou do direito dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a sua natureza e a sua finalidade, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e os 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, nomeadamente no que respeita às transferências de dados pessoais para países terceiros ou para organizações internacionais, salvo se for obrigado a fazê-lo pelo direito da União ou pelo direito 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 às obrigações legais de confidencialidade adequadas;

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) Tendo em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas destinadas a permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados para o exercício dos seus direitos previstos no capítulo III;

f) Presta assistência ao responsável pelo tratamento para assegurar o cumprimento das obrigações previstas nos artigos 33.º a 41.º, tendo em conta a natureza do tratamento e as informações ao seu dispor;

g) Consoante a escolha do responsável pelo tratamento, apaga todos os dados pessoais ou devolve-lhos uma vez concluída a prestação de serviços relacionados com o tratamento, e apaga as cópias existentes, salvo se a conservação dos dados pessoais for exigida ao abrigo do direito da União ou do direito dos Estados-Membros;

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, incluindo as inspeções, realizadas pelo responsável pelo tratamento ou por outro auditor por ele mandatado.

No que diz respeito ao primeiro parágrafo, alínea h), 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 do direito dos Estados-Membros em matéria de proteção de dados.

4. Caso o subcontratante contrate outro subcontratante para realizar operações específicas de tratamento por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou por outro ato normativo ao abrigo do direito da União ou do direito dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou noutro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no n.º 3, em particular a obrigação de apresentar garantias suficientes de aplicar as medidas técnicas e organizativas adequadas de forma que o tratamento satisfaça 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. Caso o subcontratante não seja uma instituição ou um órgão da União, o cumprimento de um código de conduta aprovado a que se refere o artigo 40.º, n.º 5, do Regulamento (UE) 2016/679, ou de um procedimento de certificação aprovado a que se refere o artigo 42.º do Regulamento (UE) 2016/679, pode ser utilizado como um elemento demonstrativo das garantias suficientes referidas nos n.os 1 e 4 do presente artigo.

6. Sem prejuízo da existência de um contrato entre o responsável pelo tratamento e o subcontratante, o contrato ou o outro ato normativo referidos nos n.os 3 e 4 do presente artigo podem basear-se, total ou parcialmente, nas cláusulas contratuais-tipo referidas nos n.os 7 e 8 do presente artigo, inclusive caso façam parte de uma certificação concedida ao subcontratante que não seja uma instituição ou um órgão 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 pelo procedimento de exame a que se refere o artigo 96.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 o outro ato normativo a que se referem os n.os 3 e 4 é feito por escrito, inclusive em formato eletrónico.

10. Sem prejuízo dos artigos 65.º e 66.º, o subcontratante que, em violação do presente regulamento, determine as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão.

Artigo 30.º

Tratamento sob a autoridade do responsável pelo tratamento ou 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 procede ao tratamento desses dados a não ser por instrução do responsável pelo tratamento, salvo se a tal for obrigado pelo direito da União ou pelo direito 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, do encarregado da proteção de dados e, se for caso disso, do subcontratante e do 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 ou em países terceiros, ou pertencentes a organizações internacionais;

e) Se for aplicável, as transferências de dados pessoais para um país terceiro ou para 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 os contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, e 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 para 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 feitos por escrito, inclusive em formato eletrónico.

4. As instituições e os órgãos da União disponibilizam os registos, a pedido, à Autoridade Europeia para a Proteção de Dados.

5. A não ser que tal não seja adequado devido à dimensão da instituição ou do órgão da União, as instituições e os órgãos da União conservam os seus registos de atividades de tratamento num registo central. O registo é acessível ao público.

Artigo 32.º

Cooperação com a Autoridade Europeia para a Proteção de Dados

As instituições e os órgãos da União cooperam, a pedido, com a Autoridade Europeia para a Proteção de Dados no exercício das suas funções.

SECÇÃO 2

Segurança dos dados pessoais

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 variáveis, para os direitos e as liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam medidas técnicas e organizativas apropriadas para assegurar um nível de segurança adequado ao risco, nomeadamente, conforme adequado:

a) A pseudonimização e a cifragem dos dados pessoais;

b) A capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência permanentes dos sistemas e dos serviços de tratamento;

c) A capacidade de restabelecer atempadamente a disponibilidade e o acesso aos dados pessoais em caso de incidente físico ou técnico;

d) Um processo para testar, apreciar e avaliar periodicamente 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 os riscos decorrentes da destruição, da perda e da alteração acidentais ou ilícitas dos dados, e da divulgação ou do acesso não autorizados dos 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 as pessoas singulares que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenham acesso a dados pessoais, só procedam ao seu tratamento mediante instruções do responsável pelo tratamento, salvo se a tal forem obrigadas pelo direito da União.

4. O cumprimento de um procedimento de certificação aprovado a que se refere o artigo 42.º do Regulamento (UE) 2016/679 pode ser utilizado como um elemento demonstrativo do cumprimento das obrigações estabelecidas no n.º 1 do presente artigo.

Artigo 34.º

Notificação de violações dos dados pessoais à Autoridade Europeia para a Proteção de Dados

1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a Autoridade Europeia para a Proteção de Dados sem demora indevida e, se possível, no prazo de 72 horas após ter tido conhecimento da violação, salvo se essa violação não for suscetível de constituir um risco para os direitos e para as liberdades das pessoas singulares. Caso não seja feita no prazo de 72 horas, a notificação à Autoridade Europeia para a Proteção de Dados deve ser acompanhada dos motivos do atraso.

2. O subcontratante deve notificar o responsável pelo tratamento sem demora indevida após tomar conhecimento de uma violação de dados pessoais.

3. A notificação referida no n.º 1 deve, pelo menos:

a) Descrever a natureza da violação de dados pessoais, incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, e as categorias e o número aproximado de registos de dados pessoais em causa;

b) Comunicar o nome e os 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 reparar a violação de dados pessoais, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

4. Caso, e na medida em que, não seja possível comunicar todas as informações ao mesmo tempo, as informações podem ser comunicadas por fases, sem demora indevida.

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 todas as violações de dados pessoais, incluindo os factos relacionados com a violação, os seus efeitos e as medidas de reparação adotadas. Essa documentação deve permitir à Autoridade Europeia para a Proteção de Dados verificar o respeito do presente artigo.

Artigo 35.º

Comunicação de violações de dados pessoais ao titular dos dados

1. Caso uma violação de dados pessoais seja suscetível de constituir um elevado risco para os direitos e para as liberdades das pessoas singulares, o responsável pelo tratamento deve comunicá-la ao titular dos dados sem demora indevida.

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 de dados pessoais e incluir, pelo menos, as informações e as medidas referidas no artigo 34.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 obrigatória caso esteja satisfeita uma das seguintes condições:

a) O responsável pelo tratamento aplicou medidas técnicas e organizativas de proteção adequadas aos dados pessoais afetados pela violação, nomeadamente medidas como, por exemplo, a cifragem, que tornam os dados pessoais incompreensíveis para as pessoas não autorizadas a aceder a esses dados;

b) O responsável pelo tratamento tomou medidas subsequentes que asseguram que o elevado risco para os direitos e para as liberdades dos titulares dos dados a que se refere o n.º 1 já não é suscetível de se concretizar;

c) A comunicação implicaria 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 ainda não tiver comunicado a violação de dados pessoais ao titular dos dados, a Autoridade Europeia para a Proteção de Dados, tendo avaliado a probabilidade de a violação de dados pessoais implicar um elevado risco, pode exigir-lhe que proceda a essa comunicação, ou pode constatar que está satisfeita uma das condições referidas no n.º 3.

SECÇÃO 3

Confidencialidade das comunicações eletrónicas

Artigo 36.º

Confidencialidade das comunicações eletrónicas

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

Artigo 37.º

Proteção das informações transmitidas aos equipamentos terminais dos utilizadores, neles conservadas e com eles relacionadas, e das informações tratadas e recolhidas através desses equipamentos

As instituições e os órgãos da União devem proteger as informações transmitidas aos equipamentos terminais dos utilizadores que acedem aos seus sítios Web e a aplicações móveis acessíveis ao público, conservadas nesses equipamentos e com eles relacionadas, e das informações tratadas e recolhidas através desses equipamentos, nos termos do artigo 5.º, n.º 3, da Diretiva 2002/58/CE.

Artigo 38.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 os órgãos da União devem tomar todas as medidas necessárias para impedir que os dados pessoais incluídos nessas listas, independentemente de as mesmas serem ou não acessíveis ao público, sejam utilizados para fins de *marketing* direto.

SECÇÃO 4

Avaliação de impacto relativa à proteção de dados e consulta prévia

Artigo 39.º

Avaliação de impacto relativa à proteção de dados

1. Caso um tipo de tratamento, em particular, um tipo de tratamento que utilize novas tecnologias, seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares, o responsável pelo tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento, deve proceder, antes de iniciar o tratamento, a uma avaliação do impacto das operações de tratamento previstas na 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 relativa à 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 relativa à proteção de dados a que se refere o n.º 1 é obrigatória, nomeadamente, em caso de:

a) Uma avaliação sistemática aprofundada dos aspetos pessoais relacionados com pessoas singulares baseada no tratamento automatizado, incluindo a definição de perfis, com base na qual são adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;

b) Um tratamento em grande escala de categorias especiais de dados a que se refere o artigo 10.º, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 11.º; ou

c) Um controlo sistemático em grande escala de uma zona acessível ao público.

4. A Autoridade Europeia para a Proteção de Dados deve estabelecer e tornar pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto relativa à proteção de dados nos termos do 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 a avaliação de impacto relativa à proteção de dados não é obrigatória.

6. Antes de adotar as listas referidas nos n.os 4 e 5 do presente artigo, a Autoridade Europeia para a Proteção de Dados solicita que o Comité Europeu para a Proteção de Dados criado pelo artigo 68.º do Regulamento (UE) 2016/679 analise essas listas nos termos do artigo 70.º, n.º 1, alínea e), desse regulamento, caso se refiram a operações de tratamento efetuadas por um responsável pelo tratamento que atue em conjunto com um ou mais responsáveis pelo tratamento que não sejam uma instituição ou um organismo da União.

7. 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 da proporcionalidade das operações de tratamento em relação às finalidades;

c) Uma avaliação dos riscos para os direitos e as liberdades dos titulares de dados a que se refere o n.º 1; e

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, as medidas de segurança e os procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os interesses legítimos dos titulares dos dados e de outras pessoas afetadas.

8. Ao avaliar o impacto das operações de tratamento efetuadas pelos subcontratantes, em especial para efeitos de uma avaliação de impacto relativa à 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 pelos subcontratantes em causa que não sejam instituições ou órgãos da União.

9. 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.

10. Se o tratamento efetuado por força do artigo 5.º, n.º 1, alíneas a) ou b), tiver por fundamento jurídico um ato normativo 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 normativo, não se aplicam os n.os 1 a 6 do presente artigo, salvo disposição em contrário prevista nesse ato normativo.

11. Se necessário, o responsável pelo tratamento deve proceder a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto relativa à proteção de dados, pelo menos quando existir uma alteração do risco representado pelas operações de tratamento.

Artigo 40.º

Consulta prévia

1. O responsável pelo tratamento deve consultar a Autoridade Europeia para a Proteção de Dados antes de proceder ao tratamento, caso uma avaliação de impacto relativa à proteção de dados, efetuada nos termos do artigo 39.º, indique que o tratamento, na falta de garantias, de medidas e de procedimentos de segurança para atenuar os riscos, constitui um elevado risco para os direitos e as liberdades das pessoas singulares, e o responsável pelo tratamento considere que o risco não poderá ser atenuado através de meios razoáveis, tendo em conta as tecnologias disponíveis e os custos de aplicação. O responsável pelo tratamento deve solicitar o parecer do encarregado da proteção de dados sobre a necessidade da consulta prévia.

2. Caso a Autoridade Europeia para a Proteção de Dados considere que o tratamento previsto a que se refere o n.º 1 violaria o presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deve emitir orientações por escrito, no prazo máximo de oito semanas a contar da receção do pedido de consulta, destinadas ao responsável pelo tratamento e, se aplicável, ao subcontratante, e pode recorrer a todos os seus poderes referidos no artigo 58.º. Esse prazo pode ser prorrogado por seis semanas, tendo em conta a complexidade do tratamento previsto. A Autoridade Europeia para a Proteção de Dados deve informar da prorrogação o responsável pelo tratamento e, se aplicável, o subcontratante, no prazo de um mês a contar da data de receção do pedido de consulta, indicando os motivos do atraso. Esses prazos podem ser suspensos até a Autoridade Europeia para a Proteção de Dados ter obtido as informações solicitadas para os 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 a 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 relativa à proteção de dados prevista no artigo 39.º; e

f) Outras informações solicitadas pela Autoridade Europeia para a Proteção de Dados.

4. A Comissão pode elaborar, mediante um ato de execução, uma lista de casos em que os responsáveis pelo tratamento devem consultar a Autoridade Europeia para a Proteção de Dados e dela obter a autorização prévia no que diz respeito ao tratamento de dados pessoais 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 5

Informação e consulta legislativa

Artigo 41.º

Informação e consulta

1. As instituições e os órgãos da União devem informar a Autoridade Europeia para a Proteção de Dados da elaboração de medidas administrativas e de regras internas relativas ao tratamento de dados pessoais por uma instituição ou por um órgão da União, quer individualmente quer conjuntamente.

2. Quando elaborarem as regras internas referidas no artigo 25.º, as instituições e os órgãos da União devem consultar a Autoridade Europeia para a Proteção de Dados.

Artigo 42.º

Consulta legislativa

1. Após ter adotado propostas de atos legislativos, recomendações ou propostas ao Conselho nos termos do artigo 218.º do TFUE, ou quando elaborar atos delegados ou atos de execução, a Comissão deve consultar a Autoridade Europeia para a Proteção de Dados caso exista um impacto na proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

2. Caso um ato referido no n.º 1 tenha particular importância para a proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais, a Comissão pode consultar também 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 emitir um parecer comum.

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 referido nos n.ºs 1 e 2. Em casos urgentes, ou sempre que necessário, a Comissão pode reduzir esse 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 6

Encarregado da proteção de dados

Artigo 43.º

Designação do encarregado da proteção de dados

1. Cada instituição ou órgão da União deve designar um encarregado da proteção de dados.

2. As instituições e os órgãos da União podem designar um único encarregado da proteção de dados para várias instituições e órgãos, tendo em conta a sua dimensão e a sua estrutura organizativa.

3. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em particular, 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 45.º.

4. O encarregado da proteção de dados deve ser um membro do pessoal da instituição ou do órgão da União. Tendo em conta a sua dimensão, e se a opção prevista no n.º 2 não for exercida, as instituições e os órgãos da União podem designar um encarregado da proteção de dados que exerça as suas funções com base num contrato de prestação de serviços.

5. As instituições e os órgãos da União publicam os contactos do encarregado da proteção de dados e comunicam-nos à Autoridade Europeia para a Proteção de Dados.

Artigo 44.º

Posição do encarregado da proteção de dados

1. As instituições e os órgãos da União devem assegurar que o encarregado da proteção de dados seja envolvido, de forma adequada e atempada, em todas as matérias relacionadas com a proteção de dados pessoais.

2. As instituições e os órgãos da União devem apoiar o encarregado da proteção de dados no exercício das funções referidas no artigo 45.º, fornecendo-lhe os recursos necessários para desempenhar essas funções e para aceder aos dados pessoais e às operações de tratamento, e para manter os seus conhecimentos especializados.

3. As instituições e os órgãos da União devem assegurar que o encarregado da proteção de dados não receba instruções no que diz respeito ao exercício dessas funções. O encarregado da proteção de dados não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo exercício das suas funções. O encarregado da proteção de dados reporta diretamente ao mais alto nível da direção 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 com o exercício dos direitos que lhes são conferidos pelo presente regulamento.

5. O encarregado da proteção de dados e o seu pessoal estão vinculados 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 deem origem a conflitos de interesses.

7. O encarregado da proteção de dados pode ser consultado sobre qualquer questão relativa à interpretação ou à aplicação do presente regulamento pelo responsável pelo tratamento e pelo subcontratante, pelo Comité do Pessoal ou por qualquer outra pessoa singular, sem que estes tenham que recorrer às vias oficiais. Ninguém pode ser prejudicado por uma questão levada ao conhecimento do encarregado da proteção de dados competente por alegadamente constituir uma violação 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 destituído pela instituição ou pelo órgão da União que o nomeou se tiver deixado de preencher as condições exigidas para o exercício das suas funções, e unicamente com o acordo da Autoridade Europeia para a Proteção de Dados.

9. Após a designação do encarregado da proteção de dados, o seu nome é comunicado à Autoridade Europeia para a Proteção de Dados pela instituição ou pelo órgão da União que o tenha designado.

Artigo 45.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, e os membros do pessoal que tratam 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; controlar o cumprimento do presente regulamento, de outras disposições aplicáveis do direito da União relativas à proteção de dados 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, e as auditorias correspondentes;

c) Garantir que os titulares dos dados sejam 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, nos termos dos artigos 34.º e 35.º;

e) Prestar aconselhamento, quando tal lhe for solicitado, no que diz respeito à avaliação de impacto relativa à proteção de dados, e controlar a sua realização 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 relativa à proteção de dados;

f) Prestar aconselhamento, quando tal lhe for solicitado, sobre a necessidade de consulta prévia da Autoridade Europeia para a Proteção de Dados nos termos do artigo 40.º; e consultar a Autoridade Europeia para a Proteção de Dados em caso de dúvida quanto à necessidade de consulta prévia;

g) Responder aos pedidos da Autoridade Europeia para a Proteção de Dados; no âmbito da sua esfera de competência, cooperar com a Autoridade Europeia para a Proteção de Dados e consultá-la, a seu pedido ou por iniciativa própria;

h) Assegurar que as operações de tratamento não atentem contra os direitos e as liberdades dos titulares dos dados.

2. O encarregado da proteção de dados pode emitir recomendações dirigidas ao responsável pelo tratamento e ao subcontratante a fim de melhorar concretamente a proteção de dados, e aconselhá-los sobre matérias relativas à aplicação das disposições relativas à proteção de dados. Além disso, por iniciativa própria ou a pedido do responsável pelo tratamento ou do subcontratante, do comité de pessoal ou de qualquer pessoa, pode investigar questões e factos diretamente relacionados com as suas funções de que tenha tido conhecimento e, se necessário, informar a pessoa que solicitou a investigação ou o responsável pelo tratamento ou o subcontratante.

3. Devem ser adotadas disposições de execução complementares respeitantes ao encarregado da proteção de dados por cada instituição ou órgão da União. Essas disposições de execução devem incidir em especial sobre as funções e as competências do encarregado da proteção de dados.

CAPÍTULO V

TRANSFERÊNCIAS DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

Artigo 46.º

Princípio geral das transferências

As transferências de dados pessoais, que sejam ou venham a ser objeto de tratamento após a transferência para um país terceiro ou para uma organização internacional, só são realizadas 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 para outra organização internacional. Todas as disposições do presente capítulo devem ser aplicadas de forma a assegurar que o nível de proteção das pessoas singulares garantido pelo presente regulamento não seja comprometido.

Artigo 47.º

Transferências com base numa decisão de adequação

1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou para uma organização internacional se a Comissão tiver decidido, por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ou do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, que o país terceiro, um território ou um setor ou setores específicos desse país terceiro, ou a organização internacional em causa, garantem um nível de proteção adequado, e se os dados pessoais forem transferidos exclusivamente para o desempenho de funções da competência do responsável pelo tratamento.

2. As instituições e os órgãos da União devem informar a Comissão e a Autoridade Europeia para a Proteção de Dados dos casos em que consideram que um país terceiro, um território, um setor ou setores específicos de um país terceiro, ou uma organização internacional não garantem um nível de proteção adequado nos termos do n.º 1.

3. As instituições e os órgãos da União devem tomar as medidas necessárias para dar cumprimento às decisões tomadas pela Comissão, caso esta estabeleça, ao abrigo do artigo 45.º, n.ºs 3 ou 5, do Regulamento (UE) 2016/679, ou do artigo 36.º, n.ºs 3 ou 5, da Diretiva (UE) 2016/680, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, asseguram ou deixaram de assegurar um nível de proteção adequado.

Artigo 48.º

Transferências sujeitas a garantias adequadas

1. Na falta de uma decisão nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ou do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, os responsáveis pelo tratamento ou os subcontratantes só podem transferir dados pessoais para um país terceiro ou para 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. As garantias adequadas a que se refere o n.º 1 podem ser previstas, sem 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 pelo procedimento de exame a que se refere o artigo 96.º, n.º 2;

c) Cláusulas-tipo de proteção de dados adotadas pela Autoridade Europeia para a Proteção de Dados e aprovadas pela Comissão pelo procedimento de exame a que se refere o artigo 96.º, n.º 2;

d) Nos casos em que o subcontratante não é uma instituição ou um órgão da União, regras vinculativas aplicáveis às empresas, códigos de conduta ou procedimentos de certificação, ao abrigo do artigo 46.º, n.º 2, alíneas b), e) e f), do Regulamento (UE) 2016/679.

3. Sob reserva de autorização da Autoridade Europeia para a Proteção de Dados, as garantias adequadas a que se refere o n.º 1 podem também ser previstas, 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 autorizações concedidas pela Autoridade Europeia para a Proteção de Dados com base no artigo 9.º, n.º 7, do Regulamento (CE) n.º 45/2001 mantêm-se válidas até à sua alteração, substituição ou revogação, se necessário, pela Autoridade Europeia para a Proteção de Dados.

5. As instituições e os órgãos da União devem informar a Autoridade Europeia para a Proteção de Dados das categorias de casos em que o presente artigo foi aplicado.

Artigo 49.º

Transferências ou divulgações não autorizadas pelo direito da União

As decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento ou o subcontratante transfiram ou divulguem dados pessoais só são reconhecidas ou executadas se tiverem por base um acordo internacional, como, por exemplo, 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 50.º

Derrogações em situações específicas

1. Na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ou do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, ou de garantias adequadas nos termos do artigo 48.º do presente regulamento, uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro ou para uma organização internacional só são efetuadas caso se verifique uma das seguintes condições:

a) O titular dos dados deu o seu consentimento explícito 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 é necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou para a aplicação de diligências prévias à formação do contrato decididas a pedido do titular dos dados;

c) A transferência é necessária para a celebração ou para a execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo tratamento e outra pessoa singular ou coletiva;

d) A transferência é necessária por razões importantes de interesse público;

e) A transferência é necessária para a declaração, o exercício ou a defesa de um direito num processo judicial;

f) A transferência é necessária para proteger os interesses vitais do titular dos dados ou de outras pessoas, se o titular dos dados estiver física ou legalmente incapaz de dar o seu consentimento; ou

g) A transferência é realizada a partir de um registo que, nos termos do direito da União, se destina à informação do público e se encontra 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. As alíneas a), b), e c) do n.º 1 não são aplicáveis a atividades executadas por instituições e órgãos da União no exercício dos seus poderes públicos.

3. O interesse público referido no n.º 1, alínea d), deve ser reconhecido no direito da União.

4. Uma transferência efetuada nos termos do n.º 1, alínea g), não pode 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.

5. Na falta de uma decisão de adequação, o direito da União pode estabelecer expressamente, por razões importantes de interesse público, limites à transferência de categorias específicas de dados pessoais para países terceiros ou para organizações internacionais.

6. As instituições e os órgãos da União devem informar a Autoridade Europeia para a Proteção de Dados das categorias de casos em que o presente artigo foi aplicado.

Artigo 51.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 com 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 relativa à 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 às 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 relativas à proteção de dados pessoais, inclusive no que diz respeito a conflitos de competência com países terceiros.

CAPÍTULO VI

AUTORIDADE EUROPEIA PARA A PROTEÇÃO DE DADOS

Artigo 52.º

Autoridade Europeia para a Proteção de Dados

1. É criada 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 as liberdades fundamentais das pessoas singulares, especialmente o direito à proteção de dados, sejam respeitados pelas instituições e pelos órgãos 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 das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais por uma instituição ou um órgão da União, bem como do aconselhamento das instituições e dos órgãos 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 57.º e os poderes conferidos pelo artigo 58.º.

4. O Regulamento (CE) n.º 1049/2001 é aplicável aos documentos detidos pela Autoridade Europeia para a Proteção de Dados. A Autoridade Europeia para a Proteção de Dados adota as regras de aplicação do Regulamento (CE) n.º 1049/2001 no que diz respeito a esses documentos.

Artigo 53.º

Nomeação da Autoridade Europeia para a Proteção de Dados

1. O Parlamento Europeu e o Conselho nomeiam, de comum acordo e por um período de cinco anos, a Autoridade Europeia para a Proteção de Dados, 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 elaborada pela Comissão é pública e deve ser constituída, no mínimo, por três candidatos. Com base na lista elaborada pela Comissão, a comissão competente do Parlamento Europeu pode decidir realizar uma audição que lhe permita exprimir a sua preferência.

2. A lista de candidatos referida no n.º 1 deve ser constituída por pessoas que ofereçam todas as garantias de independência e que disponham de conhecimentos especializados no domínio da proteção de dados, além da experiência e da competência requeridas para o desempenho das funções de Autoridade Europeia para a Proteção de Dados.

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 exoneração 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, 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 exoneração 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 54.º

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

1. A Autoridade Europeia para a Proteção de Dados é considerada equiparada a um juiz do Tribunal de Justiça no que se refere à determinação da remuneração, dos subsídios, da pensão de reforma e de quaisquer outros benefícios equivalentes à remuneração que lhe sejam devidos.

2. A autoridade orçamental deve assegurar que a Autoridade Europeia para a Proteção de Dados disponha dos recursos humanos e financeiros necessários para o desempenho das suas funções.

3. O orçamento da Autoridade Europeia para a Proteção de Dados deve figurar numa rubrica específica da secção relativa às despesas administrativas do orçamento geral da União.

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 dependem exclusivamente dela. O seu número é aprovado anualmente no âmbito do exercício orçamental. O artigo 75.º, n.º 2, do Regulamento (UE) 2016/679 é aplicável ao pessoal da Autoridade Europeia para a Proteção de Dados que desempenha as atribuições conferidas ao Comité Europeu para a Proteção de Dados pelo direito da União.

5. Os funcionários e outros agentes do secretariado da Autoridade Europeia para a Proteção de Dados estão sujeitos às regras e à regulamentação aplicáveis aos funcionários e outros agentes da União.

6. A Autoridade Europeia para a Proteção de Dados tem sede em Bruxelas.

Artigo 55.º

Independência

1. A Autoridade Europeia para a Proteção de Dados desempenha as suas funções e exerce os seus poderes com total independência, nos termos do 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 terceiros.

3. A Autoridade Europeia para a Proteção de Dados deve abster-se de praticar atos incompatíveis com as suas atribuições e, durante o seu mandato, não pode exercer outras atividades profissionais, remuneradas ou não.

4. Após a cessação do seu mandato, a Autoridade Europeia para a Proteção de Dados deve agir com integridade e discrição relativamente à aceitação de funções e benefícios.

Artigo 56.º

Sigilo profissional

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

Artigo 57.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 pelas instituições e pelos órgãos da União, com exceção do tratamento de dados pessoais pelo Tribunal de Justiça no exercício das suas funções jurisdicionais;

b) Promove a sensibilização do público e a sua compreensão dos riscos, das regras, das garantias e dos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser objeto de especial atenção;

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 aos titulares dos dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades nacionais de controlo para esse efeito;

e) Trata as reclamações apresentadas pelos titulares dos dados ou por organismos, organizações ou associações nos termos do artigo 67.º, investiga, na medida do necessário, o conteúdo das reclamações, e informa os seus autores do andamento e do resultado das investigações num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outras autoridades de controlo;

f) Realiza investigações sobre a aplicação do presente regulamento, nomeadamente com base em informações recebidas de outras autoridades de controlo ou de outras autoridades públicas;

g) Presta aconselhamento, por iniciativa própria ou mediante pedido, a todas as instituições e órgãos da União sobre medidas legislativas e administrativas relacionadas com a proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais;

h) Acompanha factos novos relevantes, na medida em que tenham incidência na proteção dos 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 48.º, n.º 2, alínea c);

j) Estabelece e conserva uma lista relativamente ao requisito de avaliação de impacto relativa à proteção de dados, nos termos do artigo 39.º, n.º 4;

k) Participa nas atividades do Comité Europeu para a Proteção de Dados;

l) Assegura o secretariado do Comité Europeu para a Proteção de Dados, nos termos do artigo 75.º do Regulamento (UE) 2016/679;

m) Presta aconselhamento sobre o tratamento a que se refere o artigo 40.º, n.º 2;

n) Autoriza as cláusulas contratuais e as disposições referidas no artigo 48.º, n.º 3;

o) Conserva registos internos das violações do presente regulamento e das medidas tomadas nos termos do artigo 58.º, n.º 2;

p) Executa outras tarefas relacionadas com a proteção de dados pessoais; e

q) Elabora o seu regulamento interno.

2. A Autoridade Europeia para a Proteção de Dados facilita a apresentação das reclamações previstas no n.º 1, alínea e), disponibilizando um formulário de reclamações que possa ser 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. Caso os pedidos sejam manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter 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 caráter manifestamente infundado ou excessivo dos pedidos.

Artigo 58.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 necessite 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, do responsável pelo tratamento e do subcontratante, acesso a todos os dados pessoais e a todas as informações necessárias ao desempenho das suas funções;

e) Obter acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os seus equipamentos e os seus meios de tratamento de dados, nos termos do direito da União.

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 caso as operações de tratamento tenham violado as disposições do presente regulamento;

c) Submeter questões ao responsável pelo tratamento ou ao subcontratante em causa e, se necessário, ao Parlamento Europeu, ao Conselho e à Comissão;

d) Ordenar que o responsável pelo tratamento ou o subcontratante satisfaçam os pedidos apresentados pelos titulares dos dados para poderem exercer os seus direitos nos termos do presente regulamento;

e) Ordenar que o responsável pelo tratamento ou o subcontratante tomem medidas para que as operações de tratamento cumpram as disposições do presente regulamento, se necessário, de uma forma específica e num prazo específico;

f) Ordenar que o responsável pelo tratamento comunique aos titulares dos dados as violações dos seus dados pessoais;

g) Impor uma limitação temporária ou definitiva ao tratamento, incluindo 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 aos quais os dados pessoais tenham sido divulgados nos termos do artigo 19.º, n.º 2, e do artigo 21.º;

i) Impor coimas nos termos do artigo 66.º em caso de desrespeito, por uma instituição ou por um órgão da União, de qualquer das medidas referidas nas alíneas d) a h) e j) do presente número, em função das circunstâncias de cada caso;

j) Ordenar a suspensão dos fluxos de dados para um destinatário num Estado-Membro ou num país terceiro, ou para uma organização internacional.

3. A Autoridade Europeia para a Proteção de Dados dispõe dos seguintes poderes de autorização e consultivos:

a) Aconselhar os titulares dos dados sobre o exercício dos seus direitos;

b) Aconselhar o responsável pelo tratamento, pelo procedimento de consulta prévia referido no artigo 40.º, e nos termos do artigo 41.º, n.º 2;

c) Emitir, por iniciativa própria ou mediante pedido, pareceres dirigidos às instituições e aos órgãos da União, e ao público, sobre questões relacionadas 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 48.º, n.º 2, alínea c);

e) Autorizar as cláusulas contratuais referidas no artigo 48.º, n.º 3, alínea a);

f) Autorizar os acordos administrativos referidos no artigo 48.º, n.º 3, alínea b);

g) Autorizar operações de tratamento de acordo comos atos de execução adotados nos termos do artigo 40.º, n.º 4.

4. A Autoridade Europeia para a Proteção de Dados dispõe do poder de submeter questões à apreciação do Tribunal de Justiça nas condições previstas nos Tratados e de intervir em processos judiciais intentados junto do Tribunal de Justiça.

5. 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 ações judiciais efetivas e a processos equitativos, previsto no direito da União.

Artigo 59.º

Dever de resposta do responsável pelo tratamento e do subcontratante às alegações

Caso a Autoridade Europeia para a Proteção de Dados exerça os poderes previstos no artigo 58.º, n.º 2, alíneas a), b) e c), o responsável pelo tratamento ou o subcontratante em causa devem comunicar-lhe a sua opinião, num prazo razoável a fixar por aquela autoridade, tendo em conta as circunstâncias de cada caso. A resposta deve incluir igualmente uma descrição das medidas tomadas, caso existam, em resposta às observações da Autoridade Europeia para a Proteção de Dados.

Artigo 60.º

Relatório de atividades

1. A Autoridade Europeia para a Proteção de Dados apresenta um relatório anual de atividades ao Parlamento Europeu, ao Conselho e à Comissão e, simultaneamente, torna-o público.

2. A Autoridade Europeia para a Proteção de Dados transmite o relatório referido no n.º 1 às restantes instituições e órgãos da União, os quais podem apresentar observações tendo em vista um eventual exame do relatório pelo Parlamento Europeu.

CAPÍTULO VII

COOPERAÇÃO E COERÊNCIA

Artigo 61.º

Cooperação entre a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo

A Autoridade Europeia para a Proteção de Dados deve cooperar com as autoridades nacionais de controlo e com a Autoridade Comum de Controlo criada nos termos do artigo 25.º da Decisão 2009/917/JAI do Conselho ([1]), na medida do necessário para o exercício das respetivas funções, em especial partilhando as informações relevantes, solicitando mutuamente o exercício dos poderes respetivos e respondendo aos pedidos que tenham trocado entre si.

Artigo 62.º

Supervisão coordenada da Autoridade Europeia para a Proteção de Dados e das autoridades nacionais de controlo

1. Caso um ato da União faça referência ao presente artigo, a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo, agindo no âmbito das respetivas competências, devem cooperar ativamente no âmbito das suas responsabilidades para assegurar uma supervisão eficaz dos sistemas informáticos de grande escala e dos órgãos e organismos da União.

2. Se necessário, as autoridades em causa, agindo no âmbito das respetivas competências e responsabilidades, devem partilhar as informações relevantes, prestar assistência mútua 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 relacionados com o exercício de uma supervisão independente ou com o exercício dos direitos dos titulares dos dados, elaborar propostas harmonizadas para resolver problemas e promover a sensibilização para os direitos da proteção dos dados.

3. Para os efeitos previstos no n.º 2, a Autoridade Europeia para a Proteção de Dados e as autoridades nacionais de controlo devem reunir-se pelo menos duas vezes por ano no quadro do Comité Europeu para a Proteção de Dados. Para esse efeito, o Comité Europeu para a Proteção de Dados pode definir outros métodos de trabalho, 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 comum relativo às atividades de supervisão coordenada.

([1]) 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, p. 20).

CAPÍTULO VIII

VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

Artigo 63.º

Direito de apresentar reclamações à Autoridade Europeia para a Proteção de Dados

1. Sem prejuízo de outras vias de recurso judicial, administrativo ou extrajudicial, os titulares dos dados têm o direito de apresentar reclamações à Autoridade Europeia para a Proteção de Dados se considerarem 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 autor da reclamação 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 sobre o resultado da reclamação, considera-se que adotou uma decisão negativa.

Artigo 64.º

Direito à ação judicial

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

2. Os recursos contra as decisões da Autoridade Europeia para a Proteção de Dados, incluindo as decisões previstas no artigo 63.º, n.º 3, são interpostos no Tribunal de Justiça.

3. O Tribunal de Justiça tem competência de plena jurisdição para decidir sobre os recursos interpostos contra as coimas referidas no artigo 66.º. O Tribunal de Justiça pode anular, reduzir ou aumentar as referidas coimas dentro dos limites do artigo 66.º.

Artigo 65.º

Direito de indemnização

Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização da instituição ou do órgão da União 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 às instituições e aos órgãos da União, em função das circunstâncias de cada caso, se uma instituição ou um órgão da União não cumprir uma ordem da Autoridade Europeia para a Proteção de Dados nos termos do artigo 58.º, n.º 2, alíneas d) a h) e j). Ao decidir da imposição de uma coima e do montante da mesma, devem ser tidos em conta, em cada caso, 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 em causa, bem como o número de titulares de dados afetados e o nível dos danos sofridos;

b) As medidas tomadas pela instituição ou pelo órgão da União para atenuar os danos sofridos pelos titulares dos dados;

c) O grau de responsabilidade da instituição ou do órgão da União, tendo em conta as medidas técnicas e organizativas que aplicaram por força dos artigos 27.º e 33.º;

d) A existência de violações similares anteriormente cometidas pela instituição ou pelo órgão da União em causa;

e) O grau de cooperação com a Autoridade Europeia para a Proteção de Dados a fim de sanar a violação e de atenuar os seus eventuais efeitos negativos;

f) As categorias de dados pessoais 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 o órgão da União a notificaram e, em caso afirmativo, em que medida o fizeram;

h) O cumprimento das medidas a que se refere o artigo 58.º previamente impostas à instituição ou ao órgão da União em causa relativamente à mesma matéria. O procedimento que leva à imposição de coimas deve ser executado num prazo razoável, em função das circunstâncias de cada caso e tendo em conta as medidas e os procedimentos relevantes referidos no artigo 69.º.

2. Nos termos dos artigos 8.º, 12.º, 27.º a 35.º, 39.º, 40.º, 43.º, 44.º e 45.º, a violação das obrigações pela instituição ou pelo órgão da União deve ser sujeita, nos termos do n.º 1 do presente artigo, a coimas de um montante máximo de 25 000 EUR por infração, e de um montante total de 250 000 EUR por ano.

3. Nos termos do n.º 1, a violação das seguintes disposições pela instituição ou pelo órgão da União deve ser sujeita a coimas de um montante máximo de 50 000 EUR por infração, e de um montante 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 para uma organização internacional, por força dos artigos 46.º a 50.º.

4. Se uma instituição ou um órgão da União violarem, 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 ao abrigo do presente artigo, a Autoridade Europeia para a Proteção de Dados deve conceder à instituição ou ao órgão da União que são alvo do procedimento por si aplicado, a oportunidade de se pronunciarem sobre as objeções que formulou. 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 autores das reclamações 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 das pessoas 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 previstas no presente artigo constituem receitas do orçamento geral da União.

Artigo 67.º

Representação dos titulares dos dados

O titular dos dados tem o direito de mandatar um organismo, uma organização ou uma associação sem fins lucrativos, devidamente constituídos ao abrigo do direito da União ou de um Estado-Membro, cujos objetivos estatutários sejam de interesse público e cuja atividade incida sobre a proteção dos direitos e das 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 nos artigos 63.º e 64.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 de um órgão da União pode apresentar uma reclamação à Autoridade Europeia para a Proteção de Dados relativa a uma alegada violação das disposições do presente regulamento, inclusive sem passar pelas vias oficiais. Ninguém pode ser prejudicado por ter apresentado uma reclamação à Autoridade Europeia para a Proteção de Dados alegando tal violação.

Artigo 69.º

Sanções

O incumprimento, intencional ou negligente, das obrigações estabelecidas no presente regulamento por um funcionário ou por outro agente da União é passível de sanções disciplinares ou de outras sanções, nos termos do Estatuto dos Funcionários.

CAPÍTULO IX

TRATAMENTO DE DADOS PESSOAIS OPERACIONAIS POR ÓRGÃOS E ORGANISMOS DA UNIÃO NO EXERCÍCIO DE ATIVIDADES ABRANGIDAS PELO ÂMBITO DE APLICAÇÃO DA PARTE III, TÍTULO V, CAPÍTULOS 4 OU 5, DO TFUE

Artigo 70.º

Âmbito de aplicação do capítulo

O presente capítulo aplica-se apenas ao tratamento de dados pessoais operacionais por órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, sem prejuízo das regras específicas de proteção de dados aplicáveis a esses órgãos e organismos da União.

Artigo 71.º

Princípios relativos ao tratamento dos dados pessoais operacionais

1. Os dados pessoais operacionais são:

a) Tratados de forma lícita e leal («licitude e lealdade»);

b) Recolhidos para finalidades específicas, explícitas e legítimas, e não tratados de forma incompatível com essas finalidades («limitação das finalidades»);

c) Adequados, pertinentes e não excessivos relativamente às finalidades para as quais são tratados («minimização dos dados»);

d) Exatos e, se necessário, atualizados; devem ser tomadas todas as medidas adequadas para que os dados pessoais operacionais inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora («exatidão»);

e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados («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 acidental, adotando medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).

2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no ato normativo que cria o órgão ou o organismo da União, que sejam diferentes das finalidades para as quais os dados pessoais operacionais foram recolhidos, desde que:

a) O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais operacionais com essa finalidade, nos termos do direito da União; e

b) O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União.

3. O tratamento pelo mesmo ou por outro responsável pelo tratamento pode incluir o arquivo de interesse público e a utilização científica, estatística ou histórica dos dados para as finalidades previstas no ato normativo que cria o órgão ou o organismo da União, sob reserva de garantias adequadas dos direitos e liberdades do titular dos dados.

4. O responsável pelo tratamento é responsável pelo cumprimento dos n.os 1, 2 e 3, e deve poder comprová-lo.

Artigo 72.º

Licitude do tratamento dos dados pessoais operacionais

1. O tratamento de dados pessoais operacionais só é lícito se e na medida em que for necessário para o desempenho de uma função pelos órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, e tiver por base o direito da União.

2. Os atos normativos específicos da União que regulam o tratamento abrangido pelo âmbito do presente capítulo devem especificar, pelo menos, os objetivos do tratamento, os dados pessoais operacionais a tratar, as finalidades do tratamento e os prazos aplicáveis à conservação dos dados pessoais operacionais e à revisão periódica da necessidade de prolongar a conservação dos dados pessoais operacionais.

Artigo 73.º

Distinção entre as diferentes categorias de titulares de dados

O responsável pelo tratamento estabelece, se aplicável e na medida do possível, uma distinção clara entre os dados pessoais das diferentes categorias de titulares de dados, tais como as categorias constantes dos atos normativos que criam os órgãos e os organismos da União.

Artigo 74.º

Distinção entre os dados pessoais operacionais e verificação da sua qualidade

1. O responsável pelo tratamento estabelece, na medida do possível, uma distinção entre os dados pessoais operacionais baseados em factos e os dados pessoais operacionais baseados em apreciações pessoais.

2. O responsável pelo tratamento toma todas as medidas razoáveis para garantir que os dados pessoais operacionais inexatos, incompletos ou desatualizados não sejam transmitidos nem disponibilizados. Para esse efeito, o responsável pelo tratamento verifica, na medida do possível e caso seja pertinente, a qualidade dos dados pessoais operacionais antes de estes serem transmitidos ou disponibilizados, por exemplo, consultando a autoridade competente da qual os dados provêm. Na medida do possível, em todas as transmissões de dados pessoais operacionais, o responsável pelo tratamento fornece as informações necessárias que permitam ao destinatário apreciar até que ponto os dados pessoais operacionais são exatos, completos e fiáveis, e estão atualizados.

3. Caso se verifique que foram transmitidos dados pessoais operacionais inexatos ou que foram transmitidos dados pessoais operacionais de forma ilícita, o destinatário deve ser informado sem demora. Neste caso, os dados pessoais operacionais em causa são retificados ou apagados, ou o seu tratamento é limitado nos termos do artigo 82.º.

Artigo 75.º

Condições específicas do tratamento

1. Quando o direito da União aplicável ao responsável pelo tratamento que transmite os dados estabelece condições específicas de tratamento, o responsável pelo tratamento informa o destinatário dos dados pessoais operacionais dessas condições e da obrigação de as respeitar.

2. O responsável pelo tratamento respeita as condições específicas de tratamento previstas pela autoridade competente que transmite os dados, nos termos do artigo 9.º, n.os 3 e 4, da Diretiva (UE) 2016/680.

Artigo 76.º

Tratamento de categorias especiais de dados pessoais operacionais

1. O tratamento de dados pessoais operacionais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, e o tratamento de dados genéticos, de dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, de dados pessoais operacionais relativos à saúde ou relativos à vida sexual ou à orientação sexual de uma pessoa só são autorizados se forem estritamente necessários para fins operacionais, no âmbito do mandato do órgão ou do organismo da União em causa, e se estiverem sujeitos a garantias adequadas dos direitos e das liberdades do titular dos dados. É proibida a discriminação de pessoas singulares com base nesses dados pessoais.

2. O encarregado da proteção de dados deve ser informado sem demora indevida da aplicação do presente artigo.

Artigo 77.º

Decisões individuais automatizadas, incluindo a definição de perfis

1. São proibidas as decisões baseadas exclusivamente no tratamento automatizado de dados, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, salvo se forem autorizadas pelo direito da União ao qual o responsável pelo tratamento está sujeito e desde que esse direito preveja garantias adequadas dos direitos e das liberdades do titular dos dados, pelo menos o direito de obter a intervenção humana do responsável pelo tratamento.

2. As decisões a que se refere o n.º 1 do presente artigo não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 76.º, salvo se forem aplicadas medidas adequadas para salvaguardar os direitos, as liberdades e os legítimos interesses do titular dos dados.

3. Em conformidade com o direito da União, são proibidas as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais a que se refere o artigo 76.º.

Artigo 78.º

Comunicação e regras de exercício dos direitos dos titulares dos dados

1. O responsável pelo tratamento toma todas as medidas razoáveis para fornecer ao titular dos dados as informações a que se refere o artigo 79.º e efetua as comunicações relativas aos artigos 80.º a 84.º e 92.º a respeito do tratamento de uma forma concisa, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. As informações são fornecidas pelos meios adequados, inclusive eletrónicos. Em regra geral, o responsável pelo tratamento fornece as informações na mesma forma que o pedido.

2. O responsável pelo tratamento facilita o exercício dos direitos do titular dos dados, nos termos dos artigos 79.º a 84.º.

3. O responsável pelo tratamento informa o titular dos dados por escrito sobre a resposta dada ao seu pedido sem demora indevida e, em qualquer caso, no prazo máximo de três meses após a receção do pedido do titular dos dados.

4. O responsável pelo tratamento fornece as informações previstas nos termos do artigo 79.º, e informações sobre as comunicações efetuadas ou sobre as medidas tomadas ao abrigo dos artigos 80.º a 84.º e 92.º, gratuitamente. Caso os pedidos apresentados por um titular de dados sejam manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter recorrente, o responsável pelo tratamento pode recusar dar-lhes seguimento. Cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

5. Se o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta um pedido referido nos artigos 80.º ou 82.º, pode solicitar que lhe sejam fornecidas informações adicionais necessárias para confirmar a identidade do titular dos dados.

Artigo 79.º

Informações a facultar ou a prestar ao titular dos dados

1. O responsável pelo tratamento faculta ao titular dos dados, pelo menos, as seguintes informações:

a) A identidade e os contactos do órgão ou organismo da União;

b) Os contactos do encarregado da proteção de dados;

c) As finalidades do tratamento a que os dados pessoais operacionais se destinam;

d) O direito de apresentar reclamações à Autoridade Europeia para a Proteção de Dados, e os contactos da Autoridade;

e) O direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais operacionais que lhe digam respeito, bem como a retificação ou o apagamento dos dados e a limitação do seu tratamento.

2. Para além das informações a que se refere o n.º 1, o responsável pelo tratamento presta ao titular dos dados, nos casos específicos previstos no direito da União, as seguintes informações adicionais a fim de lhe permitir exercer os seus direitos:

a) O fundamento jurídico do tratamento;

b) O prazo de conservação dos dados pessoais operacionais ou, se tal não for possível, os critérios usados para estabelecer esse prazo;

c) Se aplicável, as categorias de destinatários dos dados pessoais operacionais; inclusive nos países terceiros ou nas organizações internacionais;

d) Se for caso disso, informações adicionais, especialmente se os dados pessoais operacionais forem recolhidos sem conhecimento do seu titular.

3. O responsável pelos dados pode adiar, limitar ou omitir a prestação das informações a que se refere o n.º 2 aos titulares dos dados se e enquanto essas medidas constituírem medidas necessárias e proporcionadas numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos das pessoas singulares em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;

b) Evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais, ou a execução de sanções penais;

c) Proteger a segurança pública dos Estados-Membros;

d) Proteger a segurança nacional dos Estados-Membros;

e) Proteger os direitos e as liberdades de terceiros, nomeadamente as vítimas e as testemunhas.

Artigo 80.º

Direito de acesso do titular dos dados

O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais operacionais que lhe digam respeito estão ou não a ser tratados e, em caso afirmativo, tem o direito de aceder aos dados pessoais operacionais e às seguintes informações:

a) As finalidades e o fundamento jurídico do tratamento;

b) As categorias de dados pessoais operacionais em questão;

c) Os destinatários ou as categorias de destinatários aos quais os dados pessoais operacionais foram divulgados, especialmente se se tratar de destinatários de países terceiros ou de organizações internacionais;

d) Se possível, o prazo previsto de conservação dos dados pessoais operacionais ou, se não for possível, os critérios usados para fixar esse prazo;

e) O direito de solicitar ao responsável pelo tratamento a retificação ou o apagamento dos dados pessoais operacionais ou a limitação do tratamento dos dados pessoais operacionais que lhe digam respeito;

f) O direito de apresentar reclamações à Autoridade Europeia para a Proteção de Dados, e os contactos da Autoridade;

g) A comunicação dos dados pessoais operacionais sujeitos a tratamento e das informações disponíveis sobre a origem dos dados.

Artigo 81.º

Limitações do direito de acesso

1. O responsável pelo tratamento pode limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto essa limitação, total ou parcial, constituir uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;

b) Evitar prejudicar a prevenção, a deteção, a investigação ou a repressão de infrações penais, ou a execução de sanções penais;

c) Proteger a segurança pública dos Estados-Membros;

d) Proteger a segurança nacional dos Estados-Membros;

e) Proteger os direitos e as liberdades de terceiros, nomeadamente as vítimas e as testemunhas.

2. Nos casos a que se refere o n.º 1, o responsável pelo tratamento informa por escrito o titular dos dados, sem demora indevida, de todos os casos de recusa ou limitação de acesso, e dos motivos da recusa ou da limitação. Essa informação pode ser omitida, caso a sua prestação possa prejudicar uma das finalidades enunciadas no n.º 1. O responsável pelo tratamento informa o titular dos dados da possibilidade de apresentar reclamações à Autoridade Europeia para a Proteção de Dados ou de intentar uma ação judicial junto do Tribunal de Justiça. O responsável pelo tratamento documenta os motivos de facto ou de direito em que a sua decisão se baseou. Essa informação deve ser facultada à Autoridade Europeia para a Proteção de Dados, a pedido desta.

Artigo 82.º

Direito de retificação ou apagamento dos dados pessoais operacionais e limitação do tratamento

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

2. O responsável pelo tratamento apaga os dados pessoais operacionais sem demora indevida, e o titular dos dados tem o direito de obter do responsável pelo tratamento o apagamento, sem demora indevida, dos dados pessoais operacionais que lhe digam respeito caso o tratamento viole o artigo 71.º, o artigo 72.º, n.º 1, ou o artigo 76.º, ou caso os dados pessoais operacionais devam ser apagados em cumprimento de uma obrigação legal a que o responsável pelo tratamento esteja sujeito.

3. Em vez de proceder ao apagamento, o responsável pelo tratamento limita o tratamento dos dados caso:

a) O titular dos dados conteste a exatidão dos dados pessoais, e a sua exatidão ou inexatidão não possa ser apurada; ou

b) Os dados pessoais tenham de ser conservados para efeitos de prova.

Caso o tratamento seja limitado nos termos do primeiro parágrafo, alínea a), o responsável pelo tratamento informa o titular dos dados antes de levantar a limitação do tratamento dos dados.

Os dados limitados só podem ser tratados para as finalidades que impediram o seu apagamento.

4. O responsável pelo tratamento informa por escrito o titular dos dados da recusa de retificação ou de apagamento de dados pessoais operacionais, ou da limitação do seu tratamento, e dos motivos da recusa. O responsável pelo tratamento pode limitar, total ou parcialmente, o fornecimento dessas informações, na medida em que tal limitação constitua uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os direitos fundamentais e os interesses legítimos da pessoa singular em causa, a fim de:

a) Evitar prejudicar os inquéritos, as investigações ou os procedimentos oficiais ou judiciais;

b) Evitar prejudicar a prevenção, a investigação, a deteção ou a repressão de infrações penais, ou a execução de sanções penais;

c) Proteger a segurança pública dos Estados-Membros;

d) Proteger a segurança nacional dos Estados-Membros;

e) Proteger os direitos e as liberdades de terceiros, nomeadamente as vítimas e as testemunhas.

O responsável pelo tratamento informa o titular dos dados da possibilidade de apresentar reclamações à Autoridade Europeia para a Proteção de Dados e de intentar uma ação judicial junto do Tribunal de Justiça.

5. O responsável pelo tratamento comunica a retificação dos dados pessoais operacionais inexatos à autoridade competente da qual provieram os dados pessoais operacionais inexatos.

6. Quando os dados pessoais operacionais tenham sido retificados ou apagados, ou o seu tratamento tenha sido limitado nos termos dos n.ºs 1, 2 ou 3, o responsável pelo tratamento notifica os destinatários e informa-os de que devem retificar ou apagar os dados pessoais operacionais, ou limitar o tratamento dos dados pessoais operacionais sob a sua responsabilidade.

Artigo 83.º

Direito de acesso no âmbito de investigações e ações penais

Caso os dados pessoais operacionais provenham de uma autoridade competente, os órgãos e os organismos da União, antes de adotarem uma decisão sobre o direito de acesso do titular de dados, devem verificar junto da autoridade competente em causa se esses dados pessoais constam de uma decisão judicial ou de um registo criminal, ou de um processo tratado no âmbito de uma investigação ou de uma ação penal no Estado-Membro dessa autoridade competente. Se for esse o caso, deve ser tomada uma decisão relativa ao direito de acesso, em consulta e em estreita cooperação com a autoridade competente em causa.

Artigo 84.º

Exercício dos direitos do titular dos dados e verificação da Autoridade Europeia para a Proteção de Dados

1. Nos casos referidos no artigo 79.º, n.º 3, no artigo 81.º e no artigo 82.º, n.º 4, os direitos do titular dos dados podem igualmente ser exercidos através da Autoridade Europeia para a Proteção de Dados.

2. O responsável pelo tratamento informa o titular dos dados da possibilidade de exercer os seus direitos através da Autoridade Europeia para a Proteção de Dados, nos termos do n.º 1.

3. Caso o direito referido no n.º 1 seja exercido, a Autoridade Europeia para a Proteção de Dados informa, pelo menos, o titular dos dados de que procedeu a todas as verificações necessárias, ou a uma revisão. A Autoridade Europeia para a Proteção de Dados informa também o titular dos dados sobre o seu direito de intentar uma ação judicial junto do Tribunal de Justiça.

Artigo 85.º

Proteção de dados desde a conceção e por defeito

1. Tendo em conta as técnicas mais avançadas, os custos de execução e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variáveis, para os direitos e as liberdades das pessoas singulares suscitados pelo tratamento, o responsável pelo tratamento deve aplicar, tanto no momento da definição dos meios de tratamento como durante o próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a pôr efetivamente em prática os princípios da proteção de dados, como a minimização, a fim de integrar as garantias necessárias no tratamento, de modo a cumprir os requisitos previstos no presente regulamento e no ato normativo que o cria, e a proteger os direitos dos titulares dos dados.

2. O responsável pelo tratamento aplica as medidas técnicas e organizativas adequadas para garantir que, por defeito, só sejam tratados os dados pessoais operacionais que sejam adequados, pertinentes e não excessivos em relação à finalidade do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais operacionais 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 operacionais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

Artigo 86.º

Responsáveis conjuntos pelo tratamento

1. Caso dois ou mais responsáveis pelo tratamento ou um ou mais responsáveis pelo tratamento, juntamente com um ou mais responsáveis pelo tratamento que não sejam instituições ou órgãos da União, determinem conjuntamente as finalidades e os meios do tratamento, são considerados responsáveis conjuntos pelo tratamento. Os responsáveis conjuntos pelo tratamento determinam, por acordo entre si e de modo transparente, as respetivas responsabilidades pelo cumprimento das suas obrigações em matéria de proteção de dados, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de prestar as informações referidas no artigo 79.º, a não ser e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou pelo direito do Estado-Membro a que estão sujeitos. No referido acordo, pode ser designado 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 as relações respetivas dos responsáveis conjuntos pelo tratamento em relação ao titular dos dados. O teor do acordo deve ser disponibilizado ao titular dos dados.

3. Independentemente dos termos do acordo a que se refere o n.º 1, o titular dos dados pode exercer os direitos que o presente regulamento lhe confere em relação e contra cada um dos responsáveis pelo tratamento.

Artigo 87.º

Subcontratantes

1. Caso o tratamento dos dados seja 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 tal forma que o tratamento satisfaça os requisitos previstos no presente regulamento e no ato normativo que cria o responsável pelo tratamento, e assegure a defesa dos direitos do titular dos dados.

2. O subcontratante não pode contratar outro subcontratante sem a autorização escrita prévia, específica ou geral, do responsável pelo tratamento. Em caso de autorização geral por escrito, o subcontratante deve informar o responsável pelo tratamento das 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 essas alterações.

3. O tratamento em subcontratação é regulado por contrato, ou por outro ato normativo ao abrigo do direito da União ou de um Estado-Membro, que vincula o subcontratante ao responsável pelo tratamento, estabelece o objeto e a duração do tratamento, a sua natureza e a sua finalidade, o tipo de dados pessoais operacionais e as categorias dos titulares dos dados, e as obrigações e os direitos do responsável pelo tratamento. Esse contrato, ou o outro ato normativo, deve estipular, em especial, que o subcontratante:

a) Só age de acordo com instruções do responsável pelo tratamento;

b) Assegura que as pessoas autorizadas a tratar os dados pessoais operacionais assumiram um compromisso de confidencialidade ou estão sujeitas às obrigações legais de confidencialidade adequadas;

c) Presta assistência ao responsável pelo tratamento por todos os meios adequados, de modo a assegurar o cumprimento das disposições relativas aos direitos do titular dos dados;

d) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais operacionais depois de concluída a prestação dos serviços relacionados com o tratamento, e apaga as cópias existentes, a não ser que a conservação dos dados pessoais operacionais seja exigida ao abrigo do direito da União ou de um Estado-Membro;

e) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo;

f) Respeita as condições referidas no n.º 2 no presente número na contratação de outro subcontratante.

4. O contrato ou o outro ato normativo a que se refere o n.º 3 é feito por escrito, inclusive em formato eletrónico.

5. Se, em violação do presente regulamento ou do ato normativo que cria o responsável pelo tratamento, o subcontratante determinar as finalidades e os meios do tratamento, é considerado responsável pelo tratamento em relação ao tratamento em causa.

Artigo 88.º

Registo cronológico

1. O responsável pelo tratamento conserva registos cronológicos de todas as seguintes operações de tratamento em sistemas automatizados de tratamento: recolha, alteração, consulta, divulgação — incluindo transferências –, interconexão e apagamento de dados pessoais operacionais. Os registos cronológicos das operações de consulta e divulgação permitem determinar o motivo, a data e a hora dessas operações, a identificação da pessoa que consultou ou divulgou os dados pessoais operacionais e, na medida do possível, a identidade dos destinatários desses dados pessoais operacionais.

2. Os registos cronológicos são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, de autocontrolo e de garantia da integridade e segurança dos dados pessoais operacionais, e para ações penais. Os registos cronológicos são apagados ao fim de três anos, salvo se forem necessários para controlos em curso.

3. O responsável pelo tratamento disponibiliza, a pedido, os registos cronológicos ao seu encarregado da proteção de dados e à Autoridade Europeia para a Proteção de Dados.

Artigo 89.º

Avaliação de impacto relativa à proteção de dados

1. Caso um tipo de tratamento, em particular que utilize novas tecnologias, tendo em conta a natureza, o âmbito, o contexto e as finalidades desse tratamento, seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares, o responsável pelo tratamento deve proceder, antes de iniciar o tratamento, uma avaliação do impacto das operações de tratamento previstas sobre a proteção dos dados pessoais operacionais.

2. A avaliação a que se refere o n.º 1 inclui pelo menos uma descrição geral das operações de tratamento previstas, uma avaliação dos riscos para os direitos e as liberdades dos titulares dos dados, as medidas previstas para fazer face a esses riscos, as garantias, as medidas de segurança e os mecanismos para assegurar a proteção dos dados pessoais operacionais e para demonstrar a conformidade com as regras de proteção de dados, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas afetadas.

Artigo 90.º

Consulta prévia da Autoridade Europeia para a Proteção de Dados

1. O responsável pelo tratamento consulta a Autoridade Europeia para a Proteção de Dados antes de proceder a um tratamento que fará parte de um novo sistema de ficheiro a criar, caso:

a) A avaliação de impacto relativa à proteção de dados ao abrigo do artigo 89.º indique que o tratamento constituiria um elevado risco na falta de medidas tomadas pelo responsável pelo tratamento para atenuar o risco; ou

b) O tipo de tratamento implique, especialmente no caso de se utilizarem novas tecnologias, novos mecanismos ou novos procedimentos, um elevado risco para os direitos e as liberdades dos titulares dos dados.

2. A Autoridade Europeia para a Proteção de Dados elabora uma lista das operações de tratamento sujeitas a consulta prévia nos termos do n.º 1.

3. O responsável pelo tratamento fornece à Autoridade Europeia para a Proteção de Dados a avaliação de impacto relativa à proteção de dados a que se refere o artigo 89.º e, quando lhe for solicitado, outras informações que permitam à Autoridade Europeia para a Proteção de Dados avaliar a conformidade do tratamento e, nomeadamente, os riscos para a proteção dos dados pessoais operacionais do titular dos dados e as respetivas garantias.

4. Caso a Autoridade Europeia para a Proteção de Dados considere que o tratamento previsto referido no n.º 1 violaria o presente regulamento ou o ato normativo que cria o órgão ou o organismo da União, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, deve emitir orientações por escrito, no prazo máximo de seis semanas a contar da receção do pedido de consulta, destinadas ao responsável pelo tratamento. Esse prazo pode ser prorrogado por um mês, tendo em conta a complexidade do tratamento previsto. A Autoridade Europeia para a Proteção de Dados informa o responsável pelo tratamento da prorrogação no prazo de um mês a contar da data de receção do pedido de consulta, e indica os motivos do atraso.

Artigo 91.º

Segurança do tratamento dos dados pessoais operacionais

1. O responsável pelo tratamento e o subcontratante, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos, de probabilidade e gravidade variáveis, para os direitos e as liberdades das pessoas singulares, aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, em especial no que respeita ao tratamento das categorias especiais de dados pessoais operacionais.

2. No que diz respeito ao tratamento automatizado de dados, o responsável pelo tratamento e o subcontratante, na sequência de uma avaliação dos riscos, aplicam medidas para os seguintes efeitos:

a) Impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento de dados (controlo de acesso ao equipamento);

b) Impedir que os suportes de dados possam ser lidos, copiados, alterados ou retirados sem autorização (controlo dos suportes de dados);

c) Impedir a introdução não autorizada de dados pessoais operacionais e a inspeção, alteração ou apagamento não autorizados de dados pessoais operacionais conservados (controlo de conservação);

d) Impedir que os sistemas de tratamento automatizado de dados sejam utilizados por pessoas não autorizadas por meio de equipamentos de comunicação de dados (controlo dos utilizadores);

e) Assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado de dados só tenham acesso aos dados pessoais operacionais abrangidos pela sua autorização de acesso (controlo do acesso aos dados);

f) Assegurar que possa ser verificado e determinado a que organismos os dados pessoais operacionais foram ou podem ser transmitidos ou facultados recorrendo à comunicação de dados (controlo da comunicação);

g) Assegurar que possa ser verificado e determinado *a posteriori* quais os dados pessoais operacionais introduzidos nos sistemas de tratamento automatizado de dados, e quando e por quem foram introduzidos (controlo da introdução);

h) Impedir que os dados pessoais operacionais possam ser lidos, copiados, alterados ou suprimidos sem autorização durante a sua transmissão e durante o transporte de suportes de dados (controlo do transporte dos dados);

i) Assegurar que os sistemas utilizados possam ser restaurados em caso de interrupção (recuperação);

j) Assegurar que as funções do sistema funcionem, que os erros de funcionamento sejam assinalados (fiabilidade) e que os dados pessoais operacionais conservados não possam ser falseados por um disfuncionamento do sistema (integridade).

Artigo 92.º

Notificação de violações 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 indevida e, se possível, no prazo máximo de 72 horas após ter tido conhecimento da mesma, salvo se tal violação não for suscetível de constituir um risco para os direitos e as liberdades das pessoas singulares. Se não for transmitida no prazo de 72 horas, a notificação à Autoridade Europeia para a Proteção de Dados deve ser acompanhada dos motivos do atraso.

2. A notificação referida no n.º 1 deve, pelo menos:

a) Descrever a natureza da violação de dados pessoais, incluindo, se possível e adequado, as categorias e o número aproximado de titulares dos dados afetados, bem como as categorias e o número aproximado dos registos de dados pessoais operacionais em causa;

b) Comunicar o nome e os contactos do encarregado da proteção de dados;

c) Descrever as consequências prováveis da violação de dados pessoais;

d) Descrever as medidas tomadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.

3. Caso e na medida em que não seja possível comunicar todas as informações referidas no n.º 2 ao mesmo tempo, as informações podem ser comunicadas por fases, sem demora indevida.

4. O responsável pelo tratamento documenta todas as violações de dados pessoais referidas no n.º 1, incluindo os factos relacionados com a violação, os seus efeitos e as medidas de reparação adotadas. Essa documentação deve permitir à Autoridade Europeia para a Proteção de Dados verificar o respeito do presente artigo.

5. Caso a violação de dados pessoais envolva dados pessoais operacionais transmitidos pelas autoridades competentes ou a elas destinados, o responsável pelo tratamento comunica as informações referidas no n.º 2 às autoridades competentes em causa sem demora indevida.

Artigo 93.º

Comunicação de violações de dados pessoais ao titular dos dados

1. Caso uma violação de dados pessoais seja suscetível de constituir um elevado risco para os direitos e as liberdades das pessoas singulares, o responsável pelo tratamento deve comunicar a violação ao titular dos dados sem demora indevida.

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 de dados pessoais e incluir, pelo menos, as informações e as recomendações previstas no artigo 92.º, n.º 2, alíneas b), c) e d).

3. A comunicação ao titular dos dados a que se refere o n.º 1 não é exigida caso uma das seguintes condições esteja satisfeita:

a) O responsável pelo tratamento aplicou medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas foram aplicadas aos dados pessoais operacionais afetados pela violação de dados pessoais, especialmente medidas que tornam os dados pessoais operacionais incompreensíveis para as pessoas não autorizadas a aceder a esses dados, como, por exemplo, a cifragem;

b) O responsável pelo tratamento tomou medidas subsequentes que asseguram que o elevado risco para os direitos e as liberdades dos titulares a que se refere o n.º 1 já não é suscetível de se concretizar;

c) A comunicação implicaria 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 ainda não tiver 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 constituir um elevado risco, pode exigir-lhe que proceda a essa notificação, ou pode constatar que uma das condições referidas no n.º 3 está preenchida.

5. A comunicação ao titular dos dados referida no n.º 1 do presente artigo pode ser adiada, limitada ou omitida, sob reserva das condições e pelos motivos a que se refere o artigo 79.º, n.º 3.

Artigo 94.º

Transferências de dados pessoais operacionais para países terceiros ou para organizações internacionais

1. Sob reserva das limitações e das condições estabelecidas nos atos normativos que criam o órgão ou o organismo da União, o responsável pelo tratamento pode transferir dados pessoais operacionais para uma autoridade de um país terceiro ou para uma organização internacional, na medida em que essa transmissão seja necessária para o exercício das suas funções, e apenas nos casos em que as condições previstas no presente artigo sejam respeitadas, a saber:

a) A Comissão adotou uma decisão de adequação nos termos do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, que estabelece que o país terceiro ou um território ou um setor de tratamento nesse país terceiro, ou a organização internacional em causa, asseguram um nível de proteção adequado;

b) Na falta de uma decisão de adequação da Comissão nos termos da alínea a), foi celebrado um acordo internacional entre a União e esse país terceiro ou essa organização internacional, nos termos do artigo 218.º do TFUE, estabelecendo garantias suficientes respeitantes à proteção da privacidade e dos direitos e liberdades fundamentais das pessoas;

c) Na falta de uma decisão de adequação da Comissão nos termos da alínea a) ou de um acordo internacional nos termos da alínea b), foi celebrado um acordo de cooperação entre o órgão ou organismo da União e o país terceiro em causa que permite o intercâmbio de dados pessoais operacionais, antes da data de aplicação do ato normativo que cria esse órgão ou organismo da União.

2. Os atos normativos que criam os órgãos e os organismos da União podem manter ou introduzir disposições mais específicas sobre as condições aplicáveis às transferências internacionais de dados pessoais operacionais, em especial sobre as transferências com garantias adequadas e derrogações aplicáveis a situações específicas.

3. O responsável pelo tratamento publica no seu sítio Web, e mantém atualizada, uma lista das decisões de adequação referidas no n.º 1, alínea a), dos acordos, dos convénios administrativos e de outros instrumentos relacionados com a transferência de dados pessoais operacionais nos termos do n.º 1.

4. O responsável pelo tratamento conserva registos pormenorizados de todas as transferências realizadas ao abrigo do presente artigo.

Artigo 95.º

Confidencialidade dos inquéritos judiciais e das ações penais

Os atos normativos que criam os órgãos e os organismos da União que exercem atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE podem obrigar a Autoridade Europeia para a Proteção de Dados a ter na melhor conta a confidencialidade dos inquéritos judiciais e das ações penais no exercício dos seus poderes de supervisão, nos termos do direito da União ou do direito dos Estados-Membros.

CAPÍTULO X

ATOS DE EXECUÇÃO

Artigo 96.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 XI

REEXAME

Artigo 97.º

Cláusula de reexame

O mais tardar em 30 de abril de 2022 e, em seguida, de cinco em cinco anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a aplicação do presente regulamento, acompanhado, se necessário, de propostas legislativas adequadas.

Artigo 98.º

Reexame dos atos normativos da União

1. Até 30 de abril de 2022, a Comissão deve efetuar um reexame dos atos normativos adotados com base nos Tratados que regulam o tratamento dos dados pessoais operacionais pelos órgãos e organismos da União no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, a fim de:

a) Avaliar a sua coerência com a Diretiva (UE) 2016/680 e com o capítulo IX do presente regulamento;

b) Identificar divergências suscetíveis de criar obstáculos ao intercâmbio de dados pessoais operacionais entre os órgãos e os organismos da União quando exercem atividades nesses domínios e as autoridades competentes; e

c) Identificar divergências suscetíveis de gerar a fragmentação jurídica da legislação sobre a proteção de dados na União.

2. Com base nesse reexame, a fim de assegurar uma proteção uniforme e coerente das pessoas singulares no que diz respeito ao tratamento, a Comissão pode apresentar propostas legislativas adequadas, nomeadamente na perspetiva da aplicação do capítulo IX do presente regulamento, à Europol e à Procuradoria Europeia, que incluam, se necessário, adaptações do capítulo IX do presente regulamento.

CAPÍTULO XII

DISPOSIÇÕES FINAIS

Artigo 99.º

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

O Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE são revogados com efeitos a partir de 11 de dezembro de 2018. As remissões para o regulamento e para a decisão revogados devem entender-se como sendo feitas para o presente regulamento.

Artigo 100.º

Medidas transitórias

1. O presente regulamento não obsta à aplicação da Decisão 2014/886/UE do Parlamento Europeu e do Conselho [1] nem aos mandatos atuais da Autoridade Europeia para a Proteção de Dados e da Autoridade Adjunta.

[1] 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).

2. A Autoridade Adjunta é considerada equiparada ao Secretário do Tribunal de Justiça no que se refere à determinação da remuneração, subsídios, pensão de reforma e outros benefícios equivalentes à remuneração que lhe sejam devidos.

3. O artigo 53.º, n.os 4, 5 e 7, e os artigos 55.º e 56.º do presente regulamento, são aplicáveis à atual Autoridade Adjunta até ao termo do seu mandato.

4. A Autoridade Adjunta assiste a Autoridade Europeia para a Proteção de Dados no desempenho das suas funções, e substitui-a em caso de ausência ou de impedimento, até ao termo do atual mandato da Autoridade Adjunta.

Artigo 101.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. No entanto, o presente regulamento é aplicável ao tratamento de dados pessoais pela Eurojust a partir de 12 de dezembro de 2019.

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

Feito em Estrasburgo, 23 de outubro de 2018.

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*A Presidente*
A. TAJANI	K. EDTSTADLER