

# Jornal Oficial

## da União Europeia

L 119



Edição em língua  
portuguesa

Legislação

59.º ano

4 de maio de 2016

Índice

### I Atos legislativos

#### REGULAMENTOS

- ★ 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) <sup>(1)</sup> ..... 1

#### DIRETIVAS

- ★ 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 ..... 89
- ★ Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave ..... 132

<sup>(1)</sup> Texto relevante para efeitos do EEE

PT

Os atos cujos títulos são impressos em tipo fino são atos de gestão corrente adotados no âmbito da política agrícola e que têm, em geral, um período de validade limitado.

Os atos cujos títulos são impressos em tipo negro e precedidos de um asterisco são todos os restantes.



## I

*(Atos legislativos)*

## REGULAMENTOS

## REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO

de 27 de abril de 2016

**relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**

*(Texto relevante para efeitos do EEE)*

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,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu <sup>(1)</sup>,

Tendo em conta o parecer do Comité das Regiões <sup>(2)</sup>,

Deliberando de acordo com o processo legislativo ordinário <sup>(3)</sup>,

Considerando o seguinte:

- (1) A proteção das pessoas singulares relativamente 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.
- (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.
- (3) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho <sup>(4)</sup> visa harmonizar a defesa dos direitos e das liberdades fundamentais das pessoas singulares em relação às atividades de tratamento de dados e assegurar a livre circulação de dados pessoais entre os Estados-Membros.

<sup>(1)</sup> JO C 229 de 31.7.2012, p. 90.

<sup>(2)</sup> JO C 391 de 18.12.2012, p. 127.

<sup>(3)</sup> Posição do Parlamento Europeu de 12 de março de 2014 (ainda não publicada no Jornal Oficial) e posição do Conselho em primeira leitura de 8 de abril de 2016 (ainda não publicada no Jornal Oficial). Posição do Parlamento Europeu de 14 de abril de 2016.

<sup>(4)</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

- (4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística.
- (5) A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços de dados pessoais. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas singulares, as associações e as empresas, intensificou-se na União Europeia. As autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro.
- (6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.
- (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores económicos e as autoridades públicas.
- (8) Caso o presente regulamento preveja especificações ou restrições das suas regras pelo direito de um Estado-Membro, estes podem incorporar elementos do presente regulamento no respetivo direito nacional, na medida do necessário para manter a coerência e tornar as disposições nacionais compreensíveis para as pessoas a quem se aplicam.
- (9) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.
- (10) A fim de assegurar um nível de proteção coerente e elevado das pessoas singulares e eliminar os obstáculos à circulação de dados pessoais na União, o nível de proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogênea das regras de defesa dos direitos e das liberdades fundamentais das pessoas singulares no que diz respeito ao tratamento de dados pessoais. No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento. Em conjugação com a legislação geral e horizontal sobre proteção de dados que dá aplicação à Diretiva 95/46/CE, os Estados-Membros dispõem de várias leis setoriais em domínios que necessitam de disposições mais específicas. O presente regulamento também dá aos Estados-Membros margem de manobra para especificarem as suas regras, inclusive em matéria de tratamento de categorias especiais de dados pessoais («dados sensíveis»). Nessa medida, o presente regulamento não exclui o direito dos Estados-Membros que define as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

- (11) A proteção eficaz dos dados pessoais na União exige o reforço e a especificação dos direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, bem como poderes equivalentes para controlar e assegurar a conformidade das regras de proteção dos dados pessoais e sanções equivalentes para as infrações nos Estados-Membros.
- (12) O artigo 16.º, n.º 2, do TFUE incumbe o Parlamento Europeu e o Conselho de estabelecerem as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como as normas relativas à livre circulação desses dados.
- (13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros. O bom funcionamento do mercado interno impõe que a livre circulação de dados pessoais na União não pode ser restringida ou proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais. Para ter em conta a situação particular das micro, pequenas e médias empresas, o presente regulamento prevê uma derrogação para as organizações com menos de 250 trabalhadores relativamente à conservação do registo de atividades. Além disso, as instituições e os órgãos da União, e os Estados-Membros e as suas autoridades de controlo, são incentivados a tomar em consideração as necessidades específicas das micro, pequenas e médias empresas no âmbito de aplicação do presente regulamento. A noção de micro, pequenas e médias empresaster em conta deverá inspirar-se do artigo 2.º do anexo da Recomendação 2003/361/CE da Comissão <sup>(1)</sup>.
- (14) A proteção conferida pelo presente regulamento deverá aplicar-se às pessoas singulares, independentemente da sua nacionalidade ou do seu local de residência, relativamente ao tratamento dos seus dados pessoais. O presente regulamento não abrange o tratamento de dados pessoais relativos a pessoas coletivas, em especial a empresas estabelecidas enquanto pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva.
- (15) A fim de se evitar o sério risco sério de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados pessoais estiverem contidos ou se forem destinados a um sistema de ficheiros. Os ficheiros ou 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.
- (16) O presente regulamento não se aplica às questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados pessoais relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional. O presente regulamento não se aplica ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União.
- (17) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho <sup>(2)</sup> é aplicável ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, deverão ser adaptados aos princípios e regras estabelecidos pelo presente regulamento e aplicados à luz do mesmo. A fim de proporcionar um quadro de proteção de dados sólido e coerente na União, e após a adoção do presente regulamento, deverão ser realizadas as necessárias adaptações do Regulamento (CE) n.º 45/2001, a fim de permitir a aplicação em simultâneo com o presente regulamento.
- (18) O presente regulamento não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas e, portanto, sem qualquer ligação com uma

<sup>(1)</sup> Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

<sup>(2)</sup> Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho, de 18 de dezembro de 2000, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos comunitários e à livre circulação desses dados (JO L 8 de 12.1.2001, p. 1).

atividade profissional ou comercial. As atividades pessoais ou domésticas poderão incluir a troca de correspondência e a conservação de listas de endereços ou a atividade das redes sociais e do ambiente eletrónico no âmbito dessas atividades. Todavia, o presente regulamento é aplicável aos responsáveis pelo tratamento e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

- (19) A proteção das pessoas singulares em matéria de tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, e de livre circulação desses dados, é objeto de um ato jurídico da União específico. O presente regulamento não deverá, por isso, ser aplicável às atividades de tratamento para esses efeitos. Todavia, os dados pessoais tratados pelas autoridades competentes ao abrigo do presente regulamento deverão ser regulados, quando forem usados para os efeitos referidos, por um ato jurídico da União mais específico, a saber, a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho <sup>(1)</sup>. Os Estados-Membros podem confiar às autoridades competentes na aceção da Diretiva (UE) 2016/680 funções não necessariamente a executar para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, de modo a que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do presente regulamento.

No que respeita ao tratamento de dados pessoais pelas referidas autoridades competentes para efeitos que sejam abrangidos pelo presente regulamento, os Estados-Membros deverão poder manter ou aprovar disposições mais específicas para adaptar a aplicação das regras previstas no presente regulamento. Tais disposições podem estabelecer requisitos mais específicos e precisos a respeitar pelas referidas autoridades competentes no tratamento dos dados pessoais para esses outros efeitos, tendo em conta as estruturas constitucionais, organizativas e administrativas do respetivo Estado-Membro. Nos casos em que o tratamento de dados pessoais por organismos privados fica abrangido pelo presente regulamento, este deverá prever a possibilidade de os Estados-Membros restringirem legalmente, em determinadas condições, certas obrigações e direitos, quando tal restrição constitua medida necessária e proporcionada, numa sociedade democrática, para salvaguardar interesses específicos importantes, incluindo a segurança pública e a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. Tal possibilidade é importante, por exemplo, no quadro da luta contra o branqueamento de capitais ou das atividades dos laboratórios de polícia científica.

- (20) Na medida em que o presente regulamento é igualmente aplicável, entre outras, às atividades dos tribunais e de outras autoridades judiciais, poderá determinar-se no direito da União ou dos Estados-Membros quais as operações e os procedimentos a seguir pelos tribunais e outras autoridades judiciais para o tratamento de dados pessoais. A competência das autoridades de controlo não abrange o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões. Deverá ser possível confiar o controlo de tais operações de tratamento de dados a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverão, nomeadamente, assegurar o cumprimento das regras do presente regulamento, reforçar a sensibilização os membros do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e tratar reclamações relativas às operações de tratamento dos dados.
- (21) O presente regulamento aplica-se sem prejuízo da aplicação da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho <sup>(2)</sup>, nomeadamente das normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º. A referida diretiva tem por objetivo contribuir para o correto funcionamento do mercado interno, garantindo a livre circulação dos serviços da sociedade da informação entre Estados-Membros.
- (22) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado na União. O estabelecimento pressupõe o exercício efetivo e real de uma atividade com base numa instalação estável. A forma jurídica de tal estabelecimento, quer se trate de uma sucursal quer de uma filial com personalidade jurídica, não é fator determinante nesse contexto.

<sup>(1)</sup> Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (ver página 89 do presente Jornal Oficial).

<sup>(2)</sup> Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

- (23) A fim de evitar que as pessoas singulares sejam privadas da proteção que lhes assiste por força do presente regulamento, o tratamento dos dados pessoais de titulares que se encontrem na União por um responsável pelo tratamento ou subcontratante não estabelecido na União deverá ser abrangido pelo presente regulamento se as atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares, independentemente de estarem associadas a um pagamento. A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio *web* do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União.
- (24) O tratamento de dados pessoais de titulares de dados que se encontrem na União por um responsável ou subcontratante que não esteja estabelecido na União deverá ser também abrangido pelo presente regulamento quando esteja relacionado com o controlo do comportamento dos referidos titulares de dados, na medida em que o seu comportamento tenha lugar na União. A fim de determinar se uma atividade de tratamento pode ser considerada «controlo do comportamento» de titulares de dados, deverá determinar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados pessoais que consistem em definir o perfil de uma pessoa singular, especialmente para tomar decisões relativas a essa pessoa ou analisar ou prever as suas preferências, o seu comportamento e as suas atitudes.
- (25) Sempre que o direito de um Estado-Membro seja aplicável por força do direito internacional público, o presente regulamento deverá ser igualmente aplicável aos responsáveis pelo tratamento não estabelecidos na União, por exemplo numa missão diplomática ou num posto consular de um Estado-Membro.
- (26) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados pessoais que tenham sido pseudonimizados, que possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados informações sobre uma pessoa singular identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento quer por outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta a tecnologia disponível à data do tratamento dos dados e a evolução tecnológica. Os princípios da proteção de dados não 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 ou já não possa ser identificado. O presente regulamento não diz, por isso, respeito ao tratamento dessas informações anónimas, inclusive para fins estatísticos ou de investigação.
- (27) O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas.
- (28) A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da «pseudonimização» no presente regulamento não se destina a excluir eventuais outras medidas de proteção de dados.
- (29) A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização, permitindo-se simultaneamente uma análise geral, no âmbito do mesmo responsável pelo tratamento quando este tiver tomado as medidas técnicas e organizativas necessárias para assegurar, relativamente ao tratamento em questão, a aplicação do presente regulamento ea conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. O responsável pelo tratamento que tratar os dados pessoais deverá indicar as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento.

- (30) As pessoas singulares podem ser associadas a identificadores por via eletrónica, fornecidos pelos respetivos aparelhos, aplicações, ferramentas e protocolos, tais como endereços IP (protocolo internet) ou testemunhos de conexão (cookie) ou outros identificadores, como as etiquetas de identificação por radiofrequência. Estes identificadores podem deixar vestígios que, em especial quando combinados com identificadores únicos e outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação das pessoas singulares.
- (31) As autoridades públicas a quem forem divulgados dados pessoais em conformidade com obrigações jurídicas para o exercício da sua missão oficial, tais como as autoridades fiscais e aduaneiras, as unidades de investigação financeira, as autoridades administrativas independentes ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados de valores mobiliários, não deverão ser consideradas destinatárias se receberem dados pessoais que sejam necessários para efetuar um inquérito específico de interesse geral, em conformidade com o direito da União ou dos Estados-Membros. Os pedidos de divulgação enviados pelas autoridades públicas deverão ser sempre feitos por escrito, fundamentados e ocasionais e não deverão dizer respeito à totalidade de um ficheiro nem implicar a interconexão de ficheiros. O tratamento desses dados pessoais por essas autoridades públicas deverá respeitar as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.
- (32) 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 que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrónico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sítio *web* na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-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 no seguimento de um pedido apresentado por via eletrónica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido.
- (33) Muitas vezes não é possível identificar na totalidade a finalidade do tratamento de dados pessoais para efeitos de investigação científica no momento da recolha dos dados. Por conseguinte, os titulares dos dados deverão poder dar o seu consentimento para determinadas áreas de investigação científica, desde que estejam de acordo com padrões éticos reconhecidos para a investigação científica. Os titulares dos dados deverão ter a possibilidade de dar o seu consentimento unicamente para determinados domínios de investigação ou partes de projetos de investigação, na medida permitida pela finalidade pretendida.
- (34) Os dados genéticos deverão ser definidos como os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que resultem da análise de uma amostra biológica da pessoa singular em causa, nomeadamente da análise de cromossomas, ácido desoxirribonucleico (ADN) ou ácido ribonucleico (ARN), ou da análise de um outro elemento que permita obter informações equivalentes.
- (35) Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho <sup>(1)</sup>, a essa pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.
- (36) O estabelecimento principal de um responsável pelo tratamento na União deverá ser o local onde se encontra a sua administração central na União, salvo se as decisões sobre as finalidades e os meios de tratamento dos dados pessoais forem tomadas noutro estabelecimento do responsável pelo tratamento na União. Nesse caso, esse outro

<sup>(1)</sup> Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).



estabelecimento deverá ser considerado o estabelecimento principal. O estabelecimento principal de um responsável pelo tratamento na União deverá ser determinado de acordo com critérios objetivos e deverá pressupor o exercício efetivo e real de atividades de gestão que determinem as decisões principais quanto às finalidades e aos meios de tratamento mediante instalações estáveis. Esse critério não deverá depender do facto de o tratamento ser realizado nesse local. A existência e utilização de meios técnicos e de tecnologias para o tratamento de dados pessoais ou as atividades de tratamento não constituem, em si mesmas, um estabelecimento principal nem são, portanto, um critério definidor de estabelecimento principal. O estabelecimento principal do subcontratante é o local da sua administração central na União, ou, caso não tenha administração central na União, o local onde são exercidas as principais atividades de tratamento de dados na União. Nos casos que impliquem tanto o responsável pelo tratamento como o subcontratante, a autoridade de controlo principal deverá continuar a ser a autoridade de controlo do Estado-Membro onde o responsável pelo tratamento tem o estabelecimento principal, mas a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e deverá participar no processo de cooperação previsto pelo presente regulamento. Em qualquer caso, as autoridades de controlo do Estado-Membro ou Estados-Membros em que o subcontratante tenha um ou mais estabelecimentos não deverão ser consideradas autoridades de controlo interessadas caso o projeto de decisão diga respeito apenas ao responsável pelo tratamento. Sempre que o tratamento dos dados seja efetuado por um grupo empresarial, o estabelecimento principal da empresa que exerce o controlo deverá ser considerado o estabelecimento principal do grupo empresarial, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa.

- (37) Um grupo empresarial deverá abranger uma empresa que exerce o controlo e as empresas que controla, devendo a primeira ser a que pode exercer uma influência dominante sobre as outras empresas, por exemplo, em virtude da propriedade, da participação financeira ou das regras que a regem ou da faculdade de fazer aplicar as regras relativas à proteção de dados pessoais. Uma empresa que controla o tratamento dos dados pessoais nas empresas a ela associadas deverá ser considerada, juntamente com essas empresas, um «grupo empresarial».
- (38) As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.
- (39) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas singulares que os dados pessoais que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento e a medida em que os dados pessoais são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Esse princípio diz respeito, em particular, às informações fornecidas aos titulares dos dados sobre a identidade do responsável pelo tratamento dos mesmos e os fins a que o tratamento se destina, bem como às informações que se destinam a assegurar que seja efetuado com equidade e transparência para com as pessoas singulares em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais que lhes dizem respeito que estão a ser tratados. As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento. Em especial, as finalidades específicas do tratamento dos dados pessoais deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados pessoais. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados. Para isso, é necessário assegurar que o prazo de conservação dos dados seja limitado ao mínimo. Os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados pessoais sejam conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Deverão ser adotadas todas as medidas razoáveis para que os dados pessoais inexatos sejam retificados ou apagados. Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.
- (40) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro

ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar.

- (41) Caso o presente regulamento se refira a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um parlamento, sem prejuízo dos requisitos que decorram da ordem constitucional do Estado-Membro em causa. No entanto, esse fundamento jurídico ou essa medida legislativa deverão ser claros e precisos e a sua aplicação deverá ser previsível para os seus destinatários, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia («Tribunal de Justiça») e pelo Tribunal Europeu dos Direitos do Homem.
- (42) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento deverá poder demonstrar que o titular deu o seu consentimento à operação de tratamento dos dados. Em especial, no contexto de uma declaração escrita relativa a outra matéria, deverão existir as devidas garantias de que o titular dos dados está plenamente ciente do consentimento dado e do seu alcance. Em conformidade com a Diretiva 93/13/CEE do Conselho <sup>(1)</sup>, uma declaração de consentimento, previamente formulada pelo responsável pelo tratamento, deverá ser fornecida de uma forma inteligível e de fácil acesso, numa linguagem clara e simples e sem cláusulas abusivas. Para que o consentimento seja dado com conhecimento de causa, o titular dos dados deverá conhecer, pelo menos, a identidade do responsável pelo tratamento e as finalidades a que o tratamento se destina. Não se deverá considerar que o consentimento foi dado de livre vontade se o titular dos dados não dispuser de uma escolha verdadeira ou livre ou não puder recusar nem retirar o consentimento sem ser prejudicado.
- (43) A fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto entre o titular dos dados e o responsável pelo seu tratamento, nomeadamente quando o responsável pelo tratamento é uma autoridade pública pelo que é improvável que o consentimento tenha sido dado de livre vontade em todas as circunstâncias associadas à situação específica em causa. Presume-se que o consentimento não é dado de livre vontade se não for possível dar consentimento separadamente para diferentes operações de tratamento de dados pessoais, ainda que seja adequado no caso específico, ou se a execução de um contrato, incluindo a prestação de um serviço, depender do consentimento apesar de o consentimento não ser necessário para a mesma execução.
- (44) O tratamento deverá ser considerado lícito caso seja necessário no contexto de um contrato ou da intenção de celebrar um contrato.
- (45) Sempre que o tratamento dos dados for realizado em conformidade com uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública, o tratamento deverá assentar no direito da União ou de um Estado-Membro. O presente regulamento não exige uma lei específica para cada tratamento de dados. Poderá ser suficiente uma lei para diversas operações de tratamento baseadas numa obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública. Deverá também caber ao direito da União ou dos Estados-Membros determinar qual a finalidade do tratamento dos dados. Além disso, a referida lei poderá especificar as condições gerais do presente regulamento que regem a legalidade do tratamento dos dados pessoais, estabelecer regras específicas para determinar os responsáveis pelo tratamento, o tipo de dados pessoais a tratar, os titulares dos dados em questão, as entidades a que os dados pessoais podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a licitude e equidade do tratamento. Deverá igualmente caber ao direito da União ou dos Estados-Membros determinar se o responsável pelo tratamento que exerce funções de interesse público ou prerrogativas de autoridade pública deverá ser uma autoridade pública ou outra pessoa singular ou coletiva de direito público, ou, caso tal seja do interesse público, incluindo por motivos de saúde, como motivos de saúde pública e proteção social e de gestão dos serviços de saúde, de direito privado, por exemplo uma associação profissional.
- (46) O tratamento de dados pessoais também deverá ser considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa singular. Em princípio, o tratamento

<sup>(1)</sup> Diretiva 93/13/CEE do Conselho, de 5 de abril de 1993, relativa às cláusulas abusivas nos contratos celebrados com os consumidores (JO L 95 de 21.4.1993, p. 29).

de dados pessoais com base no interesse vital de outra pessoa singular só pode ter lugar quando o tratamento não se puder basear manifestamente noutro fundamento jurídico. Alguns tipos de tratamento podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, incluindo a monitorização de epidemias e da sua propagação ou em situações de emergência humanitária, em especial em situações de catástrofes naturais e de origem humana.

- (47) Os interesses legítimos dos responsáveis pelo tratamento, incluindo os dos responsáveis a quem os dados pessoais possam ser comunicados, ou de terceiros, podem constituir um fundamento jurídico para o tratamento, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais do titular, tomando em conta as expectativas razoáveis dos titulares dos dados baseadas na relação com o responsável. Poderá haver um interesse legítimo, por exemplo, quando existir uma relação relevante e apropriada entre o titular dos dados e o responsável pelo tratamento, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento. De qualquer modo, a existência de um interesse legítimo requer uma avaliação cuidada, nomeadamente da questão de saber se o titular dos dados pode razoavelmente prever, no momento e no contexto em que os dados pessoais são recolhidos, que esses poderão vir a ser tratados com essa finalidade. Os interesses e os direitos fundamentais do titular dos dados podem, em particular, sobrepor-se ao interesse do responsável pelo tratamento, quando que os dados pessoais sejam tratados em circunstâncias em que os seus titulares já não esperam um tratamento adicional. Dado que incumbe ao legislador prever por lei o fundamento jurídico para autorizar as autoridades a procederem ao tratamento de dados pessoais, esse fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas na prossecução das suas atribuições. O tratamento de dados pessoais estritamente necessário aos objetivos de prevenção e controlo da fraude constitui igualmente um interesse legítimo do responsável pelo seu tratamento. Poderá considerar-se de interesse legítimo o tratamento de dados pessoais efetuado para efeitos de comercialização direta.
- (48) Os responsáveis pelo tratamento que façam parte de um grupo empresarial ou de uma instituição associada a um organismo central poderão ter um interesse legítimo em transmitir dados pessoais no âmbito do grupo de empresas para fins administrativos internos, incluindo o tratamento de dados pessoais de clientes ou funcionários. Os princípios gerais que regem a transmissão de dados pessoais, no âmbito de um grupo empresarial, para uma empresa localizada num país terceiro mantêm-se inalterados.
- (49) O tratamento de dados pessoais, na medida estritamente necessária e proporcionada para assegurar a segurança da rede e das informações, ou seja, a capacidade de uma rede ou de um sistema informático de resistir, com um dado nível de confiança, a eventos acidentais ou a ações maliciosas ou ilícitas que comprometam a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados pessoais conservados ou transmitidos, bem como a segurança dos serviços conexos oferecidos ou acessíveis através destas redes e sistemas, pelas autoridades públicas, equipas de intervenção em caso de emergências informáticas (CERT), equipas de resposta a incidentes no domínio da segurança informática (CSIRT), fornecedores ou redes de serviços de comunicações eletrónicas e por fornecedores de tecnologias e serviços de segurança, constitui um interesse legítimo do responsável pelo tratamento. Pode ser esse o caso quando o tratamento vise, por exemplo, impedir o acesso não autorizado a redes de comunicações eletrónicas e a distribuição de códigos maliciosos e pôr termo a ataques de «negação de serviço» e a danos causados aos sistemas de comunicações informáticas e eletrónicas.
- (50) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados pessoais tenham sido inicialmente recolhidos apenas 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 do que permitiu a recolha dos dados pessoais. Se o tratamento for necessário para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e 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 tratamento lícito compatível. O fundamento jurídico previsto no direito da União ou dos Estados-Membros para o tratamento dos dados pessoais pode igualmente servir de fundamento jurídico para o tratamento posterior. A fim de apurar se a finalidade de uma nova operação de tratamento dos dados é ou não compatível com a finalidade para que os dados pessoais foram inicialmente recolhidos, o responsável pelo seu tratamento, após ter cumprido todos os requisitos para a licitude do tratamento inicial, deverá ter em atenção, entre outros aspetos, a existência de uma ligação entre a primeira finalidade e aquela a que se destina a nova operação de tratamento que se pretende efetuar, o contexto em que os dados pessoais foram recolhidos, em especial as expectativas razoáveis do titular dos dados quanto à sua posterior utilização, baseadas na sua relação

com o responsável pelo tratamento; a natureza dos dados pessoais; as consequências que o posterior tratamento dos dados pode ter para o seu titular; e a existência de garantias adequadas tanto no tratamento inicial como nas outras operações de tratamento previstas.

Caso o titular dos dados tenha dado o seu consentimento ou o tratamento se baseie em disposições do direito da União ou de um Estado-Membro que constituam uma medida necessária e proporcionada, numa sociedade democrática, para salvaguardar, em especial, os importantes objetivos de interesse público geral, o responsável pelo tratamento deverá ser autorizado a proceder ao tratamento posterior dos dados pessoais, independentemente da compatibilidade das finalidades. Em todo o caso, deverá ser garantida a aplicação dos princípios enunciados pelo presente regulamento e, em particular, a obrigação de informar o titular dos dados sobre essas outras finalidades e sobre os seus direitos, incluindo o direito de se opor. A indicação pelo responsável pelo tratamento de eventuais atos criminosos ou ameaças à segurança pública e a transmissão dos dados pessoais pertinentes, em casos individuais ou em vários casos relativos ao mesmo ato criminoso ou ameaça à segurança pública, a uma autoridade competente deverão ser consideradas como sendo do interesse legítimo do responsável pelo tratamento. Todavia, deverá ser proibido proceder à transmissão no interesse legítimo do responsável pelo tratamento ou ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal, profissional ou outra obrigação vinculativa de confidencialidade.

- (51) Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se neste caso os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais.
- (52) As derrogações à proibição de tratamento de categorias especiais de dados pessoais deverão ser igualmente permitidas quando estiverem previstas no direito da União ou dos Estados-Membros sujeitas a salvaguardas adequadas, de forma a proteger os dados pessoais e outros direitos fundamentais, casotal seja do interesse público, nomeadamente o tratamento de dados pessoais em matéria de direito laboral, de direito de proteção social, incluindo as pensões, e para fins de segurança, monitorização e alerta em matéria de saúde, prevenção ou controlo de doenças transmissíveis e outras ameaças graves para a saúde. Essas derrogações poderão ser previstas por motivos sanitários, incluindo de saúde pública e de gestão de serviços de saúde, designadamente para assegurar a qualidade e a eficiência em termos de custos dos procedimentos utilizados para regularizar os pedidos de prestações sociais e de serviços no quadro do regime de seguro de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Uma derrogação deverá também permitir o tratamento desses dados pessoais quando tal for necessário à declaração, ao exercício ou à defesa de um direito, independentemente de se tratar de um processo judicial ou de um processo administrativo ou extrajudicial.
- (53) As categorias especiais de dados pessoais que merecem uma proteção mais elevada só deverão ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos 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, incluindo o tratamento por parte da administração e das autoridades sanitárias centrais nacionais desses dados para efeitos de controlo da qualidade, informação de gestão e supervisão geral a nível nacional e local do sistema de saúde ou de ação social, assegurando a continuidade dos cuidados de saúde ou de ação social e da prestação de cuidados de saúde transfronteiras, ou para fins de segurança, monitorização e alerta em matéria de saúde, ou para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos baseados no direito da União ou dos Estados-Membros e que têm de cumprir um objetivo, assim como para os estudos realizados no interesse público no domínio da saúde pública. 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 ou dos Estados-Membros deverá prever medidas específicas e adequadas com vista à defesa dos direitos fundamentais e dos dados pessoais das pessoas singulares. Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados pessoais na União, quando essas condições se aplicam ao tratamento transfronteiriço desses dados.

- (54) 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 liberdades das pessoas singulares. Neste 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 <sup>(1)</sup>, ou seja, todos os elementos relacionados com a saúde, a saber, o estado de saúde, incluindo a morbilidade e a incapacidade, as determinantes desse estado de saúde, as necessidades de cuidados de saúde, os recursos atribuídos aos cuidados de saúde, a prestação de cuidados de saúde e o acesso universal aos mesmos, assim como as despesas e o financiamento dos cuidados de saúde, e as causas de mortalidade. Tais atividades de tratamento de dados sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, como os empregadores ou as companhias de seguros e entidades bancárias.
- (55) Além disso, o tratamento de dados pessoais pelas autoridades públicas tendo em vista realizar os objetivos, consagrados no direito constitucional ou no direito internacional público, de associações religiosas oficialmente reconhecidas, é efetuado por motivos de interesse público.
- (56) Sempre que, no âmbito do exercício de atividades eleitorais, o funcionamento do sistema democrático num Estado-Membro exigir que os partidos políticos recolham dados pessoais sobre a opinião política dos cidadãos, o tratamento desses dados pode ser autorizado por motivos de interesse público, desde que sejam estabelecidas garantias adequadas.
- (57) Se os dados pessoais tratados pelo responsável pelo tratamento não lhe permitirem identificar uma pessoa singular, aquele não deverá ser obrigado a obter informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento a uma disposição do presente regulamento. Todavia, o responsável pelo tratamento não deverá recusar receber informações suplementares fornecidas pelo titular no intuito de 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 titular dos dados para aceder aos serviços do responsável pelo tratamento por via eletrónica.
- (58) O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. Essas informações poderão ser fornecidas por via eletrónica, por exemplo num sítio *web*, quando se destinarem ao público. Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrónica. Uma vez que as crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente.
- (59) 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, sendo caso disso, obter a título gratuito, 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 injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido.

<sup>(1)</sup> Regulamento (CE) n.º 1338/2008 do Parlamento Europeu e do Conselho, de 16 de dezembro de 2008, relativo às estatísticas comunitárias sobre saúde pública e saúde e segurança no trabalho (JO L 354 de 31.12.2008, p. 70).

- (60) Os princípios do tratamento equitativo 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 equitativo e transparente tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais forem tratados. O titular dos dados deverá também ser informado da definição de perfis e das consequências que daí advêm. 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 útil perspectiva geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.
- (61) As informações sobre o tratamento de dados pessoais relativos ao titular dos dados deverão ser a este fornecidas no momento da sua recolha junto do titular dos dados ou, se os dados pessoais tiverem sido obtidos a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias. Sempre que os dados pessoais forem suscetíveis de ser legitimamente comunicados a outro destinatário, o titular dos dados 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 outro fim que não aquele para o qual tenham sido recolhidos, antes desse tratamento o responsável pelo tratamento deverá fornecer ao titular dos dados informações sobre esse fim 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 fornecidas informações genéricas.
- (62) Todavia, não é necessário impor a obrigação de fornecer informações caso o titular dos dados já disponha da informação, caso a lei disponha expressamente o registo ou a comunicação dos dados pessoais ou caso a informação ao titular dos dados se revele impossível de concretizar ou implicar um esforço desproporcionado. Este último seria, nomeadamente, o caso de um tratamento efetuado para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos. Para esse efeito, deverá ser considerado o número de titulares de dados, a antiguidade dos dados e as devidas garantias que tenham sido adotadas.
- (63) Os titulares de 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 conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. 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, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados. Quando o responsável 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.
- (64) O responsável pelo tratamento deverá adotar todas as medidas razoáveis para verificar a identidade do titular dos dados que solicite o acesso, em especial no contexto de serviços e de identificadores por via eletrónica. Os responsáveis pelo tratamento não deverão conservar dados pessoais com a finalidade exclusiva de estar em condições de reagir a eventuais pedidos.
- (65) Os titulares dos dados deverão ter direito a que os dados que lhes digam respeito sejam retificados e o «direito a serem esquecidos» quando a conservação desses dados violar o presente regulamento ou o direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento. Em especial, os titulares de dados deverão ter direito a que os seus dados pessoais sejam apagados e deixem de ser objeto de tratamento se deixarem de ser necessários para a finalidade para a qual foram recolhidos ou tratados, se os titulares dos dados retirarem o seu consentimento ou se opuserem ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. Esse direito assume particular importância

quando 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 deseje 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 da conservação dos dados pessoais deverá ser efetuado de forma lícita quando tal se revele necessário para o exercício do direito de liberdade de expressão e informação, para o cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, por razões de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, 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.

- (66) Para reforçar o direito a ser esquecido no ambiente por via eletrónica, o âmbito do direito ao apagamento deverá ser alargado através da imposição ao responsável pelo tratamento que tenha tornado públicos os dados pessoais da adoção de medidas razoáveis, incluindo a aplicação de medidas técnicas, para informar os responsáveis que estejam a tratar esses dados pessoais de que os titulares dos dados solicitaram a supressão de quaisquer ligações para esses dados pessoais ou de cópias ou reproduções dos mesmos. Ao fazê-lo, esse responsável pelo tratamento deverá adotar as medidas que se afigurarem razoáveis, tendo em conta a tecnologia disponível e os meios ao seu dispor, incluindo medidas técnicas, para informar do pedido do titular dos dados pessoais os responsáveis que estejam a tratar os dados.
- (67) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento, a indisponibilização do acesso a determinados dados pessoais por parte dos utilizadores, ou a retirada temporária de um sítio *web* dos dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados. Deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.
- (68) Para reforçar o controlo sobre os seus próprios dados, sempre que o tratamento de dados pessoais for automatizado, o titular dos dados deverá ser autorizado a receber os dados pessoais que lhe digam respeito, que tenha fornecido a um responsável pelo tratamento num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados 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 o cumprimento de um contrato. Não deverá ser aplicável se o tratamento se basear num fundamento jurídico que não seja o consentimento ou um contrato. Por natureza própria, esse direito não deverá ser exercido em relação aos responsáveis pelo tratamento que tratem dados pessoais na prossecução das suas atribuições públicas. 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 esteja sujeito, para o exercício de atribuições de interesse público ou para 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 disser respeito a mais de um titular, o direito de receber os dados pessoais não deverá prejudicar os direitos e liberdades de outros titulares de dados nos termos do presente regulamento. Além disso, esse direito também não deverá prejudicar o direito dos titulares dos dados a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, nomeadamente, não deverá implicar o apagamento dos dados pessoais relativos ao titular que este tenha fornecido para execução de um contrato, na medida em que e enquanto os dados pessoais forem necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deverá ter o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento.
- (69) 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 ou ainda por motivos de interesse legítimo do responsável pelo tratamento ou de terceiros, o titular 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 imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.
- (70) Sempre que os dados pessoais forem objeto de tratamento para efeitos de comercialização direta, o titular deverá ter o direito de se opor, em qualquer momento e gratuitamente, a tal tratamento, incluindo a definição de perfis na medida em que esteja relacionada com a referida comercialização, quer se trate do tratamento inicial quer do tratamento posterior. Esse direito deverá ser explicitamente levado à atenção do titular e apresentado de modo claro e distinto de quaisquer outras informações.

- (71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá 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 a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. 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 equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento 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 são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas.

- (72) A definição de perfis está sujeita às regras do presente regulamento que regem o tratamento de dados pessoais, como o fundamento jurídico do tratamento ou os princípios da proteção de dados. O Comité Europeu para a Proteção de Dados criado pelo presente regulamento («Comité») deverá poder emitir orientações nesse âmbito.
- (73) O direito da União ou dos Estados-Membros podem impor restrições relativas a princípios específicos e aos direitos de informação, acesso e retificação ou apagamento de dados pessoais e ao direito à portabilidade dos dados, ao direito de oposição, às decisões baseadas na definição de perfis, bem como à comunicação de uma violação de dados pessoais ao titular dos dados, e a determinadas obrigações conexas dos responsáveis pelo tratamento, na medida em que sejam necessárias e proporcionadas numa sociedade democrática para garantir a segurança pública, incluindo a proteção da vida humana, especialmente em resposta a catástrofes naturais ou provocadas pelo homem, para a prevenção, a investigação e a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou violações da deontologia de profissões regulamentadas, para outros objetivos importantes de interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, para a conservação de registos públicos por motivos de interesse público geral, para posterior tratamento de dados pessoais arquivados para a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários ou para efeitos de defesa do titular dos dados ou dos direitos e liberdades de terceiros, incluindo a proteção social, a saúde pública e os fins humanitários. Essas restrições deverão respeitar as exigências estabelecidas na Carta e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.
- (74) Deverá ser consagrada a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas que forem adequadas e eficazes e ser capaz de comprovar que as atividades de tratamento são efetuadas em conformidade 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 liberdades das pessoas singulares.



- (75) O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes 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.
- (76) A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado.
- (77) As orientações sobre a execução de medidas adequadas e sobre a comprovação de conformidade pelos responsáveis pelo tratamento ou subcontratantes, em especial no que diz respeito à identificação dos riscos relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos riscos, poderão ser obtidas nomeadamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações fornecidas pelo Comité ou às indicações fornecidas por um encarregado da proteção de dados. O Comité poderá emitir igualmente orientações sobre operações de tratamento de dados que não sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares e indicar quais as medidas adequadas em tais casos para diminuir esse risco.
- (78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar 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 podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos.
- (79) A defesa dos direitos e liberdades dos titulares dos dados, bem como a responsabilidade dos responsáveis pelo seu tratamento e dos subcontratantes, incluindo no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição das responsabilidades nos termos do presente regulamento, nomeadamente quando o responsável pelo tratamento determina as finalidades e os meios do tratamento conjuntamente com outros responsáveis, ou quando uma operação de tratamento de dados é efetuada por conta de um responsável pelo tratamento.
- (80) Sempre que um responsável pelo tratamento ou um subcontratante não estabelecidos na União efetuarem o tratamento de dados pessoais de titulares de dados que se encontrem na União, e as suas atividades de tratamento estiverem relacionadas com a oferta de bens ou serviços a esses titulares de dados na União, independentemente de a estes ser exigido um pagamento, ou com o controlo do seu comportamento na medida que o seu comportamento tenha lugar na União, o responsável pelo tratamento ou o subcontratante deverão designar um representante, a não ser que o tratamento seja ocasional, não inclua o tratamento, em larga escala, de categorias especiais de dados pessoais, nem o tratamento de dados pessoais relativos a condenações penais e infrações, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a

natureza, o contexto, o âmbito e as finalidades do tratamento ou se o responsável pelo tratamento for uma autoridade ou organismo público. O representante deverá agir em nome do responsável pelo tratamento ou do subcontratante e deverá poder ser contactado por qualquer autoridade de controlo. O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento ou do subcontratante, emitido por escrito, que permita ao representante agir em seu nome no que diz respeito às obrigações que lhes são impostas pelo presente regulamento. A designação de um tal representante não afeta as responsabilidades que incumbem ao responsável pelo tratamento ou ao subcontratante nos termos do presente regulamento. O representante deverá executar as suas tarefas em conformidade com o mandato que recebeu do responsável pelo tratamento ou do subcontratante, incluindo no que toca à cooperação com as autoridades de controlo competentes relativamente a qualquer ação empreendida no sentido de garantir o cumprimento do presente regulamento. O representante designado deverá estar sujeito a procedimentos de execução em caso de incumprimento pelo responsável pelo tratamento ou pelo subcontratante.

- (81) 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, nomeadamente no que se refere à segurança do tratamento. O facto de o subcontratante cumprir um código de conduta aprovado ou um procedimento de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento. A realização de operações de tratamento de dados em subcontratação deverá ser regulada por um contrato ou por outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento e em que seja estabelecido o objeto e a duração do contrato, a natureza e as finalidades do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, tendo em conta as tarefas e responsabilidades específicas do subcontratante no contexto do tratamento a realizar e o risco em relação aos direitos e liberdades do titular dos dados. O responsável pelo tratamento e o subcontratante poderão optar por utilizar um contrato individual ou cláusulas contratuais-tipo que são adotadas quer diretamente pela Comissão quer por uma autoridade de controlo em conformidade com o procedimento de controlo da coerência e adotadas posteriormente pela Comissão. Após concluído o tratamento por conta do responsável pelo tratamento, o subcontratante deverá, consoante a escolha do primeiro, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação dos dados pessoais ao abrigo do direito da União ou do Estado-Membro a que o subcontratante está sujeito.
- (82) A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento ou o subcontratante deverá conservar registos de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhes esses registos, a pedido, para fiscalização dessas operações de tratamento.
- (83) 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 assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos riscos e da natureza dos dados pessoais a proteger. Ao avaliar os riscos para a segurança dos dados, deverão ser tidos em conta os riscos apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, riscos esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.
- (84) A fim de promover o cumprimento do presente regulamento nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo seu tratamento deverá encarregar-se da realização de uma avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação, será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais.
- (85) Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas

singulares. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada.

- (86) O responsável pelo tratamento deverá informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias. A comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos. Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação.
- (87) Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular. Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados. Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.
- (88) Ao estabelecer regras pormenorizadas relativamente ao formato e aos procedimentos aplicáveis à notificação das violações de dados pessoais, deverá ter-se devidamente em conta as circunstâncias dessa violação, nomeadamente a existência ou não de proteção dos dados pessoais através de medidas técnicas de proteção adequadas para reduzir eficazmente a probabilidade de usurpação da identidade ou outras formas de utilização abusiva. Além disso, tais regras e procedimentos deverão ter em conta os legítimos interesses das autoridades de polícia nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias da violação de dados pessoais.
- (89) A Diretiva 95/46/CE estabelece uma obrigação geral de notificação do tratamento de dados pessoais às autoridades de controlo. Além de esta obrigação originar encargos administrativos e financeiros, nem sempre contribuiu para a melhoria da proteção dos dados pessoais. Tais obrigações gerais e indiscriminadas de notificação deverão, por isso, ser suprimidas e substituídas por regras e procedimentos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades. Os referidos tipos de operações de tratamento poderão, nomeadamente, envolver a utilização de novas tecnologias, ou pertencer a um novo tipo e não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento, ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial responsável pelo tratamento.
- (90) Nesses casos, o responsável pelo tratamento deverá proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particulares do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse risco, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.
- (91) Tal deverá aplicar-se, nomeadamente, às operações de tratamento de grande escala que visem o tratamento de uma grande quantidade de dados pessoais a nível regional, nacional ou supranacional, possam afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado risco, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado risco para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos

titulares o exercício dos seus direitos. Dever-se-á realizar também uma avaliação de impacto sobre a proteção de dados nos casos em que os dados pessoais são tratados para tomar decisões relativas a determinadas pessoas singulares na sequência de qualquer avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares baseada na definição dos perfis desses dados ou na sequência do tratamento de categorias especiais de dados pessoais, de dados biométricos ou de dados sobre condenações penais e infrações ou medidas de segurança conexas. É igualmente exigida uma avaliação do impacto sobre a proteção de dados para o controlo de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrónicos, ou para quaisquer outras operações quando a autoridade de controlo competente considere que o tratamento é suscetível de implicar um elevado risco para os direitos e liberdades dos titulares dos dados, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala. O tratamento de dados pessoais não deverá ser considerado de grande escala se disser respeito aos dados pessoais de pacientes ou clientes de um determinado médico, profissional de cuidados de saúde, hospital ou advogado. Nesses casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória.

- (92) Em certas circunstâncias pode ser razoável e económico alargar a avaliação de impacto sobre a proteção de dados para além de um projeto único, por exemplo se as autoridades ou organismos públicos pretenderem criar uma aplicação ou uma plataforma de tratamento comum, ou se vários responsáveis pelo tratamento planearem criar uma aplicação ou um ambiente de tratamento comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada.
- (93) No contexto da adoção da legislação dos Estados-Membros que regula a prossecução das atribuições da autoridade ou do organismo público, bem como a operação ou o conjunto de operações em questão, os Estados-Membros podem considerar necessário proceder à avaliação antes de iniciar as atividades de tratamento.
- (94) Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta de garantias e de medidas e procedimentos de segurança para atenuar os riscos, implica um elevado risco para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o risco não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes de as atividades de tratamento terem início. Provavelmente, esse elevado risco decorre de determinados tipos de tratamento e da extensão e frequência do tratamento, que podem originar igualmente danos ou interferir com os direitos e liberdades da pessoa singular. A autoridade de controlo deverá responder ao pedido de consulta dentro de um determinado prazo. Contudo, a ausência de reação da autoridade de controlo no decorrer desse prazo não prejudicará qualquer intervenção que esta autoridade venha a fazer em conformidade com as suas funções e competências, definidas pelo presente regulamento, incluindo a competência para proibir certas operações de tratamento. No âmbito desse processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão pode ser apresentado à autoridade de controlo, em especial as medidas previstas para atenuar o risco para os direitos e liberdades das pessoas singulares.
- (95) O subcontratante deverá prestar assistência ao responsável pelo tratamento, se necessário e a pedido deste, para assegurar o cumprimento das obrigações decorrentes da realização de avaliações do impacto sobre a proteção de dados e da consulta prévia à autoridade de controlo.
- (96) Deverá ter também lugar uma consulta à autoridade de controlo durante os trabalhos de elaboração de uma medida legislativa ou regulamentar que preveja o tratamento de dados pessoais, de modo a assegurar a conformidade do tratamento pretendido com o presente regulamento e, em particular, a atenuar o respetivo risco para o titular dos dados.
- (97) Sempre que o tratamento dos dados for efetuado por uma autoridade pública, com exceção dos tribunais ou de autoridades judiciais independentes no exercício da sua função jurisdicional, sempre que, no setor privado, for efetuado por um responsável pelo tratamento cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados em grande escala, ou sempre que as atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados pessoais e de dados relacionados com condenações penais e infrações, o responsável pelo tratamento destes ou o subcontratante pode ser assistido por um especialista em legislação e prática de proteção de dados no controlo do cumprimento do presente regulamento a nível interno. No setor privado, as atividades principais do responsável pelo tratamento dizem respeito às suas atividades primárias e não estão relacionadas com o tratamento de dados pessoais como atividade auxiliar. O nível necessário de conhecimentos especializados deverá ser determinado, em particular, em função do tratamento de dados

realizado e da proteção exigida para os dados pessoais tratados pelo responsável pelo seu tratamento ou pelo subcontratante. Estes encarregados da proteção de dados, sejam ou não empregados do responsável pelo tratamento, deverão estar em condições de desempenhar as suas funções e atribuições com independência.

- (98) As associações ou outras entidades que representem categorias de responsáveis pelo tratamento ou de subcontratantes deverão ser incentivadas a elaborar códigos de conduta, no respeito do presente regulamento, com vista a facilitar a sua aplicação efetiva, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas. Esses códigos de conduta poderão nomeadamente regular as obrigações dos responsáveis pelo tratamento e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares.
- (99) Durante o processo de elaboração de um código de conduta, ou na sua alteração ou aditamento, as associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes deverão consultar as partes interessadas, nomeadamente os titulares dos dados, se possível, e ter em conta os contributos recebidos e as opiniões expressas em resposta a essas consultas.
- (100) A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa.
- (101) A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.
- (102) O presente regulamento não prejudica os acordos internacionais celebrados entre a União Europeia e países terceiros que regulem a transferência de dados pessoais, incluindo as garantias adequadas em benefício dos titulares dos dados. Os Estados-Membros poderão celebrar acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais, desde que tais acordos não afetem o presente regulamento ou quaisquer outras disposições do direito da União e prevejam um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.
- (103) A Comissão pode decidir, com efeitos no conjunto da União, que um país terceiro, um território ou um setor determinado de um país terceiro, ou uma organização internacional, oferece um nível adequado de proteção de dados adequado, garantindo assim a segurança jurídica e a uniformidade ao nível da União relativamente ao país terceiro ou à organização internacional que seja considerado apto a assegurar tal nível de proteção. Nestes casos, podem realizar-se transferências de dados pessoais para esse país ou organização internacional sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir, após enviar ao país terceiro ou organização internacional uma notificação e uma declaração completa dos motivos, revogar essa decisão.
- (104) Em conformidade com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou setor específico de um país terceiro, ter em consideração em que medida esse país respeita o primado do Estado de direito, o acesso à justiça e as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativamente a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país

terceiro. Este deverá dar garantias para assegurar um nível adequado de proteção essencialmente equivalente ao assegurado na União, nomeadamente quando os dados pessoais são tratados num ou mais setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer regras de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

- (105) Além dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, a Comissão deverá ter em conta as obrigações decorrentes da participação do país terceiro ou da organização internacional nos sistemas multilaterais ou regionais, em especial no que diz respeito à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Em especial, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, de 28 de janeiro de 1981, e ao seu Protocolo Adicional. A Comissão deverá consultar o Comité quando avaliar o nível de proteção nos países terceiros ou organizações internacionais.
- (106) A Comissão deverá controlar a eficácia das decisões sobre o nível de proteção assegurado num país terceiro, num território ou num setor específico de um país terceiro, ou numa organização internacional, e acompanhar a eficácia das decisões adotadas com base no artigo 25.º, n.º 6, ou no artigo 26.º, n.º 4, da Diretiva 95/46/CE. Nas suas decisões de adequação, a Comissão deverá prever um procedimento de avaliação periódica da aplicação destas. Essa revisão periódica deverá ser feita em consulta com o país terceiro ou a organização internacional em questão e ter em conta todos os desenvolvimentos pertinentes verificados no país terceiro ou organização internacional. Para efeitos de controlo e de realização das revisões periódicas, a Comissão deverá ter em consideração os pontos de vista e as conclusões a que tenham chegado o Parlamento Europeu e o Conselho, bem como outros organismos e fontes pertinentes. A Comissão deverá avaliar, num prazo razoável, a eficácia destas últimas decisões e comunicar quaisquer resultados pertinentes ao comité na aceção do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho<sup>(1)</sup>, tal como estabelecido no presente regulamento, ao Parlamento Europeu e ao Conselho.
- (107) A Comissão pode reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Por conseguinte, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos constantes do presente regulamento relativos a transferências sujeitas a garantias adequadas, incluindo regras vinculativas aplicáveis às empresas, e derrogações para situações específicas. Nesse caso, deverão ser tomadas medidas que visem uma consulta entre a Comissão e esse país terceiro ou organização internacional. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização internacional das razões da proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação.
- (108) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento ou o subcontratante deverá adotar as medidas necessárias para colmatar a insuficiência da proteção de dados no país terceiro dando para tal garantias adequadas ao titular dos dados. Tais garantias adequadas podem consistir no recurso a regras vinculativas aplicáveis às empresas, cláusulas-tipo de proteção de dados adotadas pela Comissão, cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo, ou cláusulas contratuais autorizadas por esta autoridade. Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, nomeadamente o direito de recurso administrativo ou judicial e de exigir indemnização, quer no território da União quer num país terceiro. 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 autoridades ou organismos públicos 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, como seja um memorando de entendimento, que prevejam a existência de direitos efetivos e oponíveis dos titulares dos dados. Deverá ser obtida a autorização da autoridade de controlo competente quando as garantias previstas em regimes administrativos não forem juridicamente vinculativas.
- (109) A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas

<sup>(1)</sup> Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou 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.

- (110) Os grupos empresariais ou os grupos de empresas envolvidas numa atividade económica conjunta deverão poder utilizar as regras vinculativas aplicáveis às empresas aprovadas para as suas transferências internacionais da União para entidades pertencentes ao mesmo grupo empresarial ou grupo de empresas envolvidas numa atividade económica conjunta, desde que essas regras incluam todos os princípios essenciais e direitos oponíveis que visem assegurar garantias adequadas às transferências ou categorias de transferências de dados pessoais.
- (111) Deverá prever-se a possibilidade de efetuar transferências em determinadas circunstâncias em que o titular dos dados dê o seu consentimento explícito, em que a transferência seja ocasional e necessária em relação a um contrato ou a um contencioso judicial, independentemente de se tratar de um processo judicial, de um processo administrativo ou de um qualquer procedimento não judicial, incluindo procedimentos junto de organismos de regulação. Deverá também estar prevista a possibilidade de efetuar transferências no caso de motivos importantes de interesse público previstos pelo direito da União ou de um Estado-Membro o exigirem, ou se a transferência for efetuada a partir de um registo criado por lei e destinado à consulta por parte do público ou de pessoas com um interesse legítimo. Neste último caso, a transferência não deverá abranger a totalidade dos dados nem categorias completas de dados pessoais contidos nesse registo e, quando este último se destinar a ser consultado por pessoas com um interesse legítimo, a transferência apenas deverá ser efetuada a pedido dessas pessoas ou, caso sejam os seus destinatários, tendo plenamente em conta os interesses e os direitos fundamentais do titular dos dados.
- (112) Essas derrogações deverão ser aplicáveis, em especial, às transferências de dados exigidas e necessárias por razões importantes de interesse público, por exemplo em caso de intercâmbio internacional de dados entre autoridades de concorrência, administrações fiscais ou aduaneiras, entre autoridades de supervisão financeira, entre serviços competentes em matéria de segurança social ou de saúde pública, por exemplo em caso de localização de contactos no que respeita a doenças contagiosas ou para reduzir e/ou eliminar a dopagem no desporto. Deverá igualmente ser considerada legal uma transferência de dados pessoais que seja necessária para a proteção de um interesse essencial para os interesses vitais do titular dos dados ou de outra pessoa, nomeadamente a integridade física ou a vida, se o titular dos dados estiver impossibilitado de dar o seu consentimento. Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro pode, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros deverão notificar essas decisões nacionais à Comissão. As transferências, para uma organização humanitária internacional, de dados pessoais de um titular que seja física ou legalmente incapaz de dar o seu consentimento, com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por ser do interesse vital do titular dos dados.
- (113) As transferências que possam ser classificadas como não repetitivas e que apenas digam respeito a um número limitado de titulares de dados podem igualmente ser admitidas para efeitos dos interesses legítimos imperiosos visados pelo responsável pelo tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados e desde que o responsável pelo tratamento destes tenha avaliado todas as circunstâncias associadas à operação de transferência. O responsável pelo tratamento deverá atender especialmente à natureza dos dados pessoais, à finalidade e à duração da operação ou operações de tratamento previstas, bem como à situação vigente no país de origem, no país terceiro e no país de destino final, e deverá apresentar as garantias adequadas para defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais. Tais transferências só deverão ser possíveis em raros casos em que não se aplique nenhum dos outros motivos de transferência. Para fins de investigação científica ou histórica ou fins estatísticos, deverão ser tidas em consideração as expectativas legítimas da sociedade em matéria de avanço do conhecimento. O responsável pelo tratamento deverá informar da transferência a autoridade de controlo e o titular dos dados.
- (114) Em qualquer caso, se a Comissão não tiver tomado nenhuma decisão relativamente ao nível de proteção adequado de dados num determinado país terceiro, o responsável pelo tratamento ou o subcontratante deverá adotar soluções que confirmem aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, e lhes garantam que continuarão a beneficiar dos direitos e garantias fundamentais.

- (115) Alguns países terceiros aprovam leis, regulamentos e outros atos normativos destinados a regular diretamente as atividades de tratamento pelas pessoas singulares e coletivas sob a jurisdição dos Estados-Membros. Pode ser o caso de sentenças de órgãos jurisdicionais ou de decisões de autoridades administrativas de países terceiros que exijam que o responsável pelo tratamento ou subcontratante transfira ou divulgue dados pessoais sem fundamento em nenhum acordo internacional, como seja um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros. Em virtude da sua aplicabilidade extraterritorial, essas leis, regulamentos e outros atos normativos podem violar o direito internacional e obstar à realização do objetivo de proteção das pessoas singulares, assegurado na União Europeia pelo presente regulamento. As transferências só deverão ser autorizadas quando estejam preenchidas as condições estabelecidas pelo presente regulamento para as transferências para os 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 ou dos Estados-Membros ao qual o responsável pelo tratamento está sujeito.
- (116) Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o risco de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiras podem ser também restringidos por poderes preventivos ou medidas de reparação insuficientes, regimes jurídicos incoerentes e obstáculos práticos, tais como a limitação de recursos. Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados, a fim de que possam efetuar o intercâmbio de informações e realizar investigações com as suas homólogas internacionais. Para efeitos de criação de regras de cooperação internacional que facilitem e proporcionem assistência mútua internacional para a aplicação da legislação de proteção de dados pessoais, a Comissão e as autoridades de controlo deverão trocar informações e colaborar com as autoridades competentes de países terceiros em atividades relacionadas com o exercício dos seus poderes, com base na reciprocidade e em conformidade com o presente regulamento.
- (117) A criação de autoridades de controlo nos Estados-Membros, habilitadas 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 respeita ao tratamento dos seus dados pessoais. Os Estados-Membros deverão poder criar mais do que uma autoridade de controlo, de modo a refletir a sua estrutura constitucional, organizacional e administrativa.
- (118) A independência das autoridades de controlo não deverá implicar que estas autoridades não possam ser sujeitas a procedimentos de controlo ou monitorização no que diz respeito às suas despesas nem a fiscalização judicial.
- (119) Os Estados-Membros que criem várias autoridades de controlo deverão prever na sua legislação procedimentos que garantam a participação efetiva dessas mesmas autoridades no procedimento de controlo da coerência. Esses Estados-Membros deverão, em particular, designar a autoridade de controlo que servirá de ponto de contacto único, para permitir a participação efetiva dessas autoridades no referido procedimento, a fim de assegurar uma cooperação rápida e fácil com outras autoridades de controlo, com o Comité e com a Comissão.
- (120) Deverão ser dados às autoridades de controlo os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União. As autoridades de controlo deverão ter orçamentos anuais públicos separados, que poderão estar integrados no orçamento geral do Estado ou nacional.
- (121) As condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas por lei em cada Estado-Membro e deverão prever, em especial, que os referidos membros sejam nomeados, com recurso a um processo transparente, pelo Parlamento, pelo Governo ou pelo Chefe de Estado do Estado-Membro com base numa proposta do Governo, de um dos seus membros, do Parlamento ou de uma sua câmara, ou por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro. A fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão exercer as suas funções com integridade, abster-se de qualquer ato incompatível com as mesmas e, durante o seu mandato, não deverão exercer nenhuma atividade, seja ou não remunerada, que com elas seja incompatível. A autoridade de controlo deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente criado nos termos do direito do Estado-Membro, que deverá estar exclusivamente sujeito à orientação do membro ou membros da autoridade de controlo.
- (122) As autoridades de controlo deverão ser competentes no território do respetivo Estado-Membro para exercer os poderes e desempenhar as funções que lhes são conferidas nos termos do presente regulamento. Deverá ser



abrangido, em especial, o tratamento de dados efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento ou do subcontratante no território do seu próprio Estado-Membro, o tratamento de dados pessoais efetuado por autoridades públicas ou por organismos privados que atuem no interesse público, o tratamento que afete os titulares de dados no seu território, ou o tratamento de dados efetuado por um responsável ou subcontratante não estabelecido na União quando diga respeito a titulares de dados residentes no seu território. Deverá ficar abrangido o tratamento de reclamações apresentadas por um titular de dados, a realização de investigações sobre a aplicação do presente regulamento e a promoção da sensibilização do público para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais.

- (123) As autoridades de controlo deverão controlar a aplicação das disposições do presente regulamento e contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados a nível do mercado interno. Para esse efeito, as autoridades de controlo deverão cooperar entre si e com a Comissão, sem necessidade de qualquer acordo entre os Estados-Membros quer sobre a prestação de assistência mútua quer sobre tal cooperação.
- (124) Quando o tratamento de dados pessoais ocorra no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante na União e o responsável pelo tratamento ou o subcontratante esteja estabelecido em vários Estados-Membros, ou quando o tratamento no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, na União, afete ou seja suscetível de afetar substancialmente titulares de dados em diversos Estados-Membros, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante deverá agir na qualidade de autoridade de controlo principal. Esta autoridade deverá cooperar com as outras autoridades interessadas, porque o responsável pelo tratamento ou o subcontratante tem um estabelecimento no território do seu Estado-Membro, porque há titulares de dados residentes no seu território que são substancialmente afetados, ou porque lhe foi apresentada uma reclamação. Além do mais, quando tenha sido apresentada uma reclamação por um titular de dados que não resida nesse Estado-Membro, a autoridade de controlo à qual a reclamação tiver sido apresentada deverá ser também autoridade de controlo interessada. No âmbito das suas funções de emissão de orientações sobre qualquer assunto relativo à aplicação do presente regulamento, o Comité deverá poder emitir orientações nomeadamente sobre os critérios a ter em conta para apurar se o tratamento em causa afeta substancialmente titulares de dados em mais do que um Estado-Membro e sobre aquilo que constitui uma objeção pertinente e fundamentada.
- (125) A autoridade principal deverá ser competente para adotar decisões vinculativas relativamente a medidas que deem execução às competências que lhe tenham sido atribuídas nos termos do presente regulamento. Na sua qualidade de autoridade principal, a autoridade de controlo deverá implicar no processo decisório e coordenar as autoridades de controlo interessadas. Nos casos em que a decisão consista em rejeitar no todo ou em parte a reclamação apresentada pelo titular dos dados, esta deverá ser adotada pela autoridade de controlo à qual a reclamação tenha sido apresentada.
- (126) As decisões deverão ser acordadas conjuntamente pela autoridade de controlo principal e as autoridades de controlo interessadas e deverão visar o estabelecimento principal ou único do responsável pelo tratamento ou do subcontratante e ser vinculativas para ambos. O responsável pelo tratamento ou o subcontratante deverá tomar as medidas necessárias para assegurar o cumprimento do disposto no presente regulamento e a execução da decisão notificada pela autoridade de controlo principal ao estabelecimento principal do responsável pelo tratamento ou do subcontratante no que diz respeito às atividades de tratamento de dados na União.
- (127) As autoridades de controlo que não atuem como autoridade de controlo principal deverão ter competência para tratar casos a nível local quando o responsável pelo tratamento ou subcontratante estiver estabelecido em vários Estados-Membros, mas o assunto do tratamento específico disser respeito unicamente ao tratamento efetuado num só Estado-Membro, e envolver somente titulares de dados nesse Estado-Membro, por exemplo, no caso de o assunto dizer respeito ao tratamento de dados pessoais de trabalhadores num contexto específico de emprego num Estado-Membro. Nesses casos, a autoridade de controlo deverá informar imediatamente do assunto a autoridade de controlo principal. Após ter sido informada, a autoridade de controlo principal decidirá se trata o caso de acordo com o disposto em matéria de cooperação entre a autoridade de controlo principal e a outra autoridade de controlo interessada («mecanismo de balcão único»), ou se deverá ser a autoridade de controlo que a informou a tratar o caso a nível local. Ao decidir se trata o caso, a autoridade de controlo principal deverá ter em conta se há algum estabelecimento do responsável pelo tratamento ou subcontratante no Estado-Membro da autoridade de controlo que a informou, a fim de garantir a eficaz execução da decisão relativamente ao responsável pelo tratamento ou subcontratante. Quando a autoridade de controlo principal decide tratar o caso, a

autoridade de controlo que a informou deverá ter a possibilidade de apresentar um projeto de decisão, que a autoridade de controlo principal deverá ter na melhor conta quando prepara o seu projeto de decisão no âmbito desse mecanismo de balcão único.

- (128) As regras relativas à autoridade de controlo principal e ao mecanismo de balcão único não se deverão aplicar quando o tratamento dos dados for efetuado por autoridades públicas ou organismos privados que atuem no interesse público. Em tais casos, a única autoridade de controlo competente para exercer as competências que lhe são conferidas nos termos do presente regulamento deverá ser a autoridade de controlo do Estado-Membro em que estiver estabelecida tal autoridade pública ou organismo privado.
- (129) A fim de assegurar o controlo e a aplicação coerentes do presente regulamento em toda a União, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas funções e poderes efetivos, incluindo poderes de investigação, poderes de correção e de sanção, e poderes consultivos e de autorização, nomeadamente em caso de reclamação apresentada por pessoas singulares, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal ao abrigo do direito do Estado-Membro, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e intervir em processos judiciais. Essas competências deverão incluir o poder de impor uma limitação temporário ou definitiva ao tratamento, ou mesmo a sua proibição. Os Estados-Membros podem estabelecer outras funções relacionadas com a proteção de dados pessoais ao abrigo do presente regulamento. Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas no direito da União e do Estado-Membro, com imparcialidade, com equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com o presente regulamento, tendo em conta as circunstâncias de cada caso concreto, respeitar o direito de todas as pessoas a serem ouvidas antes de ser tomada qualquer medida individual que as prejudique, e evitar custos supérfluos e inconvenientes excessivos para as pessoas em causa. Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito processual do Estado-Membro, como, por exemplo, a obrigação de obter autorização judicial prévia. As medidas juridicamente vinculativas da autoridade de controlo deverão ser emitidas por escrito, claras e inequívocas, indicar a autoridade de controlo que as emitiu e a data de emissão, ostentar a assinatura do diretor ou do membro da autoridade de controlo por eles autorizada, indicar os motivos que as justifica e mencionar o direito de recurso efetivo. Tal não deverá impedir que sejam estabelecidos requisitos suplementares nos termos do direito processual do Estado-Membro. A adoção de uma decisão juridicamente vinculativa pode dar origem a controlo jurisdicional nos Estados-Membros da autoridade de controlo que tenha adotado a decisão.
- (130) Nos casos em que a autoridade de controlo a que a reclamação é apresentada não seja a principal, a autoridade de controlo principal deverá cooperar estreitamente com a autoridade de controlo à qual tiver sido apresentada a reclamação, de acordo com as disposições em matéria de cooperação e coerência do presente regulamento. Nestes casos, a autoridade de controlo principal, ao tomar medidas destinadas a produzir efeitos jurídicos, incluindo a imposição de coimas, deverá ter na melhor conta o parecer da autoridade de controlo à qual tiver sido apresentada a reclamação, que deverá continuar a ser competente para levar a cabo qualquer investigação no território do respetivo Estado-Membro, em ligação com a autoridade de controlo principal.
- (131) Nos casos em que as funções de autoridade principal de controlo devessem ser exercidas por outra autoridade de controlo relativamente às atividades de tratamento do responsável pelo tratamento ou do subcontratante, mas em que o conteúdo concreto da reclamação ou a eventual violação diga respeito apenas às atividades de tratamento do responsável ou do subcontratante realizadas no Estado-Membro onde tenha sido apresentada a reclamação ou detetada a eventual infração, e o assunto não afete nem seja suscetível de afetar substancialmente titulares de dados noutros Estados-Membros, a autoridade de controlo que recebe uma reclamação, deteta ou é de outro modo informada de situações que impliquem eventuais violações do presente regulamento deverá procurar obter um acordo amigável. Se tal não lhe for possível, deverá exercer todos os poderes de que dispõe. Deverão ficar abrangidas: as atividades de tratamento específicas realizadas no território do Estado-Membro da autoridade de controlo ou que digam respeito a titulares de dados em território desse Estado-Membro; as atividades de tratamento realizadas no contexto de uma oferta de bens ou serviços destinados especificamente a titulares de dados no território do Estado-Membro da autoridade de controlo; ou as atividades de tratamento que tenham de ser analisadas tomando em consideração as obrigações legais aplicáveis ao abrigo do direito do Estado-Membro.
- (132) As atividades de sensibilização das autoridades de controlo dirigidas ao público deverão incluir medidas específicas a favor dos responsáveis pelo tratamento e subcontratantes, incluindo as micro, pequenas e médias empresas, bem como as pessoas singulares, em particular num contexto educacional.

- (133) As autoridades de controlo deverão prestar-se mutuamente assistência no desempenho das suas funções, por forma a assegurar a execução e aplicação coerentes do presente regulamento no mercado interno. A autoridade de controlo que solicite assistência mútua pode adotar uma medida provisória se não obtiver resposta relativamente a um pedido de assistência mútua no prazo de um mês a contar da receção desse pedido da outra autoridade de controlo.
- (134) As autoridades de controlo deverão participar, sempre que for adequado, em operações conjuntas com outras autoridades de controlo. A autoridade de controlo requerida deverá ser obrigada a responder ao pedido num prazo determinado.
- (135) A fim de assegurar a aplicação coerente do presente regulamento em toda a União, deverá ser criado um procedimento de controlo da coerência e para a cooperação entre as autoridades de controlo. Esse procedimento deverá ser aplicável, nomeadamente, quando uma autoridade de controlo tenciona adotar uma medida que vise produzir efeitos legais em relação a operações de tratamento que afetem substancialmente um número significativo de titulares de dados em vários Estados-Membros. Deverá aplicar-se igualmente sempre que uma autoridade de controlo interessada, ou a Comissão, solicitar que essa matéria seja tratada no âmbito do procedimento de controlo da coerência. Esse procedimento não deverá prejudicar medidas que a Comissão possa tomar no exercício das suas competências nos termos dos Tratados.
- (136) Quando aplicar o procedimento de controlo da coerência, o Comité deverá emitir um parecer, num prazo determinado, se a maioria dos seus membros assim o decidir ou se tal lhe solicitado por qualquer autoridade de controlo interessada ou pela Comissão. O Comité deverá também ser habilitado a adotar decisões juridicamente vinculativas em caso de litígio entre as autoridades de controlo. Para esse efeito, deverá emitir, em princípio por maioria de dois terços dos seus membros, decisões vinculativas em casos claramente definidos em que as autoridades de controlo tenham posições contraditórias, em especial no âmbito da cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas, a respeito da questão de fundo, designadamente se há violação do presente regulamento.
- (137) Pode ser urgente agir, a fim de defender os direitos e liberdades dos titulares de dados, em especial quando haja perigo de impedimento considerável do exercício de um direito do titular dos dados. Por essa razão, a autoridade de controlo deverá poder adotar no seu território medidas provisórias devidamente justificadas, válidas por um período determinado que não deverá exceder os três meses.
- (138) A aplicação desse procedimento deverá ser condição de legalidade das medidas tomadas pelas autoridades de controlo que visem produzir efeitos legais nos casos em que a sua aplicação seja obrigatória. Noutros casos com dimensão transfronteiras, deverá ser aplicado o procedimento de cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas e a assistência mútua e as operações conjuntas poderão ser realizadas entre as autoridades de controlo interessadas, bilateral ou multilateralmente, sem desencadear o procedimento de controlo da coerência.
- (139) A fim de promover a aplicação coerente do presente regulamento, o Comité deverá ser um órgão independente da União. Para atingir os seus objetivos, o Comité deverá ser dotado de personalidade jurídica. O Comité é representado pelo seu presidente. Este Comité deverá substituir o Grupo de Trabalho sobre a proteção das pessoas no que diz respeito ao tratamento de dados pessoais instituído pelo artigo 29.º da Diretiva 95/46/CE. Deverá ser composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados ou pelos seus representantes. A Comissão deverá participar nas atividades do Comité, mas sem direito de voto, e a Autoridade Europeia para a Proteção de Dados deverá também participar nas suas atividades com direito de voto em casos particulares. O Comité deverá contribuir para a aplicação coerente do presente regulamento em toda a União, incluindo mediante o aconselhamento da Comissão, nomeadamente no que respeita ao nível de proteção em países terceiros ou em organizações internacionais, e mediante a promoção da cooperação das autoridades de controlo em toda a União. O Comité deverá ser independente na prossecução das suas atribuições.
- (140) O Comité deverá ser assistido por um secretariado disponibilizado pela Autoridade Europeia para a Proteção de Dados. O pessoal da Autoridade Europeia para a Proteção de Dados encarregado de exercer as funções conferidas ao Comité pelo presente regulamento deverá agir sob a direção exclusiva do presidente deste Comité, sendo responsável perante o mesmo.
- (141) Os titulares dos dados deverão ter direito a apresentar reclamação a uma única autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e direito a uma ação judicial efetiva, nos termos

do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se a autoridade de controlo não responder a uma reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas 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 de controlo deverá informar o titular dos dados do andamento e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser comunicadas informações intermédias ao titular dos dados. As autoridades de controlo deverão 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.

- (142) Se o titular dos dados considerar que os direitos que lhe são conferidos pelo presente regulamento foram violados, deverá ter o direito de mandar um organismo, organização ou associação sem fins lucrativos que seja constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam de interesse público e que exerça a sua atividade no domínio da proteção dos dados pessoais, para apresentar uma reclamação em seu nome junto de uma autoridade de controlo, ou exercer o direito de recurso judicial em nome dos titulares dos dados ou, se tal estiver previsto no direito de um Estado-Membro, exercer o direito à indemnização em nome dos titulares dos dados. Os Estados-Membros podem prever que esse organismo, organização ou associação tenha o direito de apresentar no Estado-Membro em causa uma reclamação, independentemente do mandato do titular dos dados, e o direito a um recurso judicial efetivo, se tiver razões para considerar que ocorreu uma violação dos direitos do titular dos dados por o tratamento dos dados pessoais violar o presente regulamento. Esse organismo, organização ou associação pode não ser autorizado a pedir uma indemnização em nome do titular dos dados independentemente do mandato que lhe é conferido por este.
- (143) Todas as pessoas singulares ou coletivas têm o direito de interpor recurso de anulação das decisões do Comité para o Tribunal de Justiça nas condições previstas no artigo 263.º do TFUE. Enquanto destinatárias dessas decisões, as autoridades de controlo interessadas que as pretendam contestar têm de interpor recurso no prazo de dois meses a contar da sua notificação, em conformidade com o artigo 263.º do TFUE. Se as decisões do Comité disserem direta e individualmente respeito a um responsável pelo tratamento, um subcontratante ou ao autor da reclamação, este pode interpor recurso de anulação dessas decisões no prazo de dois meses a contar da sua publicação no sítio *web* do Comité, em conformidade com o artigo 263.º do TFUE. Sem prejuízo do direito que lhes assiste ao abrigo do artigo 263.º do TFUE, todas as pessoas, singulares ou coletivas, deverão ter direito a interpor junto dos tribunais nacionais competentes recurso efetivo das decisões das autoridades de controlo que produzam efeitos jurídicos em relação a essas pessoas. Tais decisões dizem respeito, em especial, ao exercício de poderes de investigação, correção e autorização pelas autoridades de controlo ou à recusa ou rejeição de reclamações. Porém, o direito a um recurso judicial efetivo não abrange medidas tomadas pelas autoridades de controlo que não sejam juridicamente vinculativas, como os pareceres emitidos ou o aconselhamento prestado pela autoridade de controlo. Os recursos interpostos contra as autoridades de controlo deverão ser interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidas e obedecer às disposições processuais desse Estado-Membro. Estes tribunais deverão ter jurisdição plena, incluindo o poder de analisar todas as questões de facto e de direito relevantes para o litígio.

Se a autoridade de controlo recusar ou rejeitar uma reclamação, o seu autor pode intentar uma ação perante os tribunais do mesmo Estado-Membro. No contexto de recursos judiciais relacionados com a aplicação do presente regulamento, os tribunais nacionais que considerem que uma decisão sobre a matéria é necessária ao julgamento, poderão, ou, no caso previsto no artigo 267.º do TFUE, são mesmo obrigados a solicitar ao Tribunal de Justiça uma decisão prejudicial sobre a interpretação do direito da União, concretamente do presente regulamento. Além disso, se a decisão de uma autoridade de controlo que dá execução a uma decisão do Comité for contestada junto de um tribunal nacional e estiver em causa a validade desta última decisão, o tribunal nacional em questão não tem competência para a declarar inválida, devendo reenviar a questão da validade para o Tribunal de Justiça nos termos do artigo 267.º do TFUE, na interpretação que lhe dá este tribunal, quando considera a decisão inválida. No entanto, o tribunal nacional não pode reenviar a questão da validade da decisão do Comité a pedido de uma pessoa singular ou coletiva que, tendo a possibilidade de interpor recurso de anulação da mesma, sobretudo se for a destinatária direta e individual da decisão, não o tenha feito dentro do prazo fixado no artigo 263.º do TFUE.

- (144) Sempre que um tribunal chamado a pronunciar-se num recurso da decisão de uma autoridade de supervisão tiver motivos para crer que foi interposto perante um tribunal competente noutro Estado-Membro um processo relativo ao mesmo tratamento, designadamente o mesmo assunto no que se refere às atividades de tratamento do mesmo responsável ou subcontratante, ou ações com o mesmo pedido e a mesma causa de pedir, deverá contactar esse outro tribunal a fim de confirmar a existência de tal processo relacionado. Se estiverem pendentes

processos relacionados perante um tribunal de outro Estado-Membro, o tribunal em que a ação tiver sido intentada em segundo lugar poderá suspender o processo ou pode, a pedido de uma das partes, declarar-se incompetente a favor do tribunal em que a ação tiver sido intentada em primeiro lugar se este for competente para o processo em questão e a sua legislação permitir a apensação deste tipo de processos conexos. Consideram-se relacionados os processos ligados entre si por um nexo tão estreito que haja interesse em que sejam instruídos e julgados simultaneamente a fim de evitar soluções que poderiam ser inconciliáveis se as causas fossem julgadas separadamente.

- (145) No que diz respeito a ações intentadas contra o responsável pelo tratamento ou o subcontratante, o requerente pode optar entre intentar a ação nos tribunais do Estado-Membro em que está estabelecido o responsável ou o subcontratante, ou nos tribunais do Estado-Membro de residência do titular dos dados, salvo se o responsável pelo tratamento for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.
- (146) O responsável pelo tratamento ou o subcontratante deverão reparar quaisquer danos de que alguém possa ser vítima em virtude de um tratamento que viole o presente regulamento. O responsável pelo tratamento ou o subcontratante pode ser exonerado da responsabilidade se provar que o facto que causou o dano não lhe é de modo algum imputável. O conceito de dano deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça, de uma forma que reflita plenamente os objetivos do presente regulamento. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras do direito da União ou dos Estados-Membros. Os tratamentos que violem o presente regulamento abrangem igualmente os que violem os atos delegados e de execução adotados nos termos do presente regulamento e o direito dos Estados-Membros que dê execução a regras do presente regulamento. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido. Sempre que os responsáveis pelo tratamento ou os subcontratantes estiverem envolvidos no mesmo tratamento, cada um deles deverá ser responsabilizado pela totalidade dos danos causados. Porém, se os processos forem associados a um mesmo processo judicial, em conformidade com o direito dos Estados-Membros, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento ou subcontratante pelos danos causados em virtude do tratamento efetuado, na condição de ficar assegurada a indemnização integral e efetiva do titular dos dados pelos danos que tenha sofrido. Qualquer responsável pelo tratamento ou subcontratante que tenha pago uma indemnização integral, pode posteriormente intentar uma ação de regresso contra outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento.
- (147) Quando o presente regulamento previr regras específicas relativas à competência, nomeadamente no que respeita à interposição de recurso judicial, incluindo os pedidos de indemnização, contra um responsável pelo tratamento ou um subcontratante, a aplicação das regras específicas não deverá ser prejudicada por regras de competência gerais como as previstas no Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho <sup>(1)</sup>.
- (148) A fim de reforçar a execução das regras do presente regulamento, deverão ser impostas sanções, incluindo coimas, por violação do presente regulamento, para além, ou em substituição, das medidas adequadas que venham a ser impostas pela autoridade de controlo nos termos do presente regulamento. Em caso de infração menor, ou se o montante da coima suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma coima. Importa, porém, ter em devida conta a natureza, gravidade e duração da infração, o seu caráter doloso, as medidas tomadas para atenuar os danos sofridos, o grau de responsabilidade ou eventuais infrações anteriores, a via pela qual a infração chegou ao conhecimento da autoridade de controlo, o cumprimento das medidas ordenadas contra o responsável pelo tratamento ou subcontratante, o cumprimento de um código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções, incluindo coimas, deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta, incluindo a proteção jurídica eficaz e um processo equitativo.
- (149) Os Estados-Membros deverão poder definir as normas relativas às sanções penais aplicáveis por violação do presente regulamento, inclusive por violação das normas nacionais adotadas em conformidade com o presente regulamento, e dentro dos seus limites. Essas sanções penais podem igualmente prever a privação dos lucros auferidos em virtude da violação do presente regulamento. Contudo, a imposição de sanções penais por infração às referidas normas nacionais, bem como de sanções administrativas, não deverá implicar a violação do princípio *ne bis in idem*, conforme é interpretado pelo Tribunal de Justiça.
- (150) A fim de reforçar e harmonizar as sanções administrativas para violações do presente regulamento, as autoridades de controlo deverão ter competência para impor coimas. O presente regulamento deverá definir as

<sup>(1)</sup> Regulamento (UE) n.º 1215/2012 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2012, relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (JO L 351 de 20.12.2012, p. 1).

violações e o montante máximo e o critério de fixação do valor das coimas daí decorrentes, que deverá ser determinado pela autoridade de controlo competente, em cada caso individual, tendo em conta todas as circunstâncias relevantes da situação específica, ponderando devidamente, em particular, a natureza, a gravidade e a duração da violação e das suas consequências e as medidas tomadas para garantir o cumprimento das obrigações constantes do presente regulamento e para prevenir ou atenuar as consequências da infração. Sempre que forem impostas coimas a empresas, estas deverão ser entendidas como empresas nos termos dos artigos 101.º e 102.º do TFUE para esse efeito. Sempre que forem impostas coimas a pessoas que não sejam empresas, a autoridade de supervisão deverá ter em conta o nível geral de rendimentos no Estado-Membro, bem como a situação económica da pessoa em questão, no momento de estabelecer o montante adequado da coima. O procedimento de controlo da coerência pode ser utilizado igualmente para a promoção de uma aplicação coerente das coimas. Deverá caber aos Estados-Membros determinar se as autoridades públicas deverão estar sujeitas a coimas, e em que medida. A imposição de uma coima ou o envio de um aviso não afetam o exercício de outros poderes das autoridades de controlo ou a aplicação de outras sanções previstas no presente regulamento.

- (151) Os sistemas jurídicos da Dinamarca e da Estónia não conhecem as coimas tal como são previstas no presente regulamento. As regras relativas às coimas podem ser aplicadas de modo que a coima seja imposta, na Dinamarca, pelos tribunais nacionais competentes como sanção penal e, na Estónia, pela autoridade de controlo no âmbito de um processo por infração menor, na condição de tal aplicação das regras nestes Estados-Membros ter um efeito equivalente às coimas impostas pelas autoridades de controlo. Por esse motivo, os tribunais nacionais competentes deverão ter em conta a recomendação da autoridade de controlo que propõe a coima. Em todo o caso, as coimas impostas deverão ser efetivas, proporcionadas e dissuasivas.
- (152) Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do presente regulamento, os Estados-Membros deverão criar um sistema que preveja sanções efetivas, proporcionadas e dissuasivas. A natureza das sanções, penal ou administrativa, deverá ser determinada pelo direito do Estado-Membro.
- (153) O direito dos Estados-Membros deverá conciliar as normas que regem a liberdade de expressão e de informação, nomeadamente jornalística, académica, artística e/ou literária com o direito à proteção de dados pessoais nos termos do presente regulamento. O tratamento de dados pessoais para fins exclusivamente jornalísticos ou para fins de expressão académica, artística ou literária deverá estar sujeito à derrogação ou isenção de determinadas disposições do presente regulamento se tal for necessário para conciliar o direito à proteção dos dados pessoais com o direito à liberdade de expressão e de informação, tal como consagrado no artigo 11.º da Carta. Tal deverá ser aplicável, em especial, ao tratamento de dados pessoais no domínio do audiovisual e em arquivos de notícias e hemerotecas. Por conseguinte, os Estados-Membros deverão adotar medidas legislativas que prevejam as isenções e derrogações necessárias para o equilíbrio desses direitos fundamentais. Os Estados-Membros deverão adotar essas isenções e derrogações aos princípios gerais, aos direitos do titular dos dados, ao responsável pelo tratamento destes e ao subcontratante, à transferência de dados pessoais para países terceiros ou para organizações internacionais, às autoridades de controlo independentes e à cooperação e à coerência e a situações específicas de tratamento de dados. Se estas isenções ou derrogações divergirem de um Estado-Membro para outro, deverá ser aplicável o direito do Estado-Membro a que esteja sujeito o responsável pelo tratamento. A fim de ter em conta a importância da liberdade de expressão em qualquer sociedade democrática, há que interpretar de forma lata as noções associadas a esta liberdade, como por exemplo o jornalismo.
- (154) O presente regulamento permite tomar em consideração o princípio do direito de acesso do público aos documentos oficiais na aplicação do mesmo. O acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse dessas autoridades públicas ou organismos públicos deverão poder ser divulgados publicamente por tais autoridades ou organismos, se a divulgação estiver prevista no direito da União ou do Estado-Membro que lhes for aplicável. Essas legislações deverão conciliar o acesso do público aos documentos oficiais e a reutilização da informação do setor público com o direito à proteção dos dados pessoais e podem pois prever a necessária conciliação com esse mesmo direito nos termos do presente regulamento. A referência a autoridades e organismos públicos deverá incluir, nesse contexto, todas as autoridades ou outros organismos abrangidos pelo direito do Estado-Membro relativo ao acesso do público aos documentos. A Diretiva 2003/98/CE do Parlamento Europeu e do Conselho <sup>(1)</sup> não

<sup>(1)</sup> Diretiva 2003/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público (JO L 345 de 31.12.2003, p. 90).

modifica nem de modo algum afeta o nível de proteção das pessoas singulares relativamente ao tratamento de dados pessoais nos termos das disposições do direito da União ou do Estado-Membro, nem altera, em particular, as obrigações e direitos estabelecidos no presente regulamento. Em particular, a referida diretiva não deverá ser aplicável a documentos não acessíveis ou de acesso restrito por força dos regimes de acesso por motivos de proteção de dados pessoais nem a partes de documentos acessíveis por força desses regimes que contenham dados pessoais cuja reutilização tenha sido prevista na lei como incompatível com o direito relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

- (155) O direito do Estado-Membro ou as convenções coletivas (incluindo «acordos setoriais») podem prever regras específicas para o tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente no que respeita às condições em que os dados pessoais podem ser tratados no contexto laboral, com base no consentimento do assalariado, para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas por lei ou por convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no trabalho, de saúde e segurança no trabalho, e para efeitos de exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.
- (156) O tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, deverá ficar sujeito à garantia adequada dos direitos e 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, ou para fins de investigação científica 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). Os Estados-Membros deverão prever garantias adequadas para o tratamento dos dados pessoais para fins de arquivo de interesse público, ou fins de investigação científica ou histórica ou para fins estatísticos. Os Estados-Membros deverão ser autorizados a estabelecer, sob condições específicas e mediante garantias adequadas para o titular dos dados, especificações e derrogações dos requisitos de informação e direitos à retificação, ao apagamento dos dados pessoais, a ser esquecido, à limitação do tratamento e à portabilidade dos dados e de oposição aquando do tratamento de dados pessoais para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos. As condições e garantias em causa podem implicar procedimentos específicos para o exercício desses direitos por parte do titular de dados, se tal for adequado à luz dos fins visados pelo tratamento específico a par de medidas técnicas e organizativas destinadas a reduzir o tratamento de dados pessoais de acordo com os princípios da proporcionalidade e da necessidade. O tratamento de dados para fins científicos deverá igualmente respeitar outra legislação aplicável, tal como a relativa aos ensaios clínicos.
- (157) Combinando informações provenientes dos registos, os investigadores podem obter novos conhecimentos de grande valor relativamente a problemas médicos generalizados, como as doenças cardiovasculares, o cancro e a depressão. Com base nos registos, os resultados da investigação podem ser melhorados, já que assentam numa população mais ampla. No âmbito das ciências sociais, a investigação com base em registos permite que os investigadores adquiram conhecimentos essenciais sobre a correlação a longo prazo entre uma série de condições sociais, como o desemprego e o ensino, e outras condições de vida. Os resultados da investigação obtidos através de registos fornecem conhecimentos sólidos e de elevada qualidade, que podem servir de base para a elaboração e a execução de políticas assentes no conhecimento, para melhorar a qualidade de vida de uma quantidade de pessoas e a eficácia dos serviços sociais. A fim de facilitar a investigação científica, os dados pessoais podem ser tratados para fins de investigação científica, sob reserva do estabelecimento de condições e garantias adequadas no direito da União ou dos Estados-Membros.
- (158) Quando os dados pessoais sejam tratados para fins de arquivo, o presente regulamento deverá ser também aplicável, tendo em mente que não deverá ser aplicável a pessoas falecidas. As autoridades públicas ou os organismos públicos ou privados que detenham registos de interesse público deverão ser serviços que, nos termos do direito da União ou dos Estados-Membros, tenham a obrigação legal de adquirir, conservar, avaliar, organizar, descrever, comunicar, promover, divulgar e facultar o acesso a registos de valor duradouro no interesse público geral. Os Estados-Membros deverão também ser autorizados a determinar o posterior tratamento dos dados pessoais para efeitos de arquivo, por exemplo tendo em vista a prestação de informações específicas relacionadas com o comportamento político no âmbito de antigos regimes totalitários, genocídios, crimes contra a humanidade, em especial o Holocausto, ou crimes de guerra.

- (159) Quando os dados pessoais sejam tratados para fins de investigação científica, o presente regulamento deverá ser também aplicável. Para efeitos do presente regulamento, o tratamento de dados pessoais para fins de investigação científica deverá ser entendido em sentido lato, abrangendo, por exemplo, o desenvolvimento tecnológico e a demonstração, a investigação fundamental, a investigação aplicada e a investigação financiada pelo setor privado. Deverá, além disso, ter em conta o objetivo da União mencionado no artigo 179.º, n.º 1, do TFUE, que consiste na realização de um espaço europeu de investigação. Os fins de investigação científica deverão também incluir os estudos de interesse público realizados no domínio da saúde pública. A fim de atender às especificidades do tratamento de dados pessoais para fins de investigação científica, deverão ser aplicáveis condições específicas designadamente no que se refere à publicação ou outra forma de divulgação de dados pessoais no âmbito dos fins de investigação científica. Se o resultado da investigação científica designadamente no domínio da saúde justificar a tomada de novas medidas no interesse do titular dos dados, as normas gerais do presente regulamento deverão ser aplicáveis no que respeita a essas medidas.
- (160) Quando os dados pessoais sejam tratados para fins de investigação histórica, o presente regulamento deverá ser também aplicável. Deverá também incluir-se nesse âmbito a investigação histórica e a investigação para fins genealógicos, tendo em mente que o presente regulamento não deverá ser aplicável a pessoas falecidas.
- (161) Para efeitos do consentimento na participação em atividades de investigação científica em ensaios clínicos deverão ser aplicáveis as disposições relevantes do Regulamento (UE) n.º 536/2014 do Parlamento Europeu e do Conselho <sup>(1)</sup>.
- (162) Quando os dados pessoais sejam tratados para fins estatísticos, o presente regulamento deverá ser aplicável. O direito da União ou dos Estados-Membros deverá, dentro dos limites do presente regulamento, determinar o conteúdo estatístico, o controlo de acesso, as especificações para o tratamento de dados pessoais para fins estatísticos e as medidas adequadas para garantir os direitos e liberdades do titular dos dados e para assegurar o segredo estatístico. Por fins estatísticos entende-se todas as operações de recolha e de tratamento de dados pessoais necessárias à realização de estudos estatísticos ou à produção de resultados estatísticos. Esses resultados estatísticos podem ser utilizados posteriormente para fins diferentes, inclusive fins de investigação científica. No fim estatístico está implícito que os resultados do tratamento para esse fim não sejam já dados pessoais, mas dados agregados e que esses resultados ou os dados pessoais não sejam utilizados para justificar medidas ou decisões tomadas a respeito de uma pessoa singular.
- (163) Deverão ser protegidas as informações confidenciais que a União e as autoridades nacionais de estatística recolham para a produção de estatísticas oficiais europeias e nacionais. Deverão ser desenvolvidas, elaboradas e divulgadas estatísticas europeias de acordo com os princípios estatísticos enunciados no artigo 338.º, n.º 2, do TFUE, devendo as estatísticas nacionais cumprir também o disposto no direito do Estado-Membro. O Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho <sup>(2)</sup> fornece especificações suplementares em matéria de segredo estatístico aplicável às estatísticas europeias.
- (164) No que se refere aos poderes das autoridades de controlo para obter, junto do responsável pelo tratamento ou do subcontratante, o acesso aos dados pessoais e o acesso às suas instalações, os Estados-Membros podem adotar no seu ordenamento jurídico, dentro dos limites do presente regulamento, normas específicas que visem preservar o sigilo profissional ou outras obrigações equivalentes, na medida do necessário para conciliar o direito à proteção dos dados pessoais com a obrigação de sigilo profissional. Tal não prejudica as obrigações de adotar regras em matéria de sigilo profissional a que os Estados-Membros fiquem sujeitos por força do direito da União.
- (165) O presente regulamento respeita e não afeta o estatuto de que beneficiam, nos termos do direito constitucional vigente, as igrejas e associações ou comunidades religiosas nos Estados-Membros, reconhecido pelo artigo 17.º do TFUE.
- (166) A fim de cumprir os objetivos do presente regulamento, a saber, defender os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais, e assegurar a livre circulação

<sup>(1)</sup> Regulamento (UE) n.º 536/2014 do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativo aos ensaios clínicos de medicamentos para uso humano e que revoga a Diretiva 2001/20/CE (JO L 158 de 27.5.2014, p. 1).

<sup>(2)</sup> Regulamento (CE) n.º 223/2009 do Parlamento Europeu e do Conselho, de 11 de março de 2009, relativo às Estatísticas Europeias e que revoga o Regulamento (CE, Euratom) n.º 1101/2008 relativo à transmissão de informações abrangidas pelo segredo estatístico ao Serviço de Estatística das Comunidades Europeias, o Regulamento (CE) n.º 322/97 do Conselho relativo às estatísticas comunitárias e a Decisão 89/382/CEE, Euratom do Conselho que cria o Comité do Programa Estatístico das Comunidades Europeias (JO L 87 de 31.3.2009, p. 164).



desses dados na União, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão. Em especial, deverão ser adotados atos delegados em relação aos critérios e requisitos aplicáveis aos procedimentos de certificação, às informações a fornecer por meio de ícones normalizados e aos procedimentos aplicáveis ao fornecimento de tais ícones. É especialmente importante que a Comissão proceda a consultas adequadas ao longo dos seus trabalhos preparatórios, incluindo a nível de peritos. A Comissão, aquando da preparação e elaboração dos atos delegados, deverá assegurar o envio simultâneo, em tempo útil e em devida forma, dos documentos relevantes ao Parlamento Europeu e ao Conselho.

- (167) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão nos casos previstos no presente regulamento. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011. Nesse contexto, a Comissão deverá ponderar medidas específicas para as micro, pequenas e médias empresas.
- (168) O procedimento de exame deverá ser utilizado para a adoção de atos de execução em matéria de cláusulas contratuais-tipo entre os responsáveis pelo tratamento e os subcontratantes e entre subcontratantes; códigos de conduta; normas técnicas e procedimentos de certificação; nível de proteção adequado conferido por um país terceiro, um território ou um setor específico nesse país terceiro ou uma organização internacional; cláusulas normalizadas de proteção; formatos e procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas; assistência mútua; e regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité.
- (169) A Comissão deverá adotar atos de execução imediatamente aplicáveis quando haja elementos que comprovem que um país terceiro, um território ou um setor específico nesse país terceiro ou uma organização internacional não assegura um nível de proteção adequado, e imperativos urgentes assim o exigirem.
- (170) Atendendo a que o objetivo do presente regulamento, a saber, assegurar um nível equivalente de proteção das pessoas singulares e a livre circulação de dados pessoais na União, não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão e aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode adotar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia (TUE). Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.
- (171) A Diretiva 95/46/CE deverá ser revogada pelo presente regulamento. Os tratamentos de dados que se encontrem já em curso à data de aplicação do presente regulamento deverão passar a cumprir as suas disposições no prazo de dois anos após a data de entrada em vigor. Se o tratamento dos dados se basear no consentimento dado nos termos do disposto na Diretiva 95/46/CE, não será necessário obter uma vez mais o consentimento do titular dos dados, se a forma pela qual o consentimento foi dado cumprir as condições previstas no presente regulamento, para que o responsável pelo tratamento prossiga essa atividade após a data de aplicação do presente regulamento. As decisões da Comissão que tenham sido adotadas e as autorizações que tenham emitidas pelas autoridades de controlo com base na Diretiva 95/46/CE, permanecem em vigor até ao momento em que sejam alteradas, substituídas ou revogadas.
- (172) 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 7 de março de 2012 <sup>(1)</sup>.
- (173) O presente regulamento deverá aplicar-se a todas as matérias relacionadas com a defesa dos direitos e das liberdades fundamentais em relação ao tratamento de dados pessoais, não sujeitas a obrigações específicas com o mesmo objetivo, enunciadas na Diretiva 2002/58/CE do Parlamento Europeu e do Conselho <sup>(2)</sup>, incluindo as obrigações que incumbem ao responsável pelo tratamento e os direitos das pessoas singulares. A fim de clarificar a relação entre o presente regulamento e a Diretiva 2002/58/CE, esta última deverá ser alterada em conformidade. Uma vez adotado o presente regulamento, a Diretiva 2002/58/CE deverá ser revista, em especial a fim de assegurar a coerência com o presente regulamento,

<sup>(1)</sup> JO C 192 de 30.6.2012, p. 7.

<sup>(2)</sup> Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

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 e à livre circulação desses dados.
2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.
3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

#### *Artigo 2.º*

### **Âmbito de aplicação material**

1. O presente regulamento aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.
2. O presente regulamento não se aplica ao tratamento de dados pessoais:
  - a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
  - b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;
  - c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;
  - d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.
3. O Regulamento (CE) n.º 45/2001 aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 98.º.
4. O presente regulamento não prejudica a aplicação da Diretiva 2000/31/CE, nomeadamente as normas em matéria de responsabilidade dos prestadores intermediários de serviços previstas nos seus artigos 12.º a 15.º.

#### *Artigo 3.º*

### **Âmbito de aplicação territorial**

1. O presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União.

2. O presente regulamento aplica-se ao tratamento de dados pessoais de titulares residentes no território da União, efetuado por um responsável pelo tratamento ou subcontratante não estabelecido na União, quando as atividades de tratamento estejam relacionadas com:

a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento;

b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento estabelecido não na União, mas num lugar em que se aplique o direito de um Estado-Membro por força do direito internacional público.

#### Artigo 4.º

#### Definições

Para efeitos do presente regulamento, entende-se por:

- 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
- 2) «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;
- 3) «Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;
- 4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de 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;
- 5) «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 sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;
- 6) «Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;
- 7) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;
- 8) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;
- 9) «Destinatário», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades

públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou 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 finalidades do tratamento;

- 10) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais;
- 11) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;
- 12) «Violação de dados pessoais», uma violação da segurança que provoque, 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;
- 13) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;
- 14) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;
- 15) «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 revelem informações sobre o seu estado de saúde;
- 16) «Estabelecimento principal»:
  - a) No que se refere a um responsável pelo tratamento com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União, a menos que as decisões sobre as finalidades e os meios de tratamento dos dados pessoais sejam tomadas noutro estabelecimento do responsável pelo tratamento na União e este último estabelecimento tenha competência para mandar executar tais decisões, sendo neste caso o estabelecimento que tiver tomado as referidas decisões considerado estabelecimento principal;
  - b) No que se refere a um subcontratante com estabelecimentos em vários Estados-Membros, o local onde se encontra a sua administração central na União ou, caso o subcontratante não tenha administração central na União, o estabelecimento do subcontratante na União onde são exercidas as principais atividades de tratamento no contexto das atividades de um estabelecimento do subcontratante, na medida em que se encontre sujeito a obrigações específicas nos termos do presente regulamento;
- 17) «Representante», uma pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento ou subcontratante, nos termos do artigo 27.º, representa o responsável pelo tratamento ou o subcontratante no que se refere às suas obrigações respetivas nos termos do presente regulamento;
- 18) «Empresa», uma pessoa singular ou coletiva que, independentemente da sua forma jurídica, exerce uma atividade económica, incluindo as sociedades ou associações que exercem regularmente uma atividade económica;
- 19) «Grupo empresarial», um grupo composto pela empresa que exerce o controlo e pelas empresas controladas;
- 20) «Regras vinculativas aplicáveis às empresas», as regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento ou um subcontratante estabelecido no território de um Estado-Membro para as transferências ou conjuntos de transferências de dados pessoais para um responsável ou subcontratante num ou mais países terceiros, dentro de um grupo empresarial ou de um grupo de empresas envolvidas numa atividade económica conjunta;
- 21) «Autoridade de controlo», uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 51.º;

- 22) «Autoridade de controlo interessada», uma autoridade de controlo afetada pelo tratamento de dados pessoais pelo facto de:
- a) O responsável pelo tratamento ou o subcontratante estar estabelecido no território do Estado-Membro dessa autoridade de controlo;
  - b) Os titulares de dados que residem no Estado-Membro dessa autoridade de controlo serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados; ou
  - c) Ter sido apresentada uma reclamação junto dessa autoridade de controlo;
- 23) «Tratamento transfronteiriço»:
- a) O tratamento de dados pessoais que ocorre no contexto das atividades de estabelecimentos em mais do que um Estado-Membro de um responsável pelo tratamento ou um subcontratante na União, caso o responsável pelo tratamento ou o subcontratante esteja estabelecido em mais do que um Estado-Membro; ou
  - b) O tratamento de dados pessoais que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento ou de um subcontratante, mas que afeta substancialmente, ou é suscetível de afetar substancialmente, titulares de dados em mais do que um Estados-Membro;
- 24) «Objeção pertinente e fundamentada», uma objeção a um projeto de decisão que visa determinar se há violação do presente regulamento ou se a ação prevista relativamente ao responsável pelo tratamento ou ao subcontratante está em conformidade com o presente regulamento, demonstrando claramente a gravidade dos riscos que advêm do projeto de decisão para os direitos e liberdades fundamentais dos titulares dos dados e, eventualmente, para a livre circulação de dados pessoais no território da União;
- 25) «Serviços 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 <sup>(1)</sup>;
- 26) «Organização internacional», uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza.

## CAPÍTULO II

### **Princípios**

#### *Artigo 5.º*

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

1. Os dados pessoais são:
  - a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («licitude, lealdade e transparência»);
  - b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.º, n.º 1 («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 atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («exatidão»);

<sup>(1)</sup> 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).

- e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («limitação da conservação»);
  - f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»);
2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.º 1 e tem de poder comprová-lo («responsabilidade»).

#### Artigo 6.º

##### Licitude do tratamento

1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações:
- a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
  - b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados;
  - c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito;
  - d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
  - e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento;
  - f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica.

2. Os Estados-Membros podem manter ou aprovar disposições mais específicas com o objetivo de adaptar a aplicação das regras do presente regulamento no que diz respeito ao tratamento de dados para o cumprimento do n.º 1, alíneas c) e e), determinando, de forma mais precisa, requisitos específicos para o tratamento e outras medidas destinadas a garantir a licitude e lealdade do tratamento, inclusive para outras situações específicas de tratamento em conformidade com o capítulo IX.

3. O fundamento jurídico para o tratamento referido no n.º 1, alíneas c) e e), é definido:

- a) Pelo direito da União; ou
- b) Pelo direito do Estado-Membro ao qual o responsável pelo tratamento está sujeito.

A finalidade do tratamento é determinada com esse fundamento jurídico ou, no que respeita ao tratamento referido no n.º 1, alínea e), deve ser necessária ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento. Esse fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente: as condições gerais de licitude do tratamento pelo responsável pelo seu tratamento; os tipos de dados objeto de tratamento; os titulares dos dados em questão; as entidades a que os dados pessoais poderão ser comunicados e para que efeitos; os limites a que as finalidades do tratamento devem obedecer; os prazos de conservação; e as operações e procedimentos de tratamento, incluindo as medidas destinadas a garantir a legalidade e lealdade do tratamento, como as medidas relativas a outras situações

específicas de tratamento em conformidade com o capítulo IX. O direito da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

4. Quando o tratamento para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos não for realizado com base no consentimento do titular dos dados ou em disposições do direito da União ou dos Estados-Membros que constituam uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, o responsável pelo tratamento, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados pessoais foram inicialmente recolhidos, tem nomeadamente em conta:

- a) Qualquer ligação entre a finalidade para a qual os dados pessoais foram recolhidos e a finalidade do tratamento posterior;
- b) O contexto em que os dados pessoais foram recolhidos, em particular no que respeita à relação entre os titulares dos dados e o responsável pelo seu tratamento;
- c) A natureza dos dados pessoais, em especial se as categorias especiais de dados pessoais forem tratadas nos termos do artigo 9.º, ou se os dados pessoais relacionados com condenações penais e infrações forem tratados nos termos do artigo 10.º;
- d) As eventuais consequências do tratamento posterior pretendido para os titulares dos dados;
- e) A existência de salvaguardas adequadas, que podem ser a cifragem ou a pseudonimização.

#### Artigo 7.º

##### **Condições aplicáveis ao consentimento**

1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o 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 outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.
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. Quando for aplicável o artigo 6.º, n.º 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança.

Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos.

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

#### Artigo 9.º

#### **Tratamento de categorias especiais de dados pessoais**

1. É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
2. O disposto no n.º 1 não se aplica se se verificar um dos seguintes casos:
  - a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o n.º 1 não pode ser anulada pelo titular dos dados;
  - b) Se o tratamento for 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 ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;
  - c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
  - d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;
  - e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
  - f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;
  - g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
  - h) Se o tratamento for 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 dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no n.º 3;
  - i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;



- j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados.
3. Os dados pessoais referidos no n.º 1 podem ser tratados para os fins referidos no n.º 2, alínea h), se os dados forem tratados por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional, nos termos do direito da União ou 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 dos Estados-Membros ou de regulamentação estabelecida pelas autoridades nacionais competentes.
4. Os Estados-Membros podem manter ou impor novas condições, incluindo limitações, no que respeita ao tratamento de dados genéticos, dados biométricos ou dados relativos à saúde.

#### *Artigo 10.º*

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

O tratamento de dados pessoais relacionados com condenações penais e infrações ou com medidas de segurança conexas com base no artigo 6.º, n.º 1, só é efetuado sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito da União ou de um Estado-Membro que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados. Os registos completos das condenações penais só são conservados sob o controlo das autoridades públicas.

#### *Artigo 11.º*

### **Tratamento que não exige identificação**

1. Se as finalidades para as quais se proceder ao tratamento de dados pessoais não exigirem ou tiverem deixado de exigir a identificação do titular dos dados por parte do responsável pelo seu tratamento, este último não é obrigado a manter, obter ou tratar informações suplementares para identificar o titular dos dados com o único objetivo de dar cumprimento ao presente regulamento.
2. Quando, nos casos referidos no n.º 1 do presente artigo, o responsável pelo tratamento possa demonstrar que não está em condições de identificar o titular dos dados, informa-o, se possível, desse facto. Nesses casos, os artigos 15.º a 20.º não são aplicáveis, exceto se o titular dos dados, com a finalidade de exercer os seus direitos ao abrigo dos referidos artigos, fornecer informações adicionais que permitam a sua identificação.

## *CAPÍTULO III*

### **Direitos do titular dos dados**

#### *Secção 1*

### **Transparência e regras para o exercício dos direitos dos titulares dos dados**

#### *Artigo 12.º*

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

1. O responsável pelo tratamento toma as medidas adequadas para fornecer ao titular as informações a que se referem os artigos 13.º e 14.º e qualquer comunicação prevista nos artigos 15.º a 22.º e 34.º a respeito do tratamento, de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples, em especial quando as informações são dirigidas especificamente a crianças. As informações são prestadas por escrito ou por outros meios, incluindo, se for caso disso, por meios eletrónicos. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

2. O responsável pelo tratamento facilita o exercício dos direitos do titular dos dados nos termos dos artigos 15.º a 22.º. Nos casos a que se refere o artigo 11.º, n.º 2, o responsável pelo tratamento não pode recusar-se a dar seguimento ao pedido do titular no sentido de exercer os seus direitos ao abrigo dos artigos 15.º a 22.º, exceto se demonstrar que não está em condições de identificar o titular dos dados.

3. O responsável pelo tratamento fornece ao titular as informações sobre as medidas tomadas, mediante pedido apresentado nos termos dos artigos 15.º a 20.º, sem demora injustificada e no prazo de um mês a contar da data de receção do pedido. Esse prazo pode ser prorrogado até dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. O responsável pelo tratamento informa o titular dos dados de alguma 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 reclamação a uma autoridade de controlo e intentar ação judicial.

5. As informações fornecidas nos termos dos artigos 13.º e 14.º e quaisquer comunicações e medidas tomadas nos termos dos artigos 15.º a 22.º e 34.º são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, nomeadamente devido ao seu carácter repetitivo, o responsável pelo tratamento pode:

- a) Exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos do fornecimento das informações ou da comunicação, ou de tomada das medidas solicitadas; ou
- b) Recusar-se a dar seguimento ao pedido.

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

6. Sem prejuízo do artigo 11.º, quando o responsável pelo tratamento tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se referem os artigos 15.º a 21.º, pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.

7. As informações a fornecer pelos titulares dos dados nos termos dos artigos 13.º e 14.º podem ser dadas em combinação com ícones normalizados a fim de dar, de uma forma facilmente visível, inteligível e claramente legível, uma perspetiva geral significativa do tratamento previsto. Se forem apresentados por via eletrónica, os ícones devem ser de leitura automática.

8. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 92.º, a fim de determinar quais as informações a fornecer por meio dos ícones e os procedimentos aplicáveis ao fornecimento de ícones normalizados.

## Secção 2

### **Informação e acesso aos dados pessoais**

#### *Artigo 13.º*

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

1. Quando os dados pessoais forem recolhidos junto do titular, o responsável pelo tratamento faculta-lhe, aquando da recolha desses dados pessoais, as seguintes informações:

- a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- b) Os contactos do encarregado da proteção de dados, se for caso disso;
- c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;

- d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
- e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;
- f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, 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 fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

- a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse prazo;
- b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou o seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
- c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
- d) O direito de apresentar reclamação a uma autoridade de controlo;
- e) Se a comunicação de dados pessoais constitui ou não uma obrigação legal ou contratual, ou um requisito necessário para celebrar um contrato, bem como se o titular está obrigado a fornecer os dados pessoais e as eventuais consequências de não fornecer esses dados;
- f) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

3. Quando o responsável pelo tratamento pessoais tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes, nos termos do n.º 2.

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

#### Artigo 14.º

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

1. Quando os dados pessoais não forem recolhidos junto do titular, o responsável pelo tratamento fornece-lhe as seguintes informações:

- a) A identidade e os contactos do responsável pelo tratamento e, se for caso disso, do seu representante;
- b) Os contactos do encarregado da proteção de dados, se for caso disso;
- c) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico para o tratamento;
- d) As categorias dos dados pessoais em questão;
- e) Os destinatários ou categorias de destinatários dos dados pessoais, se os houver;

- f) Se for caso disso, o facto de o responsável pelo tratamento tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas nos artigos 46.º ou 47.º, ou no artigo 49.º, n.º 1, segundo parágrafo, 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 fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente:
- a) Prazo de conservação dos dados pessoais ou, se não for possível, os critérios usados para fixar esse prazo;
  - b) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento ou de um terceiro;
  - c) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a retificação ou o apagamento, ou a limitação do tratador no que disser respeito ao titular dos dados, e do direito de se opor ao tratamento, bem como do direito à portabilidade dos dados;
  - d) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea a), ou no artigo 9.º, n.º 2, alínea a), a existência do direito de retirar consentimento em qualquer altura, sem comprometer a licitude do tratamento efetuado com base no consentimento previamente dado;
  - e) O direito de apresentar reclamação a uma autoridade de controlo;
  - f) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;
  - g) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.
3. O responsável pelo tratamento comunica as informações referidas nos n.ºs 1 e 2:
- a) Num prazo razoável após a obtenção dos dados pessoais, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;
  - b) Se os dados pessoais se destinarem a ser utilizados para fins de comunicação com o titular dos dados, o mais tardar no momento da primeira comunicação ao titular dos dados; ou
  - c) Se estiver prevista a divulgação dos dados pessoais a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.
4. Quando o responsável pelo tratamento tiver a intenção de proceder ao tratamento posterior dos dados pessoais para um fim que não seja aquele para o qual os dados pessoais tenham sido obtidos, antes desse tratamento o responsável fornece ao titular dos dados informações sobre esse fim e quaisquer outras informações pertinentes referidas no n.º 2.
5. Os n.ºs 1 a 4 não se aplicam quando e na medida em que:
- a) O titular dos dados já tenha conhecimento das informações;
  - b) Se comprove a impossibilidade de disponibilizar a informação, ou que o esforço envolvido seja desproporcionado, nomeadamente para o tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, sob reserva das condições e garantias previstas no artigo 89.º, n.º 1, e na medida em que a obrigação referida no n.º 1 do presente artigo seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento. Nesses casos, o responsável pelo tratamento toma as medidas adequadas para defender os direitos, liberdades e interesses legítimos do titular dos dados, inclusive através da divulgação da informação ao público;
  - c) A obtenção ou divulgação dos dados esteja expressamente prevista no direito da União ou do Estado-Membro ao qual o responsável pelo tratamento estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses 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 ou de um Estado-Membro, inclusive uma obrigação legal de confidencialidade.

*Artigo 15.º***Direito de acesso do titular dos dados**

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

- a) As finalidades do tratamento dos dados;
- b) As categorias dos dados pessoais em questão;
- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
- d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, 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 reclamação a uma autoridade de controlo;
- g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
- h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

2. Quando os dados pessoais forem transferidos para um país terceiro ou uma organização internacional, o titular dos dados tem o direito de ser informado das garantias adequadas, nos termos do artigo 46.º relativo à transferência de dados.

3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrónicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrónico de uso corrente.

4. O direito de obter uma cópia a que se refere o n.º 3 não prejudica os direitos e as liberdades de terceiros.

*Secção 3***Retificação e apagamento***Artigo 16.º***Direito de retificação**

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

*Artigo 17.º***Direito ao apagamento dos dados («direito a ser esquecido»)**

1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

- a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;

- b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
- c) O titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21.º, n.º 2;
- d) Os dados pessoais foram tratados ilicitamente;
- e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
- f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

2. Quando o responsável pelo tratamento tiver tornado públicos os dados pessoais e for obrigado a apagá-los nos termos do n.º 1, toma as medidas que forem razoáveis, incluindo de caráter técnico, tendo em consideração a tecnologia disponível e os custos da sua aplicação, para informar os responsáveis pelo tratamento efetivo dos dados pessoais de que o titular dos dados lhes solicitou o apagamento das ligações para esses dados pessoais, bem como das cópias ou reproduções dos mesmos.

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

- a) Ao exercício da liberdade de expressão e de informação;
- b) Ao cumprimento de uma obrigação legal que exija o tratamento prevista pelo direito da União ou de um Estado-Membro a que o responsável esteja sujeito, ao exercício de funções de interesse público ou ao exercício da autoridade pública de que esteja investido o responsável pelo tratamento;
- c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e i), bem como do artigo 9.º, n.º 3;
- d) Para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos desse tratamento; ou
- e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

#### Artigo 18.º

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

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, se se aplicar uma das seguintes situações:

- a) Contestar a exatidão dos dados pessoais, durante um período que permita ao responsável pelo tratamento verificar a sua exatidão;
- b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização;
- c) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial;
- d) Se tiver oposto ao tratamento nos termos do artigo 21.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular dos dados.

2. Quando o tratamento tiver sido limitado nos termos do n.º 1, os dados pessoais só podem, à exceção da conservação, ser objeto de tratamento com o consentimento do titular, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial, de defesa dos direitos de outra pessoa singular ou coletiva, ou por motivos ponderosos de interesse público da União ou de um Estado-Membro.

3. O titular que tiver obtido a limitação do tratamento nos termos do n.º 1 é informado pelo responsável pelo tratamento antes de ser anulada a limitação ao referido tratamento.

#### *Artigo 19.º*

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

O responsável pelo tratamento comunica a cada destinatário a quem os dados pessoais tenham sido transmitidos qualquer retificação ou apagamento dos dados pessoais ou limitação do tratamento a que se tenha procedido em conformidade com o artigo 16.º, o artigo 17.º, n.º 1, e o artigo 18.º, salvo se tal comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o titular dos dados o solicitar, o responsável pelo tratamento fornece-lhe informações sobre os referidos destinatários.

#### *Artigo 20.º*

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

1. O titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido a um responsável pelo tratamento, num formato estruturado, de uso corrente e de leitura automática, e o direito de transmitir esses dados a outro responsável pelo tratamento sem que o responsável a quem os dados pessoais foram fornecidos o possa impedir, se:
  - a) O tratamento se basear no consentimento dado nos termos do artigo 6.º, n.º 1, alínea a), ou do artigo 9.º, n.º 2, alínea a), ou num contrato referido no artigo 6.º, n.º 1, alínea b); e
  - b) O tratamento for realizado por meios automatizados.
2. Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito a que os dados pessoais sejam transmitidos diretamente entre os responsáveis pelo tratamento, sempre que tal seja tecnicamente possível.
3. O exercício do direito a que se refere o n.º 1 do presente artigo aplica-se sem prejuízo do artigo 17.º. Esse direito não se aplica ao tratamento necessário para o exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento.
4. O direito a que se refere o n.º 1 não prejudica os direitos e as liberdades de terceiros.

#### *Secção 4*

### **Direito de oposição e decisões individuais automatizadas**

#### *Artigo 21.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 6.º, n.º 1, alínea e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim.

4. O mais tardar no momento da primeira comunicação ao titular dos dados, o direito a que se referem os n.ºs 1 e 2 é explicitamente levado à atenção do titular dos dados e é apresentado de modo claro e distinto de quaisquer outras informações.
5. No contexto da utilização dos serviços da sociedade da informação, e sem prejuízo da Diretiva 2002/58/CE, o titular dos dados pode exercer o seu direito de oposição por meios automatizados, utilizando especificações técnicas.
6. Quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, nos termos do artigo 89.º, n.º 1, 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 para a prossecução de atribuições de interesse público.

#### Artigo 22.º

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

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
2. O n.º 1 não se aplica se a decisão:
  - a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;
  - b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou
  - c) For baseada no consentimento explícito do titular dos dados.
3. Nos casos a que se referem o n.º 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.
4. As decisões a que se refere o n.º 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, a não ser que o n.º 2, alínea a) ou g), do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

#### Secção 5

##### **Limitações**

#### Artigo 23.º

##### **Limitações**

1. O direito da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 22.º e no artigo 34.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 22.º, desde que tal limitação respeite a essência dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada numa sociedade democrática para assegurar, designadamente:
  - a) A segurança do Estado;
  - b) A defesa;
  - c) A segurança pública;



- d) A prevenção, investigação, deteção ou repressão de infrações penais, ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;
  - e) Outros objetivos importantes do interesse público geral da União ou de um Estado-Membro, nomeadamente um interesse económico ou financeiro importante da União ou de um Estado-Membro, incluindo nos domínios monetário, orçamental ou fiscal, da saúde pública e da segurança social;
  - f) A defesa da independência judiciária e dos processos judiciais;
  - g) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;
  - h) 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 e) e g);
  - i) A defesa do titular dos dados ou dos direitos e liberdades de outrem;
  - j) A execução de ações cíveis.
2. Em especial, as medidas legislativas referidas no n.º 1 incluem, quando for relevante, disposições explícitas relativas, pelo menos:
- 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;
  - g) Aos riscos específicos para os direitos e liberdades dos titulares dos dados; e
  - h) Ao direito dos titulares dos dados a serem informados da limitação, a menos que tal possa prejudicar o objetivo da limitação.

#### CAPÍTULO IV

##### ***Responsável pelo tratamento e subcontratante***

##### Secção 1

##### **Obrigações gerais**

##### *Artigo 24.º*

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

1. Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.
2. Caso sejam proporcionadas em relação às atividades de tratamento, as medidas a que se refere o n.º 1 incluem a aplicação de políticas adequadas em matéria de proteção de dados pelo responsável pelo tratamento.
3. O cumprimento de códigos de conduta aprovados conforme referido no artigo 40.º ou de procedimentos de certificação aprovados conforme referido no artigo 42.º pode ser utilizada como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

*Artigo 25.º***Proteção de dados desde a conceção e por defeito**

1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.ºs 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42.º.

*Artigo 26.º***Responsáveis conjuntos pelo tratamento**

1. Quando dois ou mais responsáveis pelo tratamento determinem conjuntamente as finalidades e os meios desse tratamento, ambos são responsáveis conjuntos pelo tratamento. Estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.º e 14.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que se estejam sujeitos. O acordo pode designar um ponto de contacto para os titulares dos dados.
2. O acordo a que se refere o n.º 1 reflete devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. A essência do acordo é disponibilizada 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 lhe confere o presente regulamento em relação a cada um dos responsáveis pelo tratamento.

*Artigo 27.º***Representantes dos responsáveis pelo tratamento ou dos subcontratantes não estabelecidos na União**

1. Se for aplicável o artigo 3.º, n.º 2, o responsável pelo tratamento ou o subcontratante designa por escrito um representante seu na União.
2. A obrigação a que se refere o n.º 1 do presente artigo não se aplica:
  - a) Às operações de tratamento que sejam ocasionais, não abranjam o tratamento, em grande escala, de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou o tratamento de dados pessoais relativos a condenações penais e infrações referido no artigo 10.º, e não seja suscetível de implicar riscos para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento; ou
  - b) Às autoridades ou organismos públicos;

3. O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados cujos dados pessoais são objeto do tratamento no contexto da oferta que lhes é feita de bens ou serviços ou cujo comportamento é controlado.
4. Para efeitos do cumprimento do presente regulamento, o representante é mandatado pelo responsável pelo tratamento ou pelo subcontratante para ser contactado em complemento ou em substituição do responsável pelo tratamento ou do subcontratante, em especial por autoridades de controlo e por titulares, relativamente a todas as questões relacionadas com o tratamento.
5. A designação de um representante pelo responsável pelo tratamento ou pelo subcontratante não prejudica as ações judiciais que possam vir a ser intentadas contra o próprio responsável pelo tratamento ou o próprio subcontratante.

#### Artigo 28.º

#### Subcontratante

1. Quando o tratamento dos dados for efetuado por sua conta, o responsável pelo tratamento recorre apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do presente regulamento e assegure a defesa dos direitos do titular dos dados.
2. O subcontratante não contrata outro subcontratante sem que o responsável pelo tratamento tenha dado, previamente e por escrito, autorização específica ou geral. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.
3. O tratamento em subcontratação é regulado por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, e as obrigações e direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo estipulam, designadamente, que o subcontratante:
  - a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento, incluindo no que respeita às transferências de dados para países terceiros ou organizações internacionais, a menos que seja obrigado a fazê-lo pelo direito da União ou do Estado-Membro a que está sujeito, informando nesse caso o responsável pelo tratamento desse requisito jurídico antes do tratamento, salvo se a lei proibir tal informação por motivos importantes de interesse público;
  - b) Assegura que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou estão sujeitas a adequadas obrigações legais de confidencialidade;
  - c) Adota todas as medidas exigidas nos termos do artigo 32.º;
  - d) Respeita as condições a que se referem os n.ºs 2 e 4 para contratar outro subcontratante;
  - e) Toma em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento através de medidas técnicas e organizativas adequadas, para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados tendo em vista o exercício dos seus direitos previstos no capítulo III;
  - f) Presta assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das obrigações previstas nos artigos 32.º a 36.º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;
  - g) Consoante a escolha do responsável pelo tratamento, apaga ou devolve-lhe todos os dados pessoais depois de concluída a prestação de serviços relacionados com o tratamento, apagando as cópias existentes, a menos que a conservação dos dados seja exigida ao abrigo do direito da União ou dos Estados-Membros; e
  - h) Disponibiliza ao responsável pelo tratamento todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no presente artigo e facilita e contribui para as auditorias, inclusive as inspeções, conduzidas pelo responsável pelo tratamento ou por outro auditor por este mandatado.

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

4. Se o subcontratante contratar outro subcontratante para a realização de operações específicas de tratamento de dados por conta do responsável pelo tratamento, são impostas a esse outro subcontratante, por contrato ou outro ato normativo ao abrigo do direito da União ou dos Estados-Membros, as mesmas obrigações em matéria de proteção de dados que as estabelecidas no contrato ou outro ato normativo entre o responsável pelo tratamento e o subcontratante, referidas no n.º 3, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento seja conforme com os requisitos do presente regulamento. Se esse outro subcontratante não cumprir as suas obrigações em matéria de proteção de dados, o subcontratante inicial continua a ser plenamente responsável, perante o responsável pelo tratamento, pelo cumprimento das obrigações desse outro subcontratante.

5. O facto de o subcontratante cumprir um código de conduta aprovado conforme referido no artigo 40.º ou um procedimento de certificação aprovado conforme referido no artigo 42.º pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os n.ºs 1 e 4 do presente artigo.

6. Sem prejuízo de um eventual contrato individual entre o responsável pelo tratamento e o subcontratante, o contrato ou outro ato normativo referidos nos n.ºs 3 e 4 do presente artigo podem ser baseados, totalmente ou em parte, nas cláusulas contratuais-tipo referidas nos n.ºs 7 e 8 do presente artigo, inclusivamente quando fazem parte de uma certificação concedida ao responsável pelo tratamento ou ao subcontratante por força dos artigos 42.º e 43.º.

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 93.º, n.º 2.

8. A autoridade de controlo pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos n.ºs 3 e 4 do presente artigo e de acordo com o procedimento de controlo da coerência referido no artigo 63.º.

9. O contrato ou outro ato normativo a que se referem os n.ºs 3 e 4 devem ser feitos por escrito, incluindo em formato eletrónico.

10. Sem prejuízo do disposto nos artigos 82.º, 83.º e 84.º, o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento, é considerado responsável pelo tratamento no que respeita ao tratamento em questão.

#### *Artigo 29.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 exceto por instrução do responsável pelo tratamento, salvo se a tal for obrigado por força do direito da União ou dos Estados-Membros.

#### *Artigo 30.º*

### **Registos das atividades de tratamento**

1. Cada responsável pelo tratamento e, sendo caso disso, o seu representante conserva um registo de todas as atividades de tratamento sob a sua responsabilidade. Desse registo constam todas seguintes informações:

- a) O nome e os contactos do responsável pelo tratamento e, sendo caso disso, de qualquer responsável conjunto pelo tratamento, do representante do responsável pelo tratamento e do encarregado da proteção de dados;
- 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 países terceiros ou organizações internacionais;
  - e) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, 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 32.º, n.º 1.
2. Cada subcontratante e, sendo caso disso, o representante deste, conserva um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constará:
- a) O nome e contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento em nome do qual o subcontratante atua, bem como, sendo caso disso do representante do responsável pelo tratamento ou do subcontratante e do encarregado da proteção de dados;
  - b) As categorias de tratamentos de dados pessoais efetuados em nome de cada responsável pelo tratamento;
  - c) Se for aplicável, as transferências de dados pessoais para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 49.º, n.º 1, segundo parágrafo, 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 32.º, n.º 1.
3. Os registos a que se referem os n.ºs 1 e 2 são efetuados por escrito, incluindo em formato eletrónico.
4. O responsável pelo tratamento e, sendo caso disso, o subcontratante, o representante do responsável pelo tratamento ou do subcontratante, disponibilizam, a pedido, o registo à autoridade de controlo.
5. As obrigações a que se referem os n.ºs 1 e 2 não se aplicam às empresas ou organizações com menos de 250 trabalhadores, a menos que o tratamento efetuado seja suscetível de implicar um risco para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.º.

#### Artigo 31.º

### Cooperação com a autoridade de controlo

O responsável pelo tratamento e o subcontratante e, sendo caso disso, os seus representantes cooperam com a autoridade de controlo, a pedido desta, na prossecução das suas atribuições.

#### Secção 2

### Segurança dos dados pessoais

#### Artigo 32.º

#### Segurança do tratamento

1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

- a) A pseudonimização e a cifragem dos dados pessoais;

- b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
  - c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
  - d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.
3. O cumprimento de um código de conduta aprovado conforme referido no artigo 40.º ou de um procedimento de certificação aprovado conforme referido no artigo 42.º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo.
4. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro.

#### Artigo 33.º

##### **Notificação de uma violação de dados pessoais à autoridade de controlo**

1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.º, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.
3. A notificação referida no n.º 1 deve, pelo menos:
- a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;
  - b) Comunicar o nome e os contactos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
  - 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, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos;
4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.
5. O responsável pelo tratamento documenta quaisquer violações de dados pessoais, compreendendo os factos relacionados com as mesmas, os respetivos efeitos e a medida de reparação adotada. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.

#### Artigo 34.º

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

1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.

2. A comunicação ao titular dos dados a que se refere o n.º 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 33.º, n.º 3, alíneas b), c) e d).
3. A comunicação ao titular dos dados a que se refere o n.º 1 não é exigida se for preenchida uma das seguintes condições:
  - a) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;
  - b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1 já não é suscetível de se concretizar; ou
  - c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controlo, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições referidas no n.º 3.

### Secção 3

## **Avaliação de impacto sobre a proteção de dados e consulta prévia**

### *Artigo 35.º*

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

1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
2. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.
3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é obrigatória nomeadamente em caso de:
  - a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
  - b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º; ou
  - c) Controlo sistemático de zonas acessíveis ao público em grande escala.
4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do n.º 1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68.º.
5. A autoridade de controlo pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é obrigatória uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité.
6. Antes de adotar as listas a que se referem os n.ºs 4 e 5, a autoridade de controlo competente aplica o procedimento de controlo da coerência referido no artigo 63.º sempre que essas listas enunciem atividades de tratamento relacionadas com a oferta de bens ou serviços a titulares de dados ou com o controlo do seu comportamento em diversos Estados-Membros, ou possam afetar substancialmente a livre circulação de dados pessoais na União.

7. A avaliação inclui, pelo menos:
- a) Uma descrição sistemática das operações de tratamento previstas e a finalidade do tratamento, inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento;
  - b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos;
  - c) Uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados a que se refere o n.º 1; e
  - d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.
8. Ao avaliar o impacto das operações de tratamento efetuadas pelos responsáveis pelo tratamento ou pelos subcontratantes, em especial para efeitos de uma avaliação de impacto sobre a proteção de dados, é tido na devida conta o cumprimento dos códigos de conduta aprovados a que se refere o artigo 40.º por parte desses responsáveis ou subcontratantes.
9. Se for adequado, o responsável pelo tratamento solicita a opinião dos titulares de dados ou dos seus representantes sobre o tratamento previsto, sem prejuízo da defesa dos interesses comerciais ou públicos ou da segurança das operações de tratamento.
10. Se o tratamento efetuado por força do artigo 6.º, n.º 1, alínea c) ou e), tiver por fundamento jurídico o direito da União ou do Estado-Membro a que o responsável pelo tratamento está sujeito, e esse direito regular a operação ou as operações de tratamento específicas em questão, e se já tiver sido realizada uma avaliação de impacto sobre a proteção de dados no âmbito de uma avaliação de impacto geral no contexto da adoção desse fundamento jurídico, não são aplicáveis os n.ºs 1 a 7, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.
11. Se necessário, o responsável pelo tratamento procede a um controlo para avaliar se o tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados, pelo menos quando haja uma alteração dos riscos que as operações de tratamento representam.

#### Artigo 36.º

#### Consulta prévia

1. O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.
2. Sempre que considerar que o tratamento previsto referido no n.º 1 violaria o disposto no presente regulamento, nomeadamente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, no prazo máximo de oito semanas a contar da receção do pedido de consulta, dá orientações, por escrito, ao responsável pelo tratamento e, se o houver, ao subcontratante e pode recorrer a todos os seus poderes referidos no artigo 58.º. Esse prazo pode ser prorrogado até seis semanas, tendo em conta a complexidade do tratamento previsto. A autoridade de controlo informa da prorrogação o responsável pelo tratamento ou, se o houver, o subcontratante no prazo de um mês a contar da data de receção do pedido de consulta, juntamente com os motivos do atraso. Esses prazos podem ser suspensos até que a autoridade de controlo tenha obtido as informações que tenha solicitado para efeitos da consulta.
3. Quando consultar a autoridade de controlo nos termos do n.º 1, o responsável pelo tratamento comunica-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, nomeadamente no caso de um tratamento dentro de um grupo empresarial;
  - b) As finalidades e os meios do tratamento previsto;
  - c) As medidas e garantias previstas para defesa dos direitos e liberdades dos titulares dos dados nos termos do presente regulamento;
  - d) Se for aplicável, os contactos do encarregado da proteção de dados;



- e) A avaliação de impacto sobre a proteção de dados prevista no artigo 35.º; e
  - f) Quaisquer outras informações solicitadas pela autoridade de controlo.
4. Os Estados-Membros consultam a autoridade de controlo durante a preparação de uma proposta de medida legislativa a adotar por um parlamento nacional ou de uma medida regulamentar baseada nessa medida legislativa, que esteja relacionada com o tratamento de dados.
5. Não obstante o n.º 1, o direito dos Estados-Membros pode exigir que os responsáveis pelo tratamento consultem a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento por um responsável no exercício de uma missão de interesse público, incluindo o tratamento por motivos de proteção social e de saúde pública.

#### Secção 4

### **Encarregado da proteção de dados**

#### *Artigo 37.º*

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

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:
  - a) O tratamento for efetuado por uma autoridade ou um organismo público, excetuando os tribunais no exercício da sua função jurisdicional;
  - b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; ou
  - c) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento em grande escala de categorias especiais de dados nos termos do artigo 9.º e de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.º.
2. Um grupo empresarial pode também designar um único encarregado da proteção de dados desde que haja um encarregado da proteção de dados que seja facilmente acessível a partir de cada estabelecimento.
3. Quando o responsável pelo tratamento ou o subcontratante for uma autoridade ou um organismo público, pode ser designado um único encarregado da proteção de dados para várias dessas autoridades ou organismos, tendo em conta a respetiva estrutura organizacional e dimensão.
4. Em casos diferentes dos visados no n.º 1, o responsável pelo tratamento ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designar um encarregado da proteção de dados. O encarregado da proteção de dados pode agir em nome das associações e de outros organismos que representem os responsáveis pelo tratamento ou os subcontratantes.
5. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio do direito e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 39.º.
6. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.
7. O responsável pelo tratamento ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo.

#### *Artigo 38.º*

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

1. O responsável pelo tratamento e o subcontratante asseguram que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, a todas as questões relacionadas com a proteção de dados pessoais.

2. O responsável pelo tratamento e o subcontratante apoia o encarregado da proteção de dados no exercício das funções a que se refere o artigo 39.º, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, bem como dando-lhe acesso aos dados pessoais e às operações de tratamento.
3. O responsável pelo tratamento e o subcontratante asseguram que da proteção de dados não recebe instruções relativamente ao exercício das suas funções. O encarregado não pode ser destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante pelo facto de exercer as suas funções. O encarregado da proteção de dados informa diretamente a direção ao mais alto nível do responsável pelo tratamento ou do subcontratante.
4. Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todas questões relacionadas com o tratamento dos seus dados pessoais e com o exercício dos direitos que lhe são conferidos pelo presente regulamento.
5. O encarregado da proteção de dados está vinculado à obrigação de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados-Membros.
6. O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento ou o subcontratante assegura que essas funções e atribuições não resultam num conflito de interesses.

#### Artigo 39.º

### Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:
  - a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
  - b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
  - c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.º;
  - d) Cooperar com a autoridade de controlo;
  - e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.º, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.
2. No desempenho das suas funções, o encarregado da proteção de dados tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

#### Secção 5

### Códigos de conduta e certificação

#### Artigo 40.º

### Códigos de conduta

1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem a elaboração de códigos de conduta destinados a contribuir para a correta aplicação do presente regulamento, tendo em conta as características dos diferentes setores de tratamento e as necessidades específicas das micro, pequenas e médias empresas.
2. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento ou de subcontratantes podem elaborar códigos de conduta, alterar ou aditar a esses códigos, a fim de especificar a aplicação do presente regulamento, como por exemplo:
  - a) O tratamento equitativo e transparente;

- b) Os legítimos interesses dos responsáveis pelo tratamento em contextos específicos;
- c) A recolha de dados pessoais;
- d) A pseudonimização dos dados pessoais;
- e) A informação prestada ao público e aos titulares dos dados;
- f) O exercício dos direitos dos titulares dos dados;
- g) As informações prestadas às crianças e a sua proteção, e o modo pelo qual o consentimento do titular das responsabilidades parentais da criança deve ser obtido;
- h) As medidas e procedimentos a que se referem os artigos 24.º e 25.º e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.º;
- i) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações de dados pessoais aos titulares dos dados;
- j) A transferência de dados pessoais para países terceiros ou organizações internacionais; ou
- k) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento e os titulares dos dados em relação ao tratamento, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 77.º e 79.º.

3. Além dos responsáveis pelo tratamento ou dos subcontratantes sujeitos ao presente regulamento, também os responsáveis pelo tratamento ou subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.º podem cumprir códigos de conduta aprovados em conformidade com o n.º 5 do presente artigo e de aplicabilidade geral por força do n.º 9 do presente artigo, de modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.º, n.º 2, alínea e). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias apropriadas, inclusivamente em relação aos direitos dos titulares dos dados.

4. Os códigos de conduta referidos no n.º 2 do presente artigo devem prever procedimentos que permitam ao organismo referido no artigo 41.º, n.º 1, efetuar a supervisão obrigatória do cumprimento das suas disposições por parte dos responsáveis pelo tratamento ou subcontratantes que se comprometam a aplicá-lo, sem prejuízo das funções e competências das autoridades de controlo competentes por força do artigo 55.º ou 56.º.

5. As associações e outros organismos a que se refere o n.º 2 do presente artigo que tencionem elaborar um código de conduta, ou alterar ou aditar a um código existente, apresentam o projeto de código, a alteração ou o aditamento à autoridade de controlo que é competente por força do artigo 55.º. A autoridade de controlo emite um parecer sobre a conformidade do projeto de código de conduta ou da alteração ou do aditamento com o presente regulamento e aprova este projeto, esta alteração ou este aditamento se determinar que são previstas garantias apropriadas suficientes.

6. Se o código de conduta, ou a alteração ou o aditamento for aprovado nos termos do n.º 5, e se o código de conduta em causa não estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo regista e publica o código.

7. Se o projeto do código de conduta estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo competente nos termos do artigo 55.º, antes da aprovação, apresenta o projeto do código, a alteração ou o aditamento, pelo procedimento referido no artigo 63.º, ao Comité, que emite um parecer sobre a conformidade do projeto de código de conduta, ou da alteração ou do aditamento, com o presente regulamento, ou, na situação referida no n.º 3 do presente artigo, sobre a previsão de garantias adequadas.

8. Se o parecer a que se refere o n.º 7 confirmar que o projeto do código de conduta, ou a alteração ou o aditamento, está conforme com o presente regulamento ou, na situação referida no n.º 3, prevê garantias adequadas, o Comité apresenta o seu parecer à Comissão.

9. A Comissão pode, através de atos de execução, decidir que os códigos de conduta aprovados, bem como as alterações ou os aditamentos, que lhe sejam apresentados nos termos do n.º 8 do presente artigo, são de aplicabilidade geral na União. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

10. A Comissão assegura a publicidade adequada dos códigos aprovados que declarou, mediante decisão, serem de aplicabilidade geral em conformidade com o n.º 9.

11. O Comité recolhe todos os códigos de conduta aprovados, respetivas alterações e respetivos aditamentos num registo e disponibiliza-os ao público pelos meios adequados.

#### Artigo 41.º

##### **Supervisão dos códigos de conduta aprovados**

1. Sem prejuízo das funções e competências da autoridade de controlo competente ao abrigo dos artigos 57.º e 58.º, a supervisão de conformidade com um código de conduta nos termos do artigo 40.º pode ser efetuada por um organismo que tenha um nível adequado de competência relativamente ao objeto do código e esteja acreditado para o efeito pela autoridade de controlo competente.

2. O organismo a que se refere o n.º 1 pode ser acreditado para supervisão de conformidade com um código de conduta, se:

- a) Tiver demonstrado que goza de independência e dispõe dos conhecimentos necessários em relação ao objeto do código, de forma satisfatória para a autoridade de controlo competente;
- b) Tiver estabelecido procedimentos que lhe permitam avaliar a elegibilidade dos responsáveis pelo tratamento e dos subcontratantes em questão para aplicar o código, verificar se estes respeitam as disposições do mesmo e rever periodicamente o seu funcionamento;
- c) Tiver estabelecido procedimentos e estruturas para tratar reclamações relativas a violações do código ou à forma como o código tenha sido ou esteja a ser aplicado pelo responsável pelo tratamento ou subcontratante, e para tornar estes procedimentos e estruturas transparentes para os titulares dos dados e o público; e
- d) Demonstrar, de forma satisfatória para a autoridade de controlo competente, que as suas funções e atribuições não implicam um conflito de interesses.

3. A autoridade de controlo competente apresenta os projetos de critérios para a acreditação do organismo referido no n.º 1 do presente artigo ao Comité, de acordo com o procedimento de controlo da coerência referido no artigo 63.º.

4. Sem prejuízo das funções e competências da autoridade de controlo competente e do disposto no capítulo VIII, o organismo a que se refere o n.º 1 do presente artigo toma, sob reserva das garantias adequadas, as medidas que forem adequadas em caso de violações do código por um responsável pelo tratamento ou por um subcontratante, incluindo a suspensão ou exclusão desse responsável ou subcontratante do código. O referido organismo informa a autoridade de controlo competente dessas medidas e dos motivos que levaram à sua tomada.

5. A autoridade de controlo competente revoga a acreditação do organismo a que se refere o n.º 1 se as condições para a acreditação não estiverem ou tiverem deixado de estar reunidas, ou se as medidas tomadas pelo organismo violarem o presente regulamento.

6. O presente artigo não se aplica ao tratamento realizado por autoridades e organismos públicos.

#### Artigo 42.º

##### **Certificação**

1. Os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas.

2. Além do cumprimento pelos responsáveis pelo tratamento ou pelos subcontratantes sujeitos ao presente regulamento, os procedimentos de certificação em matéria de proteção de dados, bem como selos ou marcas aprovados de acordo com o n.º 5 do presente artigo também podem ser estabelecidos para efeitos de comprovação da existência de garantias adequadas fornecidas por responsáveis pelo tratamento ou por subcontratantes que não estão sujeitos ao presente regulamento por força do artigo 3.º no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 46.º, n.º 2, alínea f). Os responsáveis pelo tratamento ou os subcontratantes assumem compromissos vinculativos e com força executiva, por meio de instrumentos contratuais ou de outros instrumentos juridicamente vinculativos, no sentido de aplicar as garantias adequadas, inclusivamente em relação aos direitos dos titulares dos dados.
3. A certificação é voluntária e está disponível através de um processo transparente.
4. A certificação prevista no presente artigo não diminui a responsabilidade dos responsáveis pelo tratamento e subcontratantes pelo cumprimento do presente regulamento nem prejudica as funções e competências das autoridades de controlo competentes por força do artigo 55.º ou 56.º.
5. A certificação prevista no presente artigo é emitida pelos organismos de certificação referidos no artigo 43.º ou pela autoridade de controlo competente, com base nos critérios por esta aprovados por força do artigo 58.º, n.º 3, ou pelo Comité por força do artigo 63.º. Caso os critérios sejam aprovados pelo Comité, podem ter como resultado uma certificação comum, o Selo Europeu de Proteção de Dados.
6. Os responsáveis pelo tratamento ou subcontratantes que submetem o seu tratamento ao procedimento de certificação fornecem ao organismo de certificação a que se refere o artigo 43.º, ou, consoante o caso, à autoridade de controlo competente, todo o acesso às suas atividades de tratamento e toda a informação de que haja necessidade para efetuar o procedimento de certificação.
7. A certificação é emitida aos responsáveis pelo tratamento e subcontratantes por um período máximo de três anos e pode ser renovada nas mesmas condições, desde que os requisitos aplicáveis continuem a estar reunidos. A certificação é retirada, consoante o caso, pelos organismos de certificação referidos no artigo 43.º ou pela autoridade de controlo competente, se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos.
8. O Comité recolhe todos os procedimentos de certificação e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados.

#### Artigo 43.º

#### Organismos de certificação

1. Sem prejuízo das atribuições e poderes da autoridade de controlo competente nos termos dos artigos 57.º e 58.º, um organismo de certificação que tenha um nível adequado de competência em matéria de proteção de dados emite e renova a certificação, após informar a autoridade de controlo para que esta possa exercer as suas competências nos termos do artigo 58.º, n.º 2, alínea h), sempre que necessário. Os Estados-Membros asseguram que estes organismos de certificação são acreditados:
  - a) Pela autoridade de controlo que é competente nos termos do artigo 55.º ou 56.º;
  - b) Pelo organismo nacional de acreditação, designado nos termos do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho <sup>(1)</sup>, em conformidade com a norma EN-ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo que é competente nos termos do artigo 55.º ou 56.º.
2. Os organismos de certificação referidos no n.º 1 são acreditados em conformidade com o mesmo, apenas se:
  - a) Tiverem demonstrado que gozam de independência e dispõem dos conhecimentos necessários em relação ao objeto da certificação, de forma satisfatória para a autoridade de controlo competente;

<sup>(1)</sup> Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

- b) Se tiverem comprometido a respeitar os critérios referidos no artigo 42.º, n.º 5, e aprovados pela autoridade de controlo que é competente por força do artigo 55.º ou 56.º ou pelo Comité por força do artigo 63.º;
- c) Tiverem estabelecido procedimentos para a emissão, revisão periódica e retirada de procedimentos de certificação, selos e marcas de proteção de dados;
- d) Tiverem estabelecido procedimentos e estruturas para tratar reclamações relativas a violações da certificação ou à forma como a certificação tenha sido ou esteja a ser implementada pelo responsável pelo tratamento ou subcontratante, e para tornar estes procedimentos e estruturas transparentes para os titulares dos dados e o público; e
- e) Demonstrarem, de forma satisfatória para a autoridade de controlo competente, que as suas funções e atribuições não implicam um conflito de interesses.

3. A acreditação dos organismos de certificação referida nos n.ºs 1 e 2 do presente artigo, é efetuada com base nos critérios aprovados pela autoridade de controlo que é competente por força do artigo 55.º ou 56.º ou pelo Comité por força do artigo 63.º. No caso de acreditações nos termos do n.º 1, alínea b), do presente artigo, esses requisitos complementam os requisitos previstos no Regulamento (CE) n.º 765/2008 e as regras técnicas que descrevem os métodos e procedimentos dos organismos de certificação.

4. Os organismos de certificação a que se refere o n.º 1 são responsáveis pela correta avaliação necessária à certificação, ou pela revogação dessa certificação, sem prejuízo da responsabilidade que cabe ao responsável pelo tratamento ou ao subcontratante pelo cumprimento do presente regulamento. A acreditação é emitida por um período máximo de cinco anos e pode ser renovada nas mesmas condições, desde que o organismo de certificação reúna os requisitos estabelecidos no presente artigo.

5. Os organismos de certificação a que se refere o n.º 1 fornecem às autoridades de controlo competentes os motivos que levaram à concessão ou revogação da certificação solicitada.

6. Os requisitos referidos no n.º 3 do presente artigo, e os critérios referidos no artigo 42.º, n.º 5, são publicados pela autoridade de controlo sob uma forma facilmente acessível. As autoridades de controlo também comunicam estes requisitos e estas informações ao Comité. O Comité recolhe todos os procedimentos de certificação e selos de proteção de dados aprovados num registo e disponibiliza-os ao público por todos os meios adequados.

7. Sem prejuízo do capítulo VIII, a autoridade de controlo competente ou o organismo nacional de acreditação revoga uma acreditação do organismo de certificação nos termos do n.º 1 do presente artigo, se as condições para a acreditação não estiverem ou tiverem deixado de estar reunidas, ou se as medidas tomadas pelo organismo de certificação violarem o presente regulamento.

8. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 92.º, a fim de especificar os requisitos a ter em conta relativamente aos procedimentos de certificação em matéria de proteção de dados referidos no artigo 42.º, n.º 1.

9. A Comissão pode adotar atos de execução estabelecendo normas técnicas para os procedimentos de certificação e os selos e marcas em matéria de proteção de dados, e regras para promover e reconhecer esses procedimentos de certificação, selos e marcas. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

## CAPÍTULO V

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

#### *Artigo 44.º*

#### **Princípio geral das transferências**

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

## Artigo 45.º

**Transferências com base numa decisão de adequação**

1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional se a Comissão tiver decidido que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.
  2. Ao avaliar a adequação do nível de proteção, a Comissão tem nomeadamente em conta os seguintes elementos:
    - a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;
    - b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e
    - c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.
  3. Após avaliar a adequação do nível de proteção, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se for caso disso, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b), do presente artigo. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.
  4. A Comissão controla, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões adotadas nos termos do n.º 3 do presente artigo e das decisões adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE.
  5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.º 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.º 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3 do presente artigo, através de atos de execução, sem efeitos retroativos. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.
- Por imperativos de urgência devidamente justificados, a Comissão adota atos de execução imediatamente aplicáveis pelo procedimento a que se refere o artigo 93.º, n.º 3.
6. A Comissão inicia consultas com o país terceiro ou a organização internacional com vista a corrigir a situação que tiver dado origem à decisão tomada nos termos do n.º 5.
  7. As decisões tomadas ao abrigo do n.º 5 do presente artigo não prejudicam as transferências de dados pessoais para o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 46.º a 49.º.
  8. A Comissão publica no *Jornal Oficial da União Europeia* e no seu *sítio web* uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado.

9. As decisões adotadas pela Comissão com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o n.º 3 ou o n.º 5 do presente artigo.

#### Artigo 46.º

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

1. Não tendo sido tomada qualquer decisão nos termos do artigo 45.º, n.º 3, os responsáveis pelo tratamento ou subcontratantes só podem transferir dados pessoais para um país terceiro ou uma organização internacional se tiverem apresentado garantias adequadas, e na condição de os titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas eficazes.

2. Podem ser previstas as garantias adequadas referidas no n.º 1, sem requerer nenhuma autorização específica de uma autoridade de controlo, por meio de:

- a) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos;
- b) Regras vinculativas aplicáveis às empresas em conformidade com o artigo 47.º;
- c) Cláusulas-tipo de proteção de dados adotadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;
- d) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão pelo procedimento de exame referido no artigo 93.º, n.º 2;
- e) Um código de conduta, aprovado nos termos do artigo 40.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou
- f) Um procedimento de certificação, aprovado nos termos do artigo 42.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.

3. Sob reserva de autorização da autoridade de controlo competente, podem também ser previstas as garantias adequadas referidas no n.º 1, nomeadamente por meio de:

- a) Cláusulas contratuais entre os responsáveis pelo tratamento ou subcontratantes e os responsáveis pelo tratamento, subcontratantes ou destinatários dos dados pessoais no país terceiro ou 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. A autoridade de controlo aplica o procedimento de controlo da coerência a que se refere o artigo 63.º nos casos enunciados no n.º 3 do presente artigo.

5. As autorizações concedidas por um Estado-Membro ou uma autoridade de controlo com base no artigo 26.º, n.º 2, da Diretiva 95/46/CE continuam válidas até que a mesma autoridade de controlo as altere, substitua ou revogue, caso seja necessário. As decisões adotadas pela Comissão com base no artigo 26.º, n.º 4, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas, caso seja necessário, por uma decisão da Comissão adotada em conformidade com o n.º 2 do presente artigo.

#### Artigo 47.º

##### **Regras vinculativas aplicáveis às empresas**

1. Pelo procedimento de controlo da coerência previsto no artigo 63.º, a autoridade de controlo competente aprova regras vinculativas aplicáveis às empresas, que devem:

- a) Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento;



- b) Conferir expressamente aos titulares dos dados direitos oponíveis relativamente ao tratamento dos seus dados pessoais; e
  - c) Preencher os requisitos estabelecidos no n.º 2.
2. As regras vinculativas aplicáveis às empresas a que se refere o n.º 1 especificam, pelo menos:
- a) A estrutura e os contactos do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta e de cada uma das entidades que o compõe;
  - b) As transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão;
  - c) O seu carácter juridicamente vinculativo, a nível interno e externo;
  - d) A aplicação dos princípios gerais de proteção de dados, nomeadamente a limitação das finalidades, a minimização dos dados, a limitação dos prazos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, o fundamento jurídico para o tratamento, o tratamento de categorias especiais de dados pessoais, as medidas de garantia da segurança dos dados e os requisitos aplicáveis a transferências posteriores para organismos não abrangidos pelas regras vinculativas aplicáveis às empresas;
  - e) Os direitos dos titulares dos dados relativamente ao tratamento e regras de exercício desses direitos, incluindo o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado, nomeadamente a definição de perfis a que se refere o artigo 22.º, o direito de apresentar uma reclamação à autoridade de controlo competente e aos tribunais competentes dos Estados-Membros nos termos do artigo 79.º, bem como o de obter reparação e, se for caso disso, indemnização pela violação das regras vinculativas aplicáveis às empresas;
  - f) A aceitação, por parte do responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro, da responsabilidade por toda e qualquer violação das regras vinculativas aplicáveis às empresas cometida por uma entidade envolvida que não se encontre estabelecida na União; o responsável pelo tratamento ou o subcontratante só pode ser exonerado dessa responsabilidade, no todo ou em parte, mediante prova de que o facto que causou o dano não é imputável à referida entidade;
  - g) A forma como as informações sobre as regras vinculativas aplicáveis às empresas, nomeadamente, sobre as disposições referidas nas alíneas d), e) e f) do presente número, são comunicadas aos titulares dos dados para além das informações referidas nos artigos 13.º e 14.º;
  - h) As funções de qualquer encarregado da proteção de dados, designado nos termos do artigo 37.º ou de qualquer outra pessoa ou entidade responsável pelo controlo do cumprimento das regras vinculativas aplicáveis às empresas, a nível do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, e pela supervisão das ações de formação e do tratamento de reclamações;
  - i) Os procedimentos de reclamação;
  - j) Os procedimentos existentes no grupo empresarial ou no grupo de empresas envolvidas numa atividade económica conjunta para assegurar a verificação do cumprimento das regras vinculativas aplicáveis às empresas. Esses procedimentos incluem a realização de auditorias sobre a proteção de dados e o recurso a métodos que garantam a adoção de medidas corretivas capazes de preservar os direitos dos respetivos titulares. Os resultados dessa verificação devem ser comunicados à pessoa ou entidade referida na alínea h) e ao Conselho de Administração da empresa ou grupo empresarial que exerce o controlo ou do grupo de empresas envolvidas numa atividade económica conjunta, devendo também ser facultados à autoridade de controlo competente, a pedido desta;
  - k) Os procedimentos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controlo;
  - l) O procedimento de cooperação com a autoridade de controlo para assegurar o cumprimento, por qualquer entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta, em especial facultando à autoridade de controlo os resultados de verificações das medidas referidas na alínea j);
  - m) Os procedimentos de comunicação, à autoridade de controlo competente, de todos os requisitos legais a que uma entidade do grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas; e
  - n) Ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal.

3. A Comissão pode especificar o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas na aceção do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

#### Artigo 48.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 como base um acordo internacional, como um acordo de assistência judiciária mútua, em vigor entre o país terceiro em causa e a União ou um dos Estados-Membros, sem prejuízo de outros motivos de transferência nos termos do presente capítulo.

#### Artigo 49.º

### Derrogações para situações específicas

1. Na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, ou de garantias adequadas nos termos do artigo 46.º, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só são efetuadas caso se verifique uma das seguintes condições:

- a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas;
- b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados;
- c) A transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva;
- d) A transferência for necessária por importantes razões de interesse público;
- e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial;
- f) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento;
- g) A transferência for realizada a partir de um registo que, nos termos do direito da União ou do Estado-Membro, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito da União ou de um Estado-Membro se encontrem preenchidas nesse caso concreto.

Quando uma transferência não puder basear-se no disposto no artigo 45.º ou 46.º, incluindo nas regras vinculativas aplicáveis às empresas, e não for aplicável nenhuma das derrogações previstas para as situações específicas a que se refere o primeiro parágrafo do presente número, a transferência para um país terceiro ou uma organização internacional só pode ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares dos dados, for necessária para efeitos dos interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais. O responsável pelo tratamento informa da transferência a autoridade de controlo. Para além de fornecer a informação referida nos artigos 13.º e 14.º, o responsável pelo tratamento presta informações ao titular dos dados sobre a transferência e os interesses legítimos visados.

2. As transferências efetuadas nos termos do n.º 1, primeiro parágrafo, alínea g), não envolvem a totalidade dos dados pessoais nem categorias completas de dados pessoais constantes do registo. Quando o registo se destinar a ser consultado por pessoas com um interesse legítimo, as transferências só podem ser efetuadas a pedido dessas pessoas ou se forem elas os seus destinatários.

3. O n.º 1, primeiro parágrafo, alíneas a), b) e c), e segundo parágrafo, não é aplicável a atividades levadas a cabo por autoridades públicas no exercício dos seus poderes.
4. O interesse público referido no n.º 1, primeiro parágrafo, alínea d), é reconhecido pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento se encontre sujeito.
5. Na falta de uma decisão de adequação, o direito da União ou de um Estado-Membro podem, por razões importantes de interesse público, estabelecer expressamente limites à transferência de categorias específicas de dados para países terceiros ou organizações internacionais. Os Estados-Membros notificam a Comissão dessas disposições.
6. O responsável pelo tratamento ou o subcontratante documenta a avaliação, bem como as garantias adequadas referidas no n.º 1, segundo parágrafo, do presente artigo, nos registos a que se refere o artigo 30.º.

#### *Artigo 50.º*

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

Em relação a países terceiros e a organizações internacionais, a Comissão e as autoridades de controlo tomam as medidas necessárias para:

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

#### *CAPÍTULO VI*

### ***Autoridades de controlo independentes***

#### *Secção 1*

### **Estatuto independente**

#### *Artigo 51.º*

### **Autoridade de controlo**

1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União («autoridade de controlo»).
2. As autoridades de controlo contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de controlo cooperam entre si e com a Comissão, nos termos do capítulo VII.
3. Quando estiverem estabelecidas mais do que uma autoridade de controlo num Estado-Membro, este determina qual a autoridade de controlo que deve representar essas autoridades no Comité e estabelece disposições para assegurar que as regras relativas ao procedimento de controlo da coerência referido no artigo 63.º, sejam cumpridas pelas autoridades.
4. Os Estados-Membros notificam a Comissão das disposições do direito nacional que adotarem nos termos do presente capítulo, até 25 de maio de 2018 e, sem demora, de qualquer alteração posterior a essas mesmas disposições.

*Artigo 52.º***Independência**

1. As autoridades de controlo agem com total independência no na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do presente regulamento.
2. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem.
3. Os membros da autoridade de controlo abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.
4. Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comité.
5. Os Estados-Membros asseguram que cada autoridade de controlo selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controlo interessada.
6. Os Estados-Membros asseguram que cada autoridade de controlo fique sujeita a um controlo financeiro que não afeta a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional.

*Artigo 53.º***Condições gerais aplicáveis aos membros da autoridade de controlo**

1. Os Estados-Membros estabelecem que cada membro das respetivas autoridades de controlo seja nomeado por procedimento transparente:
  - pelo Parlamento,
  - pelo Governo,
  - pelo Chefe de Estado, ou
  - por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro.
2. Cada membro possui as habilitações, a experiência e os conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados pessoais, ao desempenho das suas funções e ao exercício dos seus poderes.
3. As funções dos membros da autoridade de controlo cessam findo o seu mandato, com a sua exoneração ou aposentação compulsiva, nos termos do direito do Estado-Membro em causa.
4. Os membros da autoridade de controlo só são exonerados se tiverem cometido uma falta grave ou se tiverem deixado de cumprir as condições exigidas para o exercício das suas funções.

*Artigo 54.º***Regras aplicáveis à constituição da autoridade de controlo**

1. Os Estados-Membros estabelecem, por via legislativa:
  - a) A constituição de cada autoridade de controlo;

- b) As qualificações e as condições de elegibilidade necessárias para a nomeação dos membros de cada autoridade de controlo;
- c) As regras e os procedimentos de nomeação dos membros de cada autoridade de controlo;
- d) A duração do mandato dos membros de cada autoridade de controlo, que não será inferior a quatro anos, salvo no caso do primeiro mandato após 24 de maio de 2016, e ser mais curta quando for necessário proteger a independência da autoridade de controlo através de um procedimento de nomeações escalonadas;
- e) Se, e em caso afirmativo, por quantos mandatos os membros de cada autoridade de controlo podem ser renomeados;
- f) As condições que regem as obrigações dos membros e do pessoal de cada autoridade de controlo, a proibição das ações, funções e benefícios que com elas são incompatíveis durante o mandato e após o seu termo e as regras que regem a cessação da relação de trabalho.

2. Os membros e o pessoal de cada autoridade de controlo ficam sujeitos, nos termos do direito da União ou dos Estados-Membros, à obrigação de sigilo profissional, tanto durante o mandato como após o seu termo, quanto a quaisquer informações confidenciais a que tenham tido acesso no desempenho das suas funções ou exercício dos seus poderes. Durante o seu mandato, essa obrigação de sigilo profissional aplica-se, em especial, à comunicação por pessoas singulares de violações do presente regulamento.

## Secção 2

### Competência, atribuições e poderes

#### Artigo 55.º

#### Competência

1. As autoridades de controlo são competentes para prosseguir as atribuições e exercer os poderes que lhes são conferidos pelo presente regulamento no território do seu próprio Estado-Membro.
2. Quando o tratamento for efetuado por autoridades públicas ou por organismos privados que atuem ao abrigo do artigo 6.º, n.º 1, alínea c) ou e), é competente a autoridade de controlo do Estado-Membro em causa. Nesses casos, não é aplicável o artigo 56.º.
3. As autoridades de controlo não têm competência para controlar operações de tratamento efetuadas por tribunais que atuem no exercício da sua função jurisdicional.

#### Artigo 56.º

### Competência da autoridade de controlo principal

1. Sem prejuízo do disposto no artigo 55.º, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento ou do subcontratante é competente para agir como autoridade de controlo principal para o tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante nos termos do artigo 60.º.
2. Em derrogação do n.º 1, cada autoridade de controlo é competente para tratar reclamações que lhe sejam apresentadas ou a eventuais violações do presente regulamento se a matéria em apreço estiver relacionada apenas com um estabelecimento no seu Estado-Membro ou se afetar substancialmente titulares de dados apenas no seu Estado-Membro.
3. Nos casos previstos no n.º 2 do presente artigo, a autoridade de controlo informa sem demora do assunto a autoridade de controlo principal. No prazo de três semanas a contar do momento em que tiver sido informada, a autoridade de controlo principal decide se trata o caso, nos termos do artigo 60.º, tendo em conta se há ou não algum estabelecimento do responsável pelo tratamento ou subcontratante no Estado-Membro sobre o qual a autoridade de controlo a tenha informado.

4. Quando a autoridade de controlo principal decide tratar o caso, aplica-se o procedimento previsto no artigo 60.º. A autoridade de controlo que tiver informado a autoridade de controlo principal pode apresentar a esta última um projeto de decisão. A autoridade de controlo principal tem esse projeto na melhor conta quando prepara o projeto de decisão referido no artigo 60.º, n.º 3.
5. Caso a autoridade de controlo principal decida não tratar o caso, é a autoridade de controlo que a informou que o trata, nos termos dos artigos 61.º e 62.º.
6. A autoridade de controlo principal é o único interlocutor do responsável pelo tratamento ou do subcontratante no tratamento transfronteiriço efetuado pelo referido responsável pelo tratamento ou subcontratante.

#### Artigo 57.º

#### Atribuições

1. Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controlo, no território respetivo:
  - a) Controla e executa a aplicação do presente regulamento;
  - b) Promove a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial;
  - c) Aconselha, em conformidade com o direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento;
  - d) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento;
  - e) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito;
  - f) Trata as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80.º, e investigar, na medida do necessário, o conteúdo da reclamação e informar o autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;
  - g) Coopera, incluindo partilhando informações e prestando assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento;
  - h) Conduz investigações sobre a aplicação do presente regulamento, incluindo com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;
  - i) Acompanha factos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, nomeadamente a evolução a nível das tecnologias da informação e das comunicações e das práticas comerciais;
  - j) Adota as cláusulas contratuais-tipo previstas no artigo 28.º, n.º 8, e no artigo 46.º, n.º 2, alínea d);
  - k) Elabora e conserva uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 35.º, n.º 4;
  - l) Dá orientações sobre as operações de tratamento previstas no artigo 36.º, n.º 2;
  - m) Incentiva a elaboração de códigos de conduta nos termos do artigo 40.º, n.º 1, dá parecer sobre eles e aprova os que preveem garantias suficientes, nos termos do artigo 40.º, n.º 5;
  - n) Incentiva o estabelecimento de procedimentos de certificação de proteção de dados, e de selos e marcas de proteção de dados, nos termos do artigo 42.º, n.º 1, e aprova os critérios de certificação nos termos do artigo 42.º, n.º 5;
  - o) Se necessário, procede a uma revisão periódica das certificações emitidas, nos termos do artigo 42.º, n.º 7;

- p) Redige e publica os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.º e de um organismo de certificação nos termos do artigo 43.º;
  - q) Conduz o processo de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 41.º e de um organismo de certificação nos termos do artigo 43.º;
  - r) Autoriza as cláusulas contratuais e disposições previstas no artigo 46.º, n.º 3;
  - s) Aprova as regras vinculativas aplicáveis às empresas nos termos do artigo 47.º;
  - t) Contribui para as atividades do Comité;
  - u) Conserva registos internos de violações do presente regulamento e das medidas tomadas nos termos do artigo 58.º, n.º 2; e
  - v) Desempenha quaisquer outras tarefas relacionadas com a proteção de dados pessoais.
2. As autoridades de controlo facilitam a apresentação das reclamações previstas no n.º 1, alínea f), tomando medidas como disponibilizar formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.
3. A prossecução das atribuições de cada autoridade de controlo é gratuita para o titular dos dados e, sendo caso disso, para o encarregado da proteção de dados.
4. Quando os pedidos forem manifestamente infundados ou excessivos, particularmente devido ao seu carácter recorrente, a autoridade de controlo pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos ou pode indeferirlos. Cabe à autoridade de controlo demonstrar o carácter manifestamente infundado ou excessivo dos pedidos.

#### Artigo 58.º

##### Poderes

1. Cada autoridade de controlo dispõe dos seguintes poderes de investigação:
- a) Ordenar que o responsável pelo tratamento e o subcontratante e, se existir, o seu representante, 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) Rever as certificações emitidas nos termos do artigo 42.º, n.º 7;
  - d) Notificar o responsável pelo tratamento ou o subcontratante de alegadas violações do presente regulamento;
  - e) Obter, da parte do responsável pelo tratamento e do subcontratante, acesso a todos os dados pessoais e a todas as informações necessárias ao exercício das suas funções;
  - f) Obter acesso a todas as instalações do responsável pelo tratamento e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito processual da União ou dos Estados-Membros.
2. Cada autoridade de controlo dispõe dos seguintes poderes de correção:
- a) Fazer advertências ao responsável pelo tratamento ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento;
  - b) Fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento;
  - c) Ordenar ao responsável pelo tratamento ou ao subcontratante que satisfaça os pedidos de exercício de direitos apresentados pelo titular dos dados nos termos do presente regulamento;

- d) Ordenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado;
- e) Ordenar ao responsável pelo tratamento que comunique ao titular dos dados uma violação de dados pessoais;
- f) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;
- g) Ordenar a retificação ou o apagamento de dados pessoais ou a limitação do tratamento nos termos dos artigos 16.º, 17.º e 18.º, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados pessoais nos termos do artigo 17.º, n.º 2, e do artigo 19.º;
- h) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 42.º e 43.º, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos;
- i) Impor uma coima nos termos do artigo 83.º, para além ou em vez das medidas referidas no presente número, consoante as circunstâncias de cada caso;
- j) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

3. Cada autoridade de controlo dispõe dos seguintes poderes consultivos e de autorização:

- a) Aconselhar o responsável pelo tratamento, pelo procedimento de consulta prévia referido no artigo 36.º;
- b) Emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao Parlamento nacional, ao Governo do Estado-Membro ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais;
- c) Autorizar o tratamento previsto no artigo 36.º, n.º 5, se a lei do Estado-Membro exigir tal autorização prévia;
- d) Emitir pareceres e aprovar projetos de códigos de conduta nos termos do artigo 40.º, n.º 5;
- e) Acreditar organismos de certificação nos termos do artigo 43.º;
- f) Emitir certificações e aprovar os critérios de certificação nos termos do artigo 42.º, n.º 5;
- g) Adotar as cláusulas-tipo de proteção de dados previstas no artigo 28.º, n.º 8, e no artigo 46.º, n.º 2, alínea d);
- h) Autorizar as cláusulas contratuais previstas no artigo 46.º, n.º 3, alínea a);
- i) Autorizar os acordos administrativos previstos no artigo 46.º, n.º 3, alínea b);
- j) Aprovar as regras vinculativas aplicáveis às empresas nos termos do artigo 47.º.

4. O exercício dos poderes conferidos à autoridade de controlo nos termos do presente artigo está sujeito a garantias adequadas, que incluem o direito à ação judicial efetiva e a um processo equitativo, previstas no direito da União e dos Estados-Membros, em conformidade com a Carta.

5. Os Estados-Membros estabelecem por lei que as suas autoridades de controlo estão habilitadas a levar as violações do presente regulamento ao conhecimento das autoridades judiciais e, se necessário, a intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições do presente regulamento.

6. Os Estados-Membros podem estabelecer por lei que as suas autoridades de controlo terão outros poderes para além dos previstos nos n.ºs 1, 2 e 3. O exercício desses poderes não deve prejudicar o efetivo funcionamento do capítulo VII.

#### Artigo 59.º

#### Relatórios de atividades

As autoridades de controlo elaboram um relatório anual de atividades, que pode incluir uma lista dos tipos de violação notificadas e dos tipos de medidas tomadas nos termos do artigo 58.º, n.º 2. Os relatórios são apresentados ao Parlamento nacional, ao Governo e às outras autoridades designadas no direito do Estado-Membro. Os relatórios são disponibilizados ao público, à Comissão e ao Comité.



## CAPÍTULO VII

**Cooperação e coerência**

## Secção 1

**Cooperação**

## Artigo 60.º

**Cooperação entre a autoridade de controlo principal e as outras autoridades de controlo interessadas**

1. A autoridade de controlo principal coopera com as outras autoridades de controlo interessadas nos termos do presente artigo para procurar alcançar um consenso. A autoridade de controlo principal e as autoridades de controlo interessadas trocam entre si todas as informações pertinentes.
2. A autoridade de controlo principal pode a qualquer momento solicitar que as outras autoridades de controlo interessadas prestem assistência mútua nos termos do artigo 61.º e pode realizar operações conjuntas nos termos do artigo 62.º, nomeadamente para proceder a investigações ou monitorizar a execução de medidas relativas a responsáveis pelo tratamento ou subcontratantes estabelecidos noutros Estados-Membros.
3. A autoridade de controlo principal comunica sem demora as informações pertinentes sobre o assunto às outras autoridades de controlo interessadas. Envia sem demora um projeto de decisão às outras autoridades de controlo interessadas para que emitam parecer e toma as suas posições em devida consideração.
4. Quando uma das outras autoridades de controlo interessadas expressa uma objeção pertinente e fundamentada ao projeto de decisão no prazo de quatro semanas após ter sido consultada nos termos do n.º 3 do presente artigo, a autoridade de controlo principal, caso não dê seguimento à objeção ou caso entenda que esta não é pertinente ou fundamentada, remete o assunto para o procedimento de controlo da coerência referido no artigo 63.º.
5. Se a autoridade de controlo principal pretender dar seguimento à objeção pertinente e fundamentada apresentada, envia às outras autoridades de controlo interessadas um projeto de decisão revisto para que emitam parecer. Esse projeto de decisão revisto é sujeito ao procedimento mencionado no n.º 4 no prazo de duas semanas.
6. Se nenhuma das outras autoridades de controlo interessadas se tiver oposto ao projeto de decisão apresentado pela autoridade de controlo principal no prazo referido nos n.ºs 4 e 5, considera-se que a autoridade de controlo principal e as autoridades de controlo interessadas estão de acordo com esse projeto de decisão e ficam por ela vinculadas.
7. A autoridade de controlo principal adota a decisão e dela notifica o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento ou do subcontratante, consoante o caso, e informa as outras autoridades de controlo interessadas e o Comité da decisão em causa, incluindo um sumário dos factos e motivos pertinentes. A autoridade de controlo à qual tenha sido apresentada uma reclamação, informa da decisão o autor da reclamação.
8. Em derrogação do n.º 7, se for recusada ou rejeitada uma reclamação, a autoridade de controlo à qual a reclamação tiver sido apresentada adota a decisão, notifica o autor da reclamação e informa desse facto o responsável pelo tratamento.
9. Se a autoridade de controlo principal e as autoridades de controlo interessadas estiverem de acordo em recusar ou rejeitar determinadas partes de uma reclamação e tomar medidas relativamente a outras partes da mesma reclamação, é adotada uma decisão separada para cada uma dessas partes da matéria. A autoridade de controlo principal adota a decisão na parte respeitante às medidas relativas ao responsável pelo tratamento e informa desse facto o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento ou do subcontratante no território do seu Estado-Membro, informando desse facto o autor da reclamação, enquanto a autoridade de controlo do autor da reclamação adota a decisão na parte relativa à recusa ou à rejeição da referida reclamação e notifica o autor da reclamação, informando desse facto o responsável pelo tratamento ou o subcontratante.
10. Após ter sido notificado da decisão da autoridade de controlo principal nos termos dos n.ºs 7 e 9, o responsável pelo tratamento ou o subcontratante tomam as medidas necessárias para garantir o cumprimento da decisão no que se refere às atividades de tratamento no contexto de todos os seus estabelecimentos na União. O responsável pelo tratamento ou o subcontratante comunica as medidas tomadas para fazer cumprir a decisão à autoridade de controlo principal, que informa as outras autoridades de controlo interessadas.

11. Se, em circunstâncias excecionais, alguma autoridade de controlo interessada tiver razões para considerar que existe uma necessidade urgente de agir para defender os interesses dos titulares dos dados, aplica-se o procedimento de urgência referido no artigo 66.º.

12. A autoridade de controlo principal e as outras autoridades de controlo interessadas trocam entre si as informações necessárias nos termos do presente artigo por meios eletrónicos, utilizando um formato normalizado.

#### Artigo 61.º

#### **Assistência mútua**

1. As autoridades de controlo prestam entre si informações úteis e assistência mútua a fim de executar e aplicar o presente regulamento de forma coerente, e tomam as medidas para cooperar eficazmente entre si. A assistência mútua abrange, em especial, os pedidos de informação e as medidas de controlo, tais como os pedidos de autorização prévia e de consulta prévia, bem como de inspeção e de investigação.

2. As autoridades de controlo tomam todas as medidas adequadas que forem necessárias para responder a um pedido de outra autoridade de controlo sem demora injustificada e, o mais tardar, um mês após a receção do pedido. Essas medidas podem incluir, particularmente, a transmissão de informações úteis sobre a condução de uma investigação.

3. Os pedidos de assistência incluem todas as informações necessárias, nomeadamente a finalidade e os motivos do pedido. As informações trocadas só podem ser utilizadas para a finalidade para que tiverem sido solicitadas.

4. A autoridade de controlo requerida não pode indeferir o pedido, a não ser que:

- a) Não seja competente relativamente ao assunto do pedido ou às medidas cuja execução lhe é pedida; ou
- b) Dar seguimento ao viole o presente regulamento ou o direito da União ou do Estado-Membro ao qual a autoridade de controlo que recebe o pedido está sujeita.

5. A autoridade de controlo requerida informa a autoridade de controlo requerente dos resultados obtidos ou, consoante o caso, do andamento do pedido ou das medidas tomadas para lhe dar resposta pedido. A autoridade de controlo requerida indica os motivos de indeferimento de um pedido por força do n.º 4.

6. As autoridades de controlo requeridas fornecem, em regra, as informações solicitadas por outras autoridades de controlo por meios eletrónicos, utilizando um formato normalizado.

7. As autoridades de controlo requeridas não cobram taxas pelas medidas por elas tomadas por força de pedidos de assistência mútua. As autoridades de controlo podem acordar regras para a indemnização recíproca de despesas específicas decorrentes da prestação de assistência mútua em circunstâncias excecionais.

8. Quando uma autoridade de controlo não prestar as informações referidas no n.º 5 do presente artigo no prazo de um mês a contar da receção do pedido apresentado por outra autoridade de controlo, a autoridade de controlo requerente pode adotar uma medida provisória no território do respetivo Estado-Membro nos termos do artigo 55.º, n.º 1. Nesse caso, presume-se que é urgente intervir, nos termos do artigo 66.º, n.º 1, e solicitar uma decisão vinculativa urgente ao Comité, nos termos do artigo 66.º, n.º 2.

9. A Comissão pode especificar, por meio de atos de execução, o formato e os procedimentos para a assistência mútua referidos no presente artigo, bem como as regras de intercâmbio por meios eletrónicos de informações entre as autoridades de controlo e entre estas e o Comité, nomeadamente o formato normalizado referido no n.º 6 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

#### Artigo 62.º

#### **Operações conjuntas das autoridades de controlo**

1. As autoridades de controlo conduzem, sempre que conveniente, operações conjuntas, incluindo investigações e medidas de execução conjuntas nas quais participem membros ou pessoal das autoridades de controlo de outros Estados-Membros.

2. Nos casos em que o responsável pelo tratamento ou o subcontratante tenha estabelecimentos em vários Estados-Membros ou nos casos em que haja um número significativo de titulares de dados em mais do que um Estado-Membro que sejam suscetíveis de ser substancialmente afetados pelas operações de tratamento, uma autoridade de controlo de cada um desses Estados-Membros tem direito a participar nas operações conjuntas. A autoridade de controlo competente nos termos do artigo 56.º, n.º 1 ou n.º 4, convida a autoridade de controlo de cada um desses Estados-Membros a participar nas operações conjuntas e responde sem demora ao pedido de uma autoridade de controlo para participar.
3. As autoridades de controlo podem, nos termos do direito do seu Estado-Membro, e com a autorização da autoridade de controlo de origem, conferir poderes, nomeadamente poderes de investigação, aos membros ou ao pessoal da autoridade de controlo de origem implicados nas operações conjuntas ou, na medida em que o direito do Estado-Membro da autoridade de controlo de acolhimento o permita, autorizar os membros ou o pessoal da autoridade de controlo de origem a exercer os seus poderes de investigação nos termos do direito do Estado-Membro da autoridade de controlo de origem. Esses poderes de investigação podem ser exercidos apenas sob a orientação e na presença de membros ou pessoal da autoridade de controlo de acolhimento. Os membros ou pessoal da autoridade de controlo de origem estão sujeitos ao direito do Estado-Membro da autoridade de controlo de acolhimento.
4. Se, nos termos do n.º 1, o pessoal da autoridade de controlo de origem exercer atividades noutro Estado-Membro, o Estado-Membro da autoridade de controlo de acolhimento assume a responsabilidade pelos seus atos, incluindo a responsabilidade por quaisquer danos por ele causados no decurso de tais atividades, de acordo com o direito do Estado-Membro em cujo território atuam.
5. O Estado-Membro em cujo território forem causados os danos indemniza-os nas condições aplicáveis aos danos causados pelo seu próprio pessoal. O Estado-Membro da autoridade de controlo de origem cujo pessoal tenha causado danos a qualquer pessoa no território de outro Estado-Membro reembolsa integralmente esse outro Estado-Membro das somas que tenha pago aos seus representantes legais.
6. Sem prejuízo do exercício dos seus direitos perante terceiros e com exceção do disposto no n.º 5, cada Estado-Membro renuncia, no caso previsto no n.º 1, a solicitar a outro Estado-Membro o reembolso do montante dos danos referido no n.º 4.
7. Sempre que se tencione efetuar uma operação conjunta e uma autoridade de controlo não cumprir, no prazo de um mês, a obrigação estabelecida no n.º 2, segunda frase, do presente artigo, as outras autoridades de controlo podem adotar uma medida provisória no território do respetivo Estado-Membro em conformidade com o artigo 55.º. Nesse caso, presume-se que é urgente intervir, nos termos do artigo 66.º, n.º 1, e solicitar um parecer ou uma decisão vinculativa urgente ao Comité, nos termos do artigo 66.º, n.º 2.

## Secção 2

### Coerência

#### Artigo 63.º

#### Procedimento de controlo da coerência

A fim de contribuir para a aplicação coerente do presente regulamento em toda a União, as autoridades de controlo cooperam entre si e, quando for relevante, com a Comissão, através do procedimento de controlo da coerência previsto na presente secção.

#### Artigo 64.º

#### Parecer do Comité

1. O Comité emite parecer sempre que uma autoridade de controlo competente tenha a intenção de adotar uma das medidas a seguir enunciadas. Para esse efeito, a autoridade de controlo competente envia o projeto de decisão ao Comité, quando esta:
  - a) Vise a adoção de uma lista das operações de tratamento sujeitas à exigência de proceder a uma avaliação do impacto sobre a proteção dos dados, nos termos do artigo 35.º, n.º 4;
  - b) Incida sobre uma questão, prevista no artigo 40.º, n.º 7, de saber se um projeto de código de conduta ou uma alteração ou aditamento a um código de conduta está em conformidade com o presente regulamento;

- c) Vise aprovar os critérios de acreditação de um organismo nos termos do artigo 41.º, n.º 3, ou um organismo de certificação nos termos do artigo 43.º, n.º 3;
  - d) Vise determinar as cláusulas-tipo de proteção de dados referidas no artigo 46.º, n.º 2, alínea d), e no artigo 28.º, n.º 8;
  - e) Vise autorizar as cláusulas contratuais previstas no artigo 46.º, n.º 3, alínea a); ou
  - f) Vise aprovar regras vinculativas aplicáveis às empresas na aceção do artigo 47.º.
2. As autoridades de controlo, o presidente do Comité ou a Comissão podem solicitar que o Comité analise qualquer assunto de aplicação geral ou que produza efeitos em mais do que um Estado-Membro, com vista a obter um parecer, nomeadamente se a autoridade de controlo competente não cumprir as obrigações em matéria de assistência mútua previstas no artigo 61.º ou de operações conjuntas previstas no artigo 62.º.
3. Nos casos referidos nos n.ºs 1 e 2, o Comité emite parecer sobre o assunto que lhe é apresentado, a não ser que tenha já antes emitido parecer sobre o mesmo assunto. Esse parecer é adotado no prazo de oito semanas por maioria simples dos membros que compõem o Comité. Esse prazo pode ser prorrogado por mais seis semanas, em virtude da complexidade do assunto em apreço. Para efeitos do projeto de decisão referido no n.º 1 e enviado aos membros do Comité nos termos do n.º 5, considera-se que os membros que não tenham levantado objeções dentro de um prazo razoável fixado pelo presidente estão de acordo com o projeto de decisão.
4. As autoridades de controlo e a Comissão comunicam sem demora injustificada, por via eletrónica, ao Comité, utilizando um formato normalizado, as informações que forem pertinentes, incluindo, consoante o caso, um resumo dos factos, o projeto de decisão, os motivos que tornam necessário adotar tal medida, bem como as posições das outras autoridades de controlo interessadas.
5. O presidente do Comité informa sem demora injustificada, por via eletrónica:
- a) Os membros do Comité e a Comissão de quaisquer informações pertinentes que lhe tenham sido comunicadas, utilizando um formato normalizado. Se necessário, o Secretariado do Comité fornece traduções das informações pertinentes; e
  - b) A autoridade de controlo referida, consoante o caso, nos n.ºs 1 e 2 e a Comissão do parecer e torna-o público.
6. As autoridades de controlo competentes não adotam os projetos de decisão referidos no n.º 1 no decurso do prazo referido no n.º 3.
7. A autoridade de controlo referida no n.º 1 tem na melhor conta o parecer do Comité e, no prazo de duas semanas a contar da receção do parecer, comunica por via eletrónica ao presidente do Comité se tenciona manter ou alterar o projeto de decisão e, se existir, o projeto de decisão alterado, utilizando um formato normalizado.
8. Quando as autoridades de controlo interessadas informarem o presidente do Comité, no prazo referido no n.º 7 do presente artigo, de que não têm intenção de seguir o parecer do Comité, no todo ou em parte, apresentando os motivos pertinentes de tal decisão, aplica-se o artigo 65.º, n.º 1.

#### *Artigo 65.º*

### **Resolução de litígios pelo Comité**

1. A fim de assegurar a aplicação correta e coerente do presente regulamento em cada caso, o Comité adota uma decisão vinculativa nos seguintes casos:
- a) Quando, num dos casos referidos no artigo 60.º, n.º 4, a autoridade de controlo interessada tiver suscitado uma objeção pertinente e fundamentada a um projeto de decisão da autoridade principal ou esta tiver rejeitado essa objeção por carecer de pertinência ou de fundamento. A decisão vinculativa diz respeito a todos os assuntos sobre que incida a referida objeção pertinente e fundamentada, sobretudo à questão de saber se há violação do presente regulamento;

- b) Quando haja posições divergentes sobre a questão de saber qual das autoridades de controlo interessadas é competente para o estabelecimento principal;
- c) Quando a autoridade de controlo competente não solicitar o parecer do Comité nos casos referidos no artigo 64.º, n.º 1, ou não seguir o parecer do Comité emitido nos termos do artigo 64.º. Nesse caso, qualquer autoridade de controlo interessada, ou a Comissão, pode remeter o assunto para o Comité.

2. A decisão a que se refere o n.º 1 é adotada por maioria de dois terços dos membros do Comité, no prazo de um mês a contar da data em que o assunto lhe é remetido. Este prazo pode ser prorrogado por mais um mês em virtude da complexidade do assunto em apreço. A decisão referida no n.º 1 é fundamentada e dirigida à autoridade de controlo principal, bem como a todas as autoridades de controlo interessadas, e é vinculativa para as partes.

3. Se não o puder fazer nos prazos referidos no n.º 2, o Comité adota a decisão no prazo de duas semanas a contar do termo do segundo mês a que se refere o n.º 2, por maioria simples dos membros que o compõem. Se houver empate na votação, a decisão é adotada pelo voto qualificado do presidente.

4. As autoridades de controlo interessadas não adotam decisão sobre a matéria submetida à apreciação do Comité nos termos do n.º 1 enquanto estiver a decorrer o prazo referido nos n.ºs 2 e 3.

5. O presidente do Comité informa, sem demora injustificada, as autoridades de controlo interessadas da decisão a que se refere o n.º 1. Do facto informa a Comissão. A decisão é imediatamente publicada no sítio *web* do Comité, depois de a autoridade de controlo ter notificado a decisão final a que se refere o n.º 6.

6. Sem demora injustificada e o mais tardar um mês depois de o Comité ter notificado a sua decisão, a autoridade de controlo principal ou, consoante o caso, a autoridade de controlo à qual tiver sido apresentada a reclamação adota a decisão final com base na decisão a que se refere o n.º 1 do presente artigo. A autoridade de controlo principal ou, consoante o caso, a autoridade de controlo à qual tiver sido apresentada a reclamação, informa o Comité da data em que a decisão final é notificada, respetivamente, ao responsável pelo tratamento ou ao subcontratante e ao titular. A decisão final das autoridades de controlo interessadas é adotada nos termos do artigo 60.º, n.ºs 7, 8 e 9. A decisão final remete para a decisão a que se refere o n.º 1 do presente artigo e especifica que a decisão referida no n.º 1 é publicada no sítio *web* do Comité nos termos do n.º 5 do presente artigo. A decisão final é acompanhada da decisão a que se refere o n.º 1 do presente artigo.

#### Artigo 66.º

#### Procedimento de urgência

1. Em circunstâncias excecionais, quando a autoridade de controlo interessada considerar que é urgente intervir a fim de defender os direitos e liberdades dos titulares dos dados, pode, em derrogação do procedimento de controlo da coerência referido nos artigos 63.º, 64.º e 65.º ou do procedimento a que se refere o artigo 60.º, adotar imediatamente medidas provisórias destinadas a produzir efeitos legais no seu próprio território, válidas por um período determinado que não seja superior a três meses. A autoridade de controlo dá sem demora conhecimento dessas medidas e dos motivos que a levaram a adotá-la às outras autoridades de controlo interessadas, ao Comité e à Comissão.

2. Quando a autoridade de controlo tiver tomado uma medida nos termos do n.º 1 e considerar necessário adotar urgentemente medidas definitivas, pode solicitar um parecer urgente ou uma decisão vinculativa urgente ao Comité, fundamentando o seu pedido de parecer ou decisão.

3. As autoridades de controlo podem solicitar um parecer urgente ou uma decisão vinculativa urgente, conforme o caso, ao Comité, quando a autoridade de controlo competente não tiver tomado nenhuma medida adequada numa situação que exija uma iniciativa urgente para defender os direitos e liberdades dos titulares dos dados, apresentando os motivos por que pede parecer ou decisão, e por que há necessidade urgente de agir.

4. Em derrogação do artigo 64.º, n.º 3, e do artigo 65.º, n.º 2, os pareceres urgentes ou decisões vinculativas urgentes a que se referem os n.ºs 2 e 3 do presente artigo são adotados no prazo de duas semanas por maioria simples dos membros do Comité.

*Artigo 67.º***Troca de informações**

Comissão pode adotar atos de execução de aplicação geral a fim de especificar as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité, nomeadamente o formato normalizado referido no artigo 64.º.

Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 93.º, n.º 2.

*Secção 3***Comité europeu para a proteção de dados***Artigo 68.º***Comité Europeu para a Proteção de Dados**

1. O Comité Europeu para a Proteção de Dados («Comité») é criado enquanto organismo da União e está dotado de personalidade jurídica.
2. O Comité é representado pelo seu presidente.
3. O Comité é composto pelo diretor de uma autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados, ou pelos respetivos representantes.
4. Quando, num determinado Estado-Membro, haja mais do que uma autoridade de controlo com responsabilidade pelo controlo da aplicação do presente regulamento, é nomeado um representante comum nos termos do direito desse Estado-Membro.
5. A Comissão tem o direito de participar nas atividades e reuniões do Comité, sem direito de voto. A Comissão designa um representante. O presidente do Comité informa a Comissão das atividades do Comité.
6. Nos casos referidos no artigo 65.º, a Autoridade Europeia para a Proteção de Dados apenas tem direito de voto nas decisões que digam respeito a princípios e normas aplicáveis às instituições, órgãos, organismos e agências da União que correspondam, em substância, às do presente regulamento.

*Artigo 69.º***Independência**

1. O Comité é independente na prossecução das suas atribuições ou no exercício dos seus poderes, nos termos dos artigos 70.º e 71.º.
2. Sem prejuízo dos pedidos da Comissão referidos no artigo 70.º, n.º 1, alínea b), e n.º 2, o Comité não solicita nem recebe instruções de outrem na prossecução das suas atribuições ou no exercício dos seus poderes.

*Artigo 70.º***Atribuições do Comité**

1. O Comité assegura a aplicação coerente do presente regulamento. Para o efeito, o Comité exerce, por iniciativa própria ou, nos casos pertinentes, a pedido da Comissão, as seguintes atividades:
  - a) Controla e assegura a correta aplicação do presente regulamento nos casos previstos nos artigos 64.º e 65.º, sem prejuízo das funções das autoridades nacionais de controlo;

- b) Aconselha a Comissão em todas as questões relacionadas com a proteção de dados pessoais na União, nomeadamente em qualquer projeto de alteração ao presente regulamento;
- c) Aconselha a Comissão sobre o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas;
- d) Emite diretrizes, recomendações e melhores práticas para os procedimentos de apagamento de ligações para os dados pessoais, de cópias ou reproduções desses dados existentes em serviços de comunicação acessíveis ao público, tal como previsto no artigo 17.º, n.º 2;
- e) Analisa, por iniciativa própria, a pedido de um dos seus membros da Comissão, qualquer questão relativa à aplicação do presente regulamento e emite diretrizes, recomendações e melhores práticas, a fim de incentivar a aplicação coerente do presente regulamento;
- f) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número, para definir mais concretamente os critérios e condições aplicáveis às decisões baseadas na definição de perfis, nos termos do artigo 22.º, n.º 2;
- g) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número, para definir violações de dados pessoais e determinar a demora injustificada a que se refere o artigo 33.º, n.ºs 1 e 2, bem como as circunstâncias particulares em que o responsável pelo tratamento ou o subcontratante é obrigado a notificar a violação de dados pessoais;
- h) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número, a respeito das circunstâncias em que as violações de dados pessoais são suscetíveis de resultar num risco elevado para os direitos e liberdades das pessoas singulares a que se refere o artigo 34.º, n.º 1;
- i) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número, para definir mais concretamente os critérios e requisitos aplicáveis às transferências de dados baseadas em regras vinculativas aplicáveis às empresas aceites pelos responsáveis pelo tratamento e em regras vinculativas aplicáveis às empresas aceites pelos subcontratantes, e outros requisitos necessários para assegurar a proteção dos dados pessoais dos titulares dos dados em causa a que se refere o artigo 47.º;
- j) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número para definir mais concretamente os critérios e requisitos aplicáveis à transferência de dados efetuadas com base no artigo 49.º, n.º 1;
- k) Elabora diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas a que se refere o artigo 58.º, n.ºs 1, 2 e 3, e de fixação de coimas nos termos do artigo 83.º;
- l) Examina a aplicação prática das diretrizes, recomendações e melhores práticas referidas nas alíneas e) e f);
- m) Emite diretrizes, recomendações e melhores práticas nos termos da alínea e) do presente número para definir procedimentos comuns para a comunicação por pessoas singulares de violações do presente regulamento, nos termos do artigo 54.º, n.º 2;
- n) Incentiva a elaboração de códigos de conduta e a criação de procedimentos de certificação, bem como de selos e marcas de proteção dos dados nos termos dos artigos 40.º e 42.º;
- o) Procede à acreditação dos organismos de certificação e à respetiva revisão periódica nos termos do artigo 43.º e conserva um registo público de organismos acreditados, nos termos do artigo 43.º, n.º 6, e de responsáveis pelo tratamento ou subcontratantes acreditados, estabelecidos em países terceiros, nos termos do artigo 42.º, n.º 7;
- p) Especifica os requisitos referidos no artigo 43.º, n.º 3, para acreditação dos organismos de certificação nos termos do artigo 42.º;
- q) Dá parecer à Comissão a respeito dos requisitos de certificação a que se refere o artigo 43.º, n.º 8;
- r) Dá parecer à Comissão sobre os símbolos a que se refere o artigo 12.º, n.º 7;
- s) Dá parecer à Comissão para a avaliação da adequação do nível de proteção num país terceiro ou organização internacional, e também para avaliar se um país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou uma organização internacional, deixou de garantir um nível adequado de proteção. Para esse efeito, a Comissão fornece ao Comité toda a documentação necessária, inclusive a correspondência com o Governo do país terceiro, relativamente a esse país terceiro, território ou setor específico, ou com a organização internacional;

- t) Emite pareceres relativos aos projetos de decisão das autoridades de controlo nos termos do procedimento de controlo da coerência referido no artigo 64.º, n.º 1, sobre os assuntos apresentados nos termos do artigo 64.º, n.º 2, e emite decisões vinculativas nos termos do artigo 65.º, incluindo nos casos referidos no artigo 66.º;
  - u) Promover a cooperação e o intercâmbio bilateral e plurilateral efetivo de informações e as melhores práticas entre as autoridades de controlo;
  - v) Promover programas de formação comuns e facilitar o intercâmbio de pessoal entre as autoridades de controlo, e, se necessário, com as autoridades de controlo de países terceiros ou com organizações internacionais;
  - w) Promover o intercâmbio de conhecimentos e de documentação sobre as práticas e a legislação no domínio da proteção de dados com autoridades de controlo de todo o mundo;
  - x) Emitir pareceres sobre os códigos de conduta elaborados a nível da União nos termos do artigo 40.º, n.º 9; e
  - y) Conservar um registo eletrónico, acessível ao público, das decisões tomadas pelas autoridades de controlo e pelos tribunais sobre questões tratadas no âmbito do procedimento de controlo da coerência.
2. Quando a Comissão consultar o Comité, pode indicar um prazo para a formulação do parecer, tendo em conta a urgência do assunto.
3. O Comité dirige os seus pareceres, diretrizes e melhores práticas à Comissão e ao comité referido no artigo 93.º, e procede à sua publicação.
4. Quando for caso disso, o Comité consulta as partes interessadas e dá-lhes a oportunidade de formular observações, num prazo razoável. Sem prejuízo do artigo 76.º, o Comité torna públicos os resultados do processo de consulta.

#### *Artigo 71.º*

### **Relatórios**

1. O Comité elabora um relatório anual sobre a proteção das pessoas singulares no que diz respeito ao tratamento na União e, quando for relevante, em países terceiros e organizações internacionais. O relatório é tornado público e enviado ao Parlamento Europeu, ao Conselho e à Comissão.
2. O relatório anual inclui uma análise da aplicação prática das diretrizes, recomendações e melhores práticas a que se refere o artigo 70.º, n.º 1, alínea l), bem como das decisões vinculativas a que se refere o artigo 65.º.

#### *Artigo 72.º*

### **Procedimento**

1. Salvo disposição em contrário do presente regulamento, o Comité decide por maioria simples dos seus membros.
2. O Comité adota o seu regulamento interno por maioria de dois terços dos membros que o compõem e determina as suas regras de funcionamento.

#### *Artigo 73.º*

### **Presidente**

1. O Comité elege de entre os seus membros, por maioria simples, um presidente e dois vice-presidentes.
2. O mandato do presidente e dos vice-presidentes tem a duração de cinco anos e é renovável uma vez.



*Artigo 74.º***Funções do presidente**

1. O presidente tem as seguintes funções:
  - a) Convoca as reuniões do Comité e prepara a respetiva ordem de trabalhos;
  - b) Comunica as decisões adotadas pelo Comité nos termos do artigo 65.º à autoridade de controlo principal e às autoridades de controlo interessadas;
  - c) Assegura o exercício das atribuições do Comité dentro dos prazos previstos, nomeadamente no que respeita ao procedimento de controlo da coerência referido no artigo 63.º.
2. O Comité estabelece a repartição de funções entre o presidente e os vice-presidentes no seu regulamento interno.

*Artigo 75.º***Secretariado**

1. O Comité dispõe de um secretariado disponibilizado pela Autoridade Europeia para a Proteção de Dados.
2. O secretariado desempenha as suas funções sob a direção exclusiva do presidente do Comité.
3. O pessoal da Autoridade Europeia para a Proteção de Dados envolvido na prossecução das atribuições conferidas ao Comité pelo presente regulamento está sujeito a uma hierarquia distinta do pessoal envolvido na prossecução das atribuições conferidas à Autoridade Europeia para a Proteção de Dados.
4. Quando for caso disso, o Comité e a Autoridade Europeia para a Proteção de Dados elaboram e publicam um memorando de entendimento que dê execução ao presente artigo e defina os termos da sua cooperação, aplicável ao pessoal da Autoridade Europeia para a Proteção de Dados envolvido na prossecução das atribuições conferidas ao Comité pelo presente regulamento.
5. O secretariado fornece ao Comité apoio de caráter analítico, administrativo e logístico.
6. O secretariado é responsável, em especial:
  - a) Pela gestão corrente do Comité;
  - b) Pela comunicação entre os membros do Comité, o seu presidente e a Comissão;
  - c) Pela comunicação com outras instituições e o público;
  - d) Pelo recurso a meios eletrónicos para a comunicação interna e externa;
  - e) Pela tradução de informações pertinentes;
  - f) Pela preparação e acompanhamento das reuniões do Comité;
  - g) Pela preparação, redação e publicação dos pareceres, das decisões em matéria de resolução de litígios entre autoridades de controlo e de outros textos adotados pelo Comité.

*Artigo 76.º***Confidencialidade**

1. Os debates do Comité são confidenciais quando o Comité o considerar necessário, nos termos do seu regulamento interno.

2. O acesso aos documentos apresentados aos membros do Comité, aos peritos e aos representantes de países terceiros é regido pelo Regulamento (CE) n.º 1049/2001 do Parlamento Europeu e do Conselho <sup>(1)</sup>.

#### CAPÍTULO VIII

### ***Vias de recurso, responsabilidade e sanções***

#### *Artigo 77.º*

#### **Direito de apresentar reclamação a uma autoridade de controlo**

1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, todos os titulares de dados têm direito a apresentar reclamação a uma autoridade de controlo, em especial no Estado-Membro da sua residência habitual, do seu local de trabalho ou do local onde foi alegadamente praticada a infração, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diga respeito viola o presente regulamento.
2. A autoridade de controlo à qual tiver sido apresentada a reclamação informa o autor da reclamação sobre o andamento e o resultado da reclamação, inclusive sobre a possibilidade de intentar ação judicial nos termos do artigo 78.º.

#### *Artigo 78.º*

#### **Direito à ação judicial contra uma autoridade de controlo**

1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todas as pessoas singulares ou coletivas têm direito à ação judicial contra as decisões juridicamente vinculativas das autoridades de controlo que lhes digam respeito.
2. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, os titulares dos dados têm direito à ação judicial se a autoridade de controlo competente nos termos dos artigos 55.º e 56.º não tratar a reclamação ou não informar o titular dos dados, no prazo de três meses, sobre o andamento ou o resultado da reclamação que tenha apresentado nos termos do artigo 77.º.
3. Os recursos contra as autoridades de controlo são interpostos nos tribunais do Estado-Membro em cujo território se encontrem estabelecidas.
4. Quando for interposto recurso de uma decisão de uma autoridade de controlo que tenha sido precedida de um parecer ou uma decisão do Comité no âmbito do procedimento de controlo da coerência, a autoridade de controlo transmite esse parecer ou decisão ao tribunal.

#### *Artigo 79.º*

#### **Direito à ação judicial contra um responsável pelo tratamento ou um subcontratante**

1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, nomeadamente o direito de apresentar reclamação a uma autoridade de controlo, nos termos do artigo 77.º, todos os titulares de dados têm direito à ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos do presente regulamento, na sequência do tratamento dos seus dados pessoais efetuado em violação do referido regulamento.
2. Os recursos contra os responsáveis pelo tratamento ou os subcontratantes são propostos nos tribunais do Estado-Membro em que tenham estabelecimento. Em alternativa, os recursos podem ser interpostos nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual, salvo se o responsável pelo tratamento ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.

<sup>(1)</sup> 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).

*Artigo 80.º***Representação dos titulares dos dados**

1. O titular dos dados tem o direito de mandar um organismo, organização ou associação sem fins lucrativos, que esteja devidamente constituído ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a defesa dos direitos e liberdades do titular dos dados no que respeita à proteção dos seus dados pessoais, para, em seu nome, apresentar reclamação, exercer os direitos previstos nos artigos 77.º, 78.º e 79.º, e exercer o direito de receber uma indemnização referido no artigo 82.º, se tal estiver previsto no direito do Estado-Membro.
2. Os Estados-Membros podem prever que o organismo, a organização ou a associação referidos no n.º 1 do presente artigo, independentemente de um mandato conferido pelo titular dos dados, tenham nesse Estado-Membro direito a apresentar uma reclamação à autoridade de controlo competente nos termos do artigo 77.º e a exercer os direitos a que se referem os artigos 78.º e 79.º, caso considerem que os direitos do titular dos dados, nos termos do presente regulamento, foram violados em virtude do tratamento.

*Artigo 81.º***Suspensão do processo**

1. Caso um tribunal de um Estado-Membro tenha informações sobre um processo pendente num tribunal de outro Estado-Membro, relativo ao mesmo assunto no que se refere às atividades de tratamento do mesmo responsável pelo tratamento ou subcontratante, deve contactar o referido tribunal desse outro Estado-Membro a fim de confirmar a existência de tal processo.
2. Caso esteja pendente num tribunal de outro Estado-Membro um processo relativo ao mesmo assunto no que se refere às atividades de tratamento do mesmo responsável pelo tratamento ou subcontratante, o tribunal onde a ação foi intentada em segundo lugar pode suspender o seu processo.
3. Caso o referido processo esteja pendente em primeira instância, o tribunal onde a ação foi intentada em segundo lugar pode igualmente declinar a sua competência, a pedido de uma das partes, se o órgão jurisdicional onde a ação foi intentada em primeiro lugar for competente para conhecer dos pedidos em questão e a sua lei permitir a respetiva apensação.

*Artigo 82.º***Direito de indemnização e responsabilidade**

1. Qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.
2. Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento. O subcontratante é responsável pelos danos causados pelo tratamento apenas se não tiver cumprido as obrigações decorrentes do presente regulamento dirigidas especificamente aos subcontratantes ou se não tiver seguido as instruções lícitas do responsável pelo tratamento.
3. O responsável pelo tratamento ou o subcontratante fica isento de responsabilidade nos termos do n.º 2, se provar que não é de modo algum responsável pelo evento que deu origem aos danos.
4. Quando mais do que um responsável pelo tratamento ou subcontratante, ou um responsável pelo tratamento e um subcontratante, estejam envolvidos no mesmo tratamento e sejam, nos termos dos n.ºs 2 e 3, responsáveis por eventuais danos causados pelo tratamento, cada responsável pelo tratamento ou subcontratante é responsável pela totalidade dos danos, a fim de assegurar a efetiva indemnização do titular dos dados.
5. Quando tenha pago, em conformidade com o n.º 4, uma indemnização integral pelos danos sofridos, um responsável pelo tratamento ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento ou subcontratantes envolvidos no mesmo tratamento a parte da indemnização correspondente à respetiva parte de responsabilidade pelo dano em conformidade com as condições previstas no n.º 2.

6. Os processos judiciais para exercer o direito de receber uma indemnização são apresentados perante os tribunais competentes nos termos do direito do Estado-Membro a que se refere o artigo 79.º, n.º 2.

### Artigo 83.º

#### Condições gerais para a aplicação de coimas

1. Cada autoridade de controlo assegura que a aplicação de coimas nos termos do presente artigo relativamente a violações do presente regulamento a que se referem os n.ºs 4, 5 e 6 é, em cada caso individual, efetiva, proporcionada e dissuasiva.

2. Consoante as circunstâncias de cada caso, as coimas são aplicadas para além ou em vez das medidas referidas no artigo 58.º, n.º 2, alíneas a) a h) e j). Ao decidir sobre a aplicação de uma coima e sobre o montante da coima em cada caso individual, é tido em devida consideração o seguinte:

- a) A natureza, a gravidade e a duração da infração tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos;
- b) O caráter intencional ou negligente da infração;
- c) A iniciativa tomada pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares;
- d) O grau de responsabilidade do responsável pelo tratamento ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 25.º e 32.º;
- e) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante;
- f) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos;
- g) As categorias específicas de dados pessoais afetadas pela infração;
- h) A forma como a autoridade de controlo tomou conhecimento da infração, em especial se o responsável pelo tratamento ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram;
- i) O cumprimento das medidas a que se refere o artigo 58.º, n.º 2, caso as mesmas tenham sido previamente impostas ao responsável pelo tratamento ou ao subcontratante em causa relativamente à mesma matéria;
- j) O cumprimento de códigos de conduta aprovados nos termos do artigo 40.º ou de procedimento de certificação aprovados nos termos do artigo 42.º; e
- k) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.

3. Se o responsável pelo tratamento ou o subcontratante violar, intencionalmente ou por negligência, no âmbito das mesmas operações de tratamento ou de operações ligadas entre si, várias disposições do presente regulamento, o montante total da coima não pode exceder o montante especificado para a violação mais grave.

4. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 10 000 000 EUR ou, no caso de uma empresa, até 2 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:

- a) As obrigações do responsável pelo tratamento e do subcontratante nos termos dos artigos 8.º, 11.º, 25.º a 39.º e 42.º e 43.º;
- b) As obrigações do organismo de certificação nos termos dos artigos 42.º e 43.º;
- c) As obrigações do organismo de supervisão nos termos do artigo 41.º, n.º 4;

5. A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante que for mais elevado:

- a) Os princípios básicos do tratamento, incluindo as condições de consentimento, nos termos dos artigos 5.º, 6.º, 7.º e 9.º;
- b) Os direitos dos titulares dos dados nos termos dos artigos 12.º a 22.º;
- c) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 44.º a 49.º;
- d) As obrigações nos termos do direito do Estado-Membro adotado ao abrigo do capítulo IX;
- e) O incumprimento de uma ordem de limitação, temporária ou definitiva, relativa ao tratamento ou à suspensão de fluxos de dados, emitida pela autoridade de controlo nos termos do artigo 58.º, n.º 2, ou o facto de não facultar acesso, em violação do artigo 58.º, n.º 1.

6. O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 58.º, n.º 2, está sujeito, em conformidade com o n.º 2 do presente artigo, a coimas até 20 000 000 EUR ou, no caso de uma empresa, até 4 % do seu volume de negócios anual a nível mundial correspondente ao exercício financeiro anterior, consoante o montante mais elevado.

7. Sem prejuízo dos poderes de correção das autoridades de controlo nos termos do artigo 58.º, n.º 2, os Estados-Membros podem prever normas que permitam determinar se e em que medida as coimas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território.

8. O exercício das competências que lhe são atribuídas pelo presente artigo por parte da autoridade de controlo fica sujeito às garantias processuais adequadas nos termos do direito da União e dos Estados-Membros, incluindo o direito à ação judicial e a um processo equitativo.

9. Quando o sistema jurídico dos Estados-Membros não preveja coimas, pode aplicar-se o presente artigo de modo a que a coima seja proposta pela autoridade de controlo competente e imposta pelos tribunais nacionais competentes, garantindo ao mesmo tempo que estas medidas jurídicas corretivas são eficazes e têm um efeito equivalente às coimas impostas pelas autoridades de controlo. Em todo o caso, as coimas impostas devem ser efetivas, proporcionadas e dissuasivas. Os referidos Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do presente número até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas.

#### Artigo 84.º

#### **Sanções**

1. Os Estados-Membros estabelecem as regras relativas às outras sanções aplicáveis em caso de violação do disposto no presente regulamento, nomeadamente às violações que não são sujeitas a coimas nos termos do artigo 7983.º, e tomam todas as medidas necessárias para garantir a sua aplicação. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

2. Os Estados-Membros notificam a Comissão das disposições do direito interno que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas.

#### CAPÍTULO IX

#### ***Disposições relativas a situações específicas de tratamento***

#### Artigo 85.º

#### **Tratamento e liberdade de expressão e de informação**

1. Os Estados-Membros conciliam por lei o direito à proteção de dados pessoais nos termos do presente regulamento com o direito à liberdade de expressão e de informação, incluindo o tratamento para fins jornalísticos e para fins de expressão académica, artística ou literária.

2. Para o tratamento efetuado para fins jornalísticos ou para fins de expressão académica, artística ou literária, os Estados-Membros estabelecem isenções ou derrogações do capítulo II (princípios), do capítulo III (direitos do titular dos dados), do capítulo IV (responsável pelo tratamento e subcontratante), do capítulo V (transferência de dados pessoais para países terceiros e organizações internacionais), do capítulo VI (autoridades de controlo independentes), do capítulo VII (cooperação e coerência) e do capítulo IX (situações específicas de tratamento de dados) se tais isenções ou derrogações forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação.

3. Os Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

#### *Artigo 86.º*

### **Tratamento e acesso do público aos documentos oficiais**

Os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para a prossecução de atribuições de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais nos termos do presente regulamento.

#### *Artigo 87.º*

### **Tratamento do número de identificação nacional**

Os Estados-Membros podem determinar em pormenor as condições específicas aplicáveis ao tratamento de um número de identificação nacional ou de qualquer outro elemento de identificação de aplicação geral. Nesse caso, o número de identificação nacional ou qualquer outro elemento de identificação de aplicação geral é exclusivamente utilizado mediante garantias adequadas dos direitos e liberdades do titular dos dados nos termos do presente regulamento.

#### *Artigo 88.º*

### **Tratamento no contexto laboral**

1. Os Estados-Membros podem estabelecer, no seu ordenamento jurídico ou em convenções coletivas, normas mais específicas para garantir a defesa dos direitos e liberdades no que respeita ao tratamento de dados pessoais dos trabalhadores no contexto laboral, nomeadamente para efeitos de recrutamento, execução do contrato de trabalho, incluindo o cumprimento das obrigações previstas no ordenamento jurídico ou em convenções coletivas, de gestão, planeamento e organização do trabalho, de igualdade e diversidade no local de trabalho, de saúde e segurança no trabalho, de proteção dos bens do empregador ou do cliente e para efeitos do exercício e gozo, individual ou coletivo, dos direitos e benefícios relacionados com o emprego, bem como para efeitos de cessação da relação de trabalho.

2. As normas referidas incluem medidas adequadas e específicas para salvaguardar a dignidade, os interesses legítimos e os direitos fundamentais do titular dos dados, com especial relevo para a transparência do tratamento de dados, a transferência de dados pessoais num grupo empresarial ou num grupo de empresas envolvidas numa atividade económica conjunta e os sistemas de controlo no local de trabalho.

3. Os Estados-Membros notificam a Comissão das disposições de direito interno que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas.

#### *Artigo 89.º*

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

1. O tratamento para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, está sujeito a garantias adequadas, nos termos do presente regulamento, para os direitos e liberdades do titular dos dados. Essas garantias asseguram a adoção de medidas técnicas e organizativas a fim de assegurar,

nomeadamente, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos desse modo. Sempre que esses fins possam ser atingidos por novos tratamentos que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins são atingidos desse modo.

2. Quando os dados pessoais sejam tratados para fins de investigação científica ou histórica ou para fins estatísticos, o direito da União ou dos Estados-Membros pode prever derrogações aos direitos a que se referem os artigos 15.º, 16.º, 18.º e 21.º, sob reserva das condições e garantias previstas no n.º 1 do presente artigo, na medida em que esses direitos sejam suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins específicos e que tais derrogações sejam necessárias para a prossecução desses fins.

3. Quando os dados pessoais sejam tratados para fins de arquivo de interesse público, o direito da União ou dos Estados-Membros pode prever derrogações aos direitos a que se referem os artigos 15.º, 16.º, 18.º, 19.º, 20.º e 21.º, sob reserva das condições e garantias previstas no n.º 1 do presente artigo, na medida em que esses direitos sejam suscetíveis de tornar impossível ou prejudicar gravemente a realização dos fins específicos e que tais derrogações sejam necessárias para a prossecução desses fins.

4. Quando o tratamento de dados previsto no n.ºs 2 e 3 também se destine, simultaneamente, a outros fins, as derrogações aplicam-se apenas ao tratamento de dados para os fins previstos nesses números.

#### Artigo 90.º

### Obrigações de sigilo

1. Os Estados-Membros podem adotar normas específicas para estabelecer os poderes das autoridades de controlo previstos no artigo 58.º, n.º 1, alíneas e) e f), relativamente a responsáveis pelo tratamento ou a subcontratantes sujeitos, nos termos do direito da União ou do Estado-Membro ou de normas instituídas pelos organismos nacionais competentes, a uma obrigação de sigilo profissional ou a outras obrigações de sigilo equivalentes, caso tal seja necessário e proporcionado para conciliar o direito à proteção de dados pessoais com a obrigação de sigilo. Essas normas são aplicáveis apenas no que diz respeito aos dados pessoais que o responsável pelo seu tratamento ou o subcontratante tenha recebido, ou que tenha recolhido no âmbito de uma atividade abrangida por essa obrigação de sigilo ou em resultado da mesma.

2. Os Estados-Membros notificam a Comissão das normas que adotarem nos termos do n.º 1, até 25 de maio de 2018 e, sem demora, de qualquer alteração subsequente das mesmas.

#### Artigo 91.º

### Normas vigentes em matéria de proteção dos dados das igrejas e associações religiosas

1. Quando, num Estado-Membro, as igrejas e associações ou comunidades religiosas apliquem, à data da entrada em vigor do presente regulamento, um conjunto completo de normas relativas à proteção das pessoas singulares relativamente ao tratamento, tais normas podem continuar a ser aplicadas, desde que cumpram o presente regulamento.

2. As igrejas e associações religiosas que apliquem um conjunto completo de normas nos termos do n.º 1 do presente artigo ficam sujeitas à supervisão de uma autoridade de controlo independente que pode ser específico, desde que cumpra as condições estabelecidas no capítulo VI do presente regulamento.

#### CAPÍTULO X

### Atos delegados e atos de execução

#### Artigo 92.º

### Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 12.º, n.º 8, e no artigo 43.º, n.º 8, é conferido à Comissão por tempo indeterminado a contar de 24 de maio de 2016.
3. A delegação de poderes referida no artigo 12.º, n.º 8, e no artigo 43.º, n.º 8, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou de uma data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.
4. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.
5. Os atos delegados adotados nos termos do artigo 12.º, n.º 8, e do artigo 43.º, n.º 8, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de três meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

#### Artigo 93.º

#### **Procedimento de comité**

1. A Comissão é assistida por um comité. 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.
3. Caso se remeta para o presente número, aplica-se o artigo 8.º do Regulamento (UE) n.º 182/2011, em conjugação com o seu artigo 5.º.

#### CAPÍTULO XI

#### **Disposições finais**

#### Artigo 94.º

#### **Revogação da Diretiva 95/46/CE**

1. A Diretiva 95/46/CE é revogada com efeitos a partir de 25 de maio de 2018.
2. As remissões para a diretiva revogada são consideradas remissões para presente regulamento. As referências ao Grupo de proteção das pessoas no que diz respeito ao tratamento de dados pessoais, criado pelo artigo 29.º da Diretiva 95/46/CE, são consideradas referências ao Comité Europeu para a Proteção de Dados criado pelo presente regulamento.

#### Artigo 95.º

#### **Relação com a Diretiva 2002/58/CE**

O presente regulamento não impõe obrigações suplementares a pessoas singulares ou coletivas no que respeita ao tratamento no contexto da prestação de serviços de comunicações eletrónicas disponíveis nas redes públicas de comunicações na União em matérias que estejam sujeitas a obrigações específicas com o mesmo objetivo estabelecidas na Diretiva 2002/58/CE.



*Artigo 96.º***Relação com acordos celebrados anteriormente**

Os acordos internacionais celebrados pelos Estados-Membros antes de 24 de maio de 2016, que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais e que sejam conformes com o direito da União aplicável antes dessa data, permanecem em vigor até serem alterados, substituídos ou revogados.

*Artigo 97.º***Relatórios da Comissão**

1. Até 25 de maio de 2020 e subsequentemente de quatro anos em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e revisão do presente regulamento. Os relatórios são tornados públicos.
2. No contexto das avaliações e revisões referidas no n.º 1, a Comissão examina, nomeadamente, a aplicação e o funcionamento do:
  - a) Capítulo V sobre a transferência de dados pessoais para países terceiros ou organizações internacionais, com especial destaque para as decisões adotadas nos termos do artigo 45.º, n.º 3, do presente regulamento, e as decisões adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE;
  - b) Capítulo VII sobre cooperação e coerência.
3. Para o efeito do n.º 1, a Comissão pode solicitar informações aos Estados-Membros e às autoridades de controlo.
4. Ao efetuar as avaliações e as revisões a que se referem os n.ºs 1 e 2, a Comissão tem em consideração as posições e as conclusões a que tenham chegado o Parlamento Europeu, o Conselho e outros organismos ou fontes pertinentes.
5. Se necessário, a Comissão apresenta propostas adequadas com vista à alteração do presente regulamento atendendo, em especial, à evolução das tecnologias da informação e aos progressos da Sociedade da Informação.

*Artigo 98.º***Revisão de outros atos jurídicos da União em matéria de proteção de dados**

Se necessário, a Comissão apresenta propostas legislativas com vista à alteração de outros atos jurídicos da União sobre a proteção dos dados pessoais, a fim de assegurar uma proteção uniforme e coerente das pessoas singulares no que diz respeito ao tratamento. Tal incide nomeadamente sobre as normas relativas à proteção das pessoas singulares no que diz respeito ao tratamento pelas instituições, órgãos, organismos e agências da União e a livre circulação desses dados.

*Artigo 99.º***Entrada em vigor e aplicação**

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

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

Feito em Bruxelas, em 27 de abril de 2016.

*Pelo Parlamento Europeu*

*O Presidente*

M. SCHULZ

*Pelo Conselho*

*A Presidente*

J.A. HENNIS-PLASSCHAERT

---

## DIRETIVAS

### 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**

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 das Regiões <sup>(1)</sup>,

Deliberando de acordo com o processo legislativo ordinário <sup>(2)</sup>,

Considerando o seguinte:

- (1) A proteção das pessoas singulares relativamente 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.
- (2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, particularmente o direito à proteção dos dados pessoais. A presente diretiva destina-se a contribuir para a realização de um espaço de liberdade, segurança e justiça.
- (3) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados pessoais registaram um aumento significativo. A tecnologia permite o tratamento de dados pessoais numa escala sem precedentes para o exercício de funções como a prevenção, investigação, deteção ou repressão de infrações penais e a execução de sanções penais.
- (4) A livre circulação de dados pessoais entre as autoridades competentes 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 nível da União, e a sua transferência para países terceiros e organizações internacionais deverão ser facilitadas, assegurando simultaneamente um elevado nível de proteção dos dados pessoais. Este contexto obriga ao estabelecimento de um regime de proteção de dados pessoais sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras.
- (5) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho <sup>(3)</sup> é aplicável a todos os tratamentos de dados pessoais nos Estados-Membros, nos setores público e privado. Não é, porém, aplicável ao tratamento de dados pessoais «no exercício de atividades não sujeitas à aplicação do direito comunitário», como as atividades realizadas nos domínios da cooperação judiciária em matéria penal e da cooperação policial.

<sup>(1)</sup> JO C 391 de 18.12.2012, p. 127.

<sup>(2)</sup> Posição do Parlamento Europeu de 12 de março de 2014 (ainda não publicada no Jornal Oficial) e posição do Conselho em primeira leitura de 8 de abril de 2016 (ainda não publicada no Jornal Oficial). Posição do Parlamento Europeu de 14 de abril de 2016.

<sup>(3)</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

- (6) A Decisão-Quadro 2008/977/JAI do Conselho <sup>(1)</sup> é aplicável no domínio da cooperação judiciária em matéria penal e da cooperação policial. O seu âmbito de aplicação limita-se ao tratamento de dados pessoais transmitidos ou disponibilizados entre Estados-Membros.
- (7) É crucial assegurar um nível elevado e coerente de proteção dos dados pessoais das pessoas singulares e facilitar o intercâmbio de dados pessoais entre as autoridades competentes dos Estados-Membros, a fim de assegurar a eficácia da cooperação judiciária em matéria penal e da cooperação policial. Para tal, o nível de proteção dos direitos e liberdades individuais 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 — incluindo a salvaguarda e a prevenção de ameaças à segurança pública — deverá ser equivalente em todos os Estados-Membros. A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados os direitos dos titulares dos dados e as obrigações de quem trata dados pessoais, mas também que haja reforço dos poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais nos Estados-Membros.
- (8) O artigo 16.º, n.º 2, do TFUE atribui ao Parlamento Europeu e ao Conselho a competência para estabelecerem regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, bem como as regras relativas à livre circulação desses dados.
- (9) Nesse sentido, o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho <sup>(2)</sup>, estabelece regras gerais para proteger as pessoas singulares relativamente ao tratamento de dados pessoais e assegurar a livre circulação de dados pessoais na União.
- (10) Na Declaração 21 sobre a proteção de dados pessoais no domínio da cooperação judiciária em matéria penal e da cooperação policial, anexada à Ata Final da Conferência Intergovernamental que adotou o Tratado de Lisboa, a conferência reconheceu que, atendendo à especificidade dos domínios em causa, poderão ser necessárias disposições específicas sobre proteção de dados pessoais e sobre a livre circulação dos dados pessoais, nos domínios da cooperação judiciária em matéria penal e da cooperação policial, com base no artigo 16.º do TFUE.
- (11) Por conseguinte, esses domínios deverão ser objeto de uma diretiva que estabeleça regras específicas relativas 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, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, no respeito da natureza específica dessas atividades. Essas autoridades competentes podem incluir não só as autoridades públicas como, por exemplo, as autoridades judiciárias, a polícia ou outras autoridades de aplicação da lei, mas também outros organismos ou entidades designados pelo direito dos Estados-Membros para o exercício da autoridade e dos poderes públicos para efeitos da presente diretiva. Caso esses organismos ou entidades tratem dados pessoais para efeitos que não sejam os da presente diretiva, é aplicável o Regulamento (UE) 2016/679. O Regulamento (UE) 2016/679 é, pois, aplicável nos casos em que um organismo ou uma entidade recolhe dados pessoais para outros efeitos e, em seguida, os trata a fim de dar cumprimento a uma obrigação legal a que está sujeito. Pode ser o caso das instituições financeiras quando retêm, para efeitos de investigação, deteção ou repressão de infrações penais, certos dados pessoais por si tratados e os fornecem apenas às autoridades nacionais competentes em casos específicos e nos termos do direito dos Estados-Membros. Os organismos ou entidades que tratam dados pessoais em nome dessas autoridades no âmbito da presente diretiva deverão estar vinculados por contrato ou por outro ato jurídico e pelas disposições aplicáveis aos subcontratantes nos termos da presente diretiva, sem prejuízo da aplicação do Regulamento (UE) 2016/679 ao tratamento de dados pessoais pelo subcontratante não abrangido pela presente diretiva.
- (12) As funções de polícia ou de outras autoridades de aplicação da lei centram-se principalmente na prevenção, investigação, deteção ou repressão de infrações penais, incluindo as atividades policiais sem conhecimento prévio de que um incidente constitui ou não uma infração penal. Estas funções podem incluir o exercício da autoridade através de medidas coercivas, tais como as atividades da polícia em manifestações, grandes eventos desportivos e distúrbios. Essas funções incluem também a manutenção da ordem pública enquanto atribuição da polícia ou de

<sup>(1)</sup> Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60).

<sup>(2)</sup> Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (ver página 1 do presente Jornal Oficial).

outras autoridades de aplicação da lei, quando necessárias para a salvaguarda e prevenção de ameaças à segurança pública e aos interesses fundamentais da sociedade protegidos por lei, e à prática de infrações penais. Os Estados-Membros podem atribuir às autoridades competentes outras funções que não sejam necessariamente executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações penais, nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública, de modo que o tratamento dos dados pessoais para esses outros efeitos, na medida em que se insira na esfera do direito da União, seja abrangido pelo âmbito de aplicação do Regulamento (UE) 2016/679.

- (13) O conceito de infração penal, na aceção da presente diretiva, deverá ser um conceito autónomo do direito da União, tal como interpretado pelo Tribunal de Justiça da União Europeia («Tribunal de Justiça»).
- (14) Uma vez que a presente diretiva não deverá aplicar-se ao tratamento de dados pessoais efetuado no exercício de atividades não sujeitas ao direito da União, não deverão ser consideradas atividades abrangidas pela presente diretiva as atividades relacionadas com a segurança nacional e as atividades das agências ou unidades que se dedicam a questões de segurança nacional e ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades inseridas no âmbito de aplicação do Título V, Capítulo 2, do Tratado da União Europeia (TUE).
- (15) A fim de assegurar o mesmo nível de proteção para as pessoas singulares através de direitos suscetíveis de proteção judicial no conjunto da União e evitar divergências que criem obstáculos ao intercâmbio de dados pessoais entre as autoridades competentes, a presente diretiva deverá prever 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, nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. A aproximação das legislações dos Estados-Membros não deverá implicar uma diminuição da proteção dos dados pessoais, devendo, pelo contrário, ter por objetivo garantir um elevado nível de proteção na União. Os Estados-Membros não deverão ser impedidos de prever garantias mais elevadas do que as estabelecidas na presente diretiva para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.
- (16) A presente diretiva não prejudica o princípio do direito de acesso do público aos documentos oficiais. Ao abrigo do Regulamento (UE) 2016/679, os dados pessoais que constem de documentos oficiais na posse de uma autoridade pública ou de um organismo público ou privado para o exercício de funções de interesse público podem ser divulgados por essa autoridade ou organismo nos termos do direito da União ou do Estado-Membro que for aplicável à autoridade ou organismo público, a fim de conciliar o acesso do público a documentos oficiais com o direito à proteção dos dados pessoais.
- (17) A proteção conferida pela presente diretiva deverá abranger as pessoas singulares, independentemente da sua nacionalidade ou lugar de residência, relativamente ao tratamento dos seus dados pessoais.
- (18) A fim de se evitar um sério risco de ser contornada, a proteção das pessoas singulares deverá ser neutra em termos tecnológicos e não deverá depender das técnicas utilizadas. A proteção das pessoas singulares deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual se os dados pessoais estiverem contidos ou se destinarem a um ficheiro. Os ficheiros ou conjuntos de ficheiros, bem como as suas capas, que não estejam estruturados de acordo com critérios específicos, não deverão ser incluídos no âmbito de aplicação da presente diretiva.
- (19) O Regulamento (CE) n.º 45/2001 do Parlamento Europeu e do Conselho <sup>(1)</sup> aplica-se ao tratamento de dados pessoais pelas instituições, órgãos, organismos ou agências da União. O Regulamento (CE) n.º 45/2001, bem como outros atos jurídicos da União aplicáveis ao tratamento de dados pessoais, deverão ser adaptados aos princípios e regras do Regulamento (UE) 2016/679.
- (20) A presente diretiva não obsta a que os Estados-Membros especifiquem as operações e os procedimentos de tratamento na legislação processual penal nacional no que se refere ao tratamento de dados pessoais pelos tribunais e as outras autoridades judiciais, em particular no que respeita aos dados pessoais que constem de uma decisão judicial ou de um registo relacionado com uma ação penal.

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

- (21) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Para determinar se uma pessoa singular é identificável, importa considerar todos os meios que possam ser razoavelmente utilizados, quer pelo responsável pelo tratamento quer por qualquer outra pessoa, para identificar direta ou indiretamente a pessoa singular. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa singular, importa considerar todos os fatores objetivos, como os custos e o tempo necessário para a identificação, tendo em conta tanto a tecnologia disponível à data do tratamento dos dados como a evolução tecnológica. Os princípios da proteção de dados não deverão, pois, aplicar-se às informações anónimas, isto é, informações que não digam respeito a nenhuma pessoa singular identificada ou identificável nem a dados pessoais tornados de tal forma anónimos que o seu titular já não possa ser identificado.
- (22) As autoridades públicas a quem os dados pessoais forem divulgados de acordo com obrigações jurídicas no exercício da sua missão oficial, tais como as autoridades fiscais e aduaneiras, as unidades de investigação financeira, as autoridades administrativas independentes, ou as autoridades dos mercados financeiros, responsáveis pela regulamentação e supervisão dos mercados de valores mobiliários não poderão ser consideradas destinatárias se receberem dados pessoais que forem necessários para efetuar um inquérito específico de interesse geral, em conformidade com o direito da União ou dos Estados-Membros. Os pedidos de divulgação enviados pelas autoridades públicas deverão ser sempre feitos por escrito, fundamentados e ocasionais e não deverão dizer respeito à totalidade de um ficheiro ou levar à interconexão de ficheiros. O tratamento de dados pessoais por essas autoridades públicas deverá estar em conformidade com as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.
- (23) Os dados genéticos deverão ser definidos como todos os dados pessoais relacionados com as características genéticas, hereditárias ou adquiridas, de uma pessoa, e que dão informações únicas sobre a fisionomia ou a saúde do indivíduo, resultantes, designadamente, da análise de cromossomas, do ácido desoxirribonucleico (ADN), do ácido ribonucleico (ARN) ou de qualquer outro elemento que permita obter informações equivalentes. Tendo em conta a complexidade e a natureza sensível das informações genéticas, existe um elevado risco de utilização injustificada e de reutilização para diversos fins não autorizados por parte do responsável pelo tratamento. As discriminações com base em características genéticas deverão ser proibidas.
- (24) Deverão ser considerados dados pessoais relativos à saúde todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Tal abrange informações sobre a pessoa singular recolhidas durante a sua inscrição para a prestação de serviços de saúde e durante essa prestação a que se refere a Diretiva 2011/24/UE do Parlamento Europeu e do Conselho <sup>(1)</sup> em relação a uma pessoa singular; qualquer número, símbolo ou sinal particular atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; ou quaisquer informações sobre, por exemplo, uma doença, deficiência, risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico atual do titular dos dados, independentemente da sua fonte, por exemplo um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico *in vitro*.
- (25) Todos os Estados-Membros fazem parte da Organização Internacional da Polícia Criminal (Interpol). No exercício das suas atribuições, a Interpol recebe, conserva e divulga dados pessoais a fim de auxiliar as autoridades competentes na prevenção e no combate à criminalidade internacional. Por conseguinte, é conveniente reforçar a cooperação entre a União e a Interpol mediante a promoção de um eficaz intercâmbio de dados pessoais, assegurando ao mesmo tempo o respeito pelos direitos e liberdades fundamentais no que se refere ao tratamento dos dados pessoais. Caso sejam transferidos dados pessoais da União para a Interpol e para países que destacaram membros para a Interpol, a presente diretiva deverá aplicar-se, em particular, no que diz respeito às disposições sobre transferências internacionais. A presente diretiva não deverá prejudicar as regras específicas previstas na Posição Comum 2005/69/JAI do Conselho <sup>(2)</sup> e na Decisão 2007/533/JAI do Conselho <sup>(3)</sup>.
- (26) O tratamento de dados pessoais tem de ser feito de forma lícita, leal e transparente para com as pessoas singulares em causa, e exclusivamente para os efeitos específicos previstos na lei. Tal não obsta, em si mesmo, a que as autoridades de aplicação da lei exerçam atividades tais como investigações encobertas ou videovigilância. Tais atividades podem ser executadas para efeitos de prevenção, investigação, deteção ou repressão de infrações

<sup>(1)</sup> Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).

<sup>(2)</sup> Posição Comum 2005/69/JAI do Conselho, de 24 de janeiro de 2005, relativa ao intercâmbio de certos dados com a Interpol (JO L 27 de 29.1.2005, p. 61).

<sup>(3)</sup> Decisão 2007/533/JAI do Conselho, de 12 de junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação Schengen de segunda geração (SIS II) (JO L 205 de 7.8.2007, p. 63).

penais ou execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, desde que estejam previstas na lei e constituam uma medida necessária e proporcionada numa sociedade democrática, tendo devidamente em conta os interesses legítimos da pessoa singular em causa. A lealdade de tratamento, que constitui um dos princípios da proteção de dados, é uma noção distinta do direito a um tribunal imparcial, tal como definido no artigo 47.º da Carta e no artigo 6.º da Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (CEDH). As pessoas singulares deverão ser alertadas para os riscos, regras, garantias e direitos associados ao tratamento dos seus dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente ao tratamento desses dados. Em especial, os efeitos específicos do tratamento deverão ser explícitos e legítimos, e deverão estar determinados no momento da recolha dos dados pessoais. Os dados pessoais deverão ser adequados e relevantes para os efeitos para os quais são tratados. É especialmente necessário garantir que os dados pessoais recolhidos não sejam excessivos nem conservados durante mais tempo do que o necessário para os efeitos para os quais são tratados. Os dados pessoais só deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. A fim de assegurar que os dados são conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar prazos para o seu apagamento ou revisão periódica. Os Estados-Membros deverão prever garantias adequadas aplicáveis aos dados pessoais conservados durante períodos mais longos a fim de fazerem parte de arquivos de interesse público ou de serem utilizados para fins científicos, estatísticos ou históricos.

- (27) Para efeitos de prevenção, investigação ou repressão de infrações penais, é necessário que as autoridades competentes tratem os dados pessoais, recolhidos no contexto da prevenção, investigação, deteção ou repressão de infrações penais específicas para além desse contexto, a fim de obter uma melhor compreensão das atividades criminais e de estabelecer ligações entre as diferentes infrações penais detetadas.
- (28) A fim de preservar a segurança do tratamento e de evitar o tratamento em violação da presente diretiva, os dados pessoais deverão ser tratados de uma forma que garanta um nível adequado de segurança e confidencialidade, nomeadamente para evitar o acesso ou a utilização desses dados e do equipamento utilizado para o seu tratamento por parte de pessoas não autorizadas, e que tenha em conta as técnicas e tecnologias mais avançadas, os custos da sua aplicação em função dos riscos e a natureza dos dados pessoais a proteger.
- (29) Os dados pessoais deverão ser recolhidos para finalidades determinadas, explícitas e legítimas abrangidas pelo âmbito de aplicação da presente diretiva e não deverão ser tratados para fins incompatíveis com os da prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais — nomeadamente a salvaguarda e a prevenção de ameaças à segurança pública. Se os dados pessoais forem tratados, pelo mesmo ou por outro responsável pelo tratamento, para uma finalidade abrangida pelo âmbito de aplicação da presente diretiva que não aquela para a qual foram recolhidos, esse tratamento deverá ser permitido, na condição de que esse tratamento seja autorizado em conformidade com as disposições legais aplicáveis e necessário e proporcionado para a prossecução dessa outra finalidade.
- (30) É conveniente aplicar o princípio da exatidão dos dados tendo em conta a natureza e a finalidade do tratamento em causa. Especialmente quando se trata de processos judiciais, as declarações que contêm dados pessoais são baseadas em perceções subjetivas da pessoa singular e nem sempre são verificáveis. Este princípio não deverá, por conseguinte, aplicar-se à exatidão da própria declaração, mas simplesmente ao facto de tal declaração ter sido feita.
- (31) O tratamento de dados pessoais nos domínios da cooperação judiciária em matéria penal e da cooperação policial implica necessariamente o tratamento de dados pessoais relativos a categorias diferentes de titulares de dados. Importa, portanto, estabelecer, se aplicável e tanto quanto possível, uma clara distinção entre dados pessoais de diferentes categorias de titulares de dados, tais como suspeitos, pessoas condenadas por um crime, vítimas e terceiros, designadamente testemunhas, pessoas que detenham informações ou contactos úteis, e os cúmplices de pessoas suspeitas ou condenadas. Tal não deverá impedir a aplicação do direito à presunção de inocência, tal como garantido pela Carta e pela CEDH, de acordo com a interpretação da jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente.
- (32) As autoridades competentes deverão assegurar que não sejam transmitidos nem disponibilizados dados pessoais incorretos, incompletos ou desatualizados. A fim de assegurar a proteção das pessoas singulares e a exatidão, exaustividade ou atualidade e fiabilidade dos dados pessoais transmitidos ou disponibilizados, as autoridades competentes deverão acrescentar, na medida do possível, as informações necessárias em todas as transmissões de dados pessoais.
- (33) Sempre que a presente diretiva se refira ao direito de um Estado-Membro, a um fundamento jurídico ou a uma medida legislativa, não se trata necessariamente de um ato legislativo adotado por um parlamento, sem prejuízo

dos requisitos que decorram da ordem constitucional do Estado-Membro em causa. No entanto, esse direito de um Estado-Membro, esse fundamento jurídico ou essa medida legislativa deverão ser claros e precisos, e a sua aplicação deverá ser previsível para os particulares, como exigido pela jurisprudência do Tribunal de Justiça e pelo Tribunal Europeu dos Direitos do Homem. O direito dos Estados-Membros que rege o tratamento de dados pessoais no âmbito da presente diretiva deverá especificar, pelo menos, os objetivos, os dados pessoais a tratar, as finalidades do tratamento e os procedimentos destinados a preservar a integridade e a confidencialidade dos dados pessoais, bem como os procedimentos para a destruição dos mesmos, proporcionando assim garantias suficientes contra o risco de abusos e de arbitrariedade.

- (34) O tratamento de dados pessoais pelas autoridades competentes 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 — deverá abranger qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais para esses efeitos, com ou sem meios automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comparação ou interconexão, a limitação do tratamento, o apagamento ou a destruição. As regras previstas na presente diretiva deverão, em especial, aplicar-se à transmissão de dados pessoais para as finalidades nela previstas aos destinatários a que esta se não aplique. Tais destinatários são as pessoas singulares ou coletivas, autoridades públicas, agências ou qualquer outro organismo a que os dados tenham sido disponibilizados de forma lícita pela autoridade competente. Caso os dados tenham sido inicialmente recolhidos por uma autoridade competente para uma das finalidades prosseguidas pela presente diretiva, o Regulamento (UE) 2016/679 deverá aplicar-se ao tratamento desses dados para fins que não os da presente diretiva se tal tratamento for autorizado pelo direito da União ou dos Estados-Membros. As regras previstas no Regulamento (UE) 2016/679 deverão, em especial, aplicar-se à transmissão de dados pessoais para fins que se não insiram no âmbito de aplicação da presente diretiva. O Regulamento (UE) 2016/679 deverá aplicar-se ao tratamento de dados pessoais por um destinatário que não seja uma autoridade competente ou que não atue nessa qualidade, na aceção da presente diretiva, e à qual os dados pessoais sejam disponibilizados de forma lícita por uma autoridade competente. Ao transporem a presente diretiva, os Estados-Membros deverão também especificar mais pormenorizadamente a aplicação das regras do Regulamento (UE) 2016/679, sob reserva das condições nele previstas.
- (35) Para ser lícito, o tratamento de dados pessoais nos termos da presente diretiva deverá ser necessário para a execução de uma missão de interesse público por uma autoridade competente com base no direito da União ou dos Estados-Membros 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. Estas funções deverão abranger a proteção dos interesses vitais do titular dos dados. O exercício das funções de prevenção, investigação, deteção ou repressão de infrações penais conferidas institucionalmente por lei às autoridades competentes permite-lhes exigir que as pessoas singulares cumpram o que lhes é solicitado. Neste caso, o consentimento do titular dos dados, na aceção do Regulamento (UE) 2016/679, não deverá constituir um fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes. Caso seja obrigado a cumprir uma obrigação legal, o titular dos dados não tem verdadeira liberdade de escolha, pelo que a sua reação não poderá ser considerada uma livre manifestação da sua vontade. Tal não deverá obstar a que os Estados-Membros prevejam por lei a possibilidade de o titular dos dados consentir que os seus dados pessoais sejam tratados para as finalidades previstas na presente diretiva, nomeadamente que sejam efetuados testes de ADN no âmbito de investigações penais ou controlada a sua localização por meio de etiquetas eletrónicas tendo em vista a execução de sanções penais.
- (36) Os Estados-Membros deverão prever que, caso o direito da União ou dos Estados-Membros aplicável à autoridade transmissora competente preveja condições específicas aplicáveis em circunstâncias específicas ao tratamento de dados pessoais, como a utilização de códigos de tratamento, a autoridade competente deverá informar o destinatário dos dados pessoais dessas condições e da obrigação de as respeitar. Tais condições poderão, por exemplo, incluir a proibição de transmitir os dados pessoais a terceiros, ou que sejam utilizados para fins que não os fins para os quais foram transmitidos, ou, ainda, não informar o titular dos dados em caso de limitação do direito de obter informações sem a aprovação prévia da autoridade transmissora competente. Essas obrigações deverão aplicar-se igualmente às transferências da autoridade transmissora competente para destinatários situados em países terceiros ou para organizações internacionais. Os Estados-Membros deverão assegurar que essa autoridade competente não aplique a destinatários situados noutros Estados-Membros nem a agências, organismos e órgãos criados nos termos do Título V, Capítulos 4 e 5, do TFUE condições diferentes das aplicáveis a transmissões de dados similares no Estado-Membro da autoridade transmissora competente.
- (37) Os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, merecem uma proteção especial, dado que o contexto do tratamento desses dados pode



implicar riscos significativos para os direitos e liberdades fundamentais. Deverão incluir-se os dados pessoais que revelem a origem racial ou étnica, não implicando o uso do termo «origem racial» na presente diretiva que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. Tais dados pessoais não deverão ser objeto de tratamento, a menos que este esteja sujeito a garantias adequadas dos direitos e liberdades do titular dos dados e seja permitido em casos autorizados por lei ou, se ainda não tiver sido autorizado por lei, se for necessário para a proteção dos interesses vitais do titular dos dados ou de um terceiro, ou ainda se estiver relacionado com dados que tenham sido manifestamente tornados públicos pelo titular dos dados. As garantias adequadas dos direitos e liberdades do titular dos dados podem, por exemplo, incluir a possibilidade de recolher esses dados apenas em ligação com outros dados sobre a pessoa singular em causa, a fim de garantir devidamente a segurança dos dados recolhidos, o estabelecimento de regras mais rigorosas sobre o acesso do pessoal da autoridade competente aos dados ou a proibição da transmissão desses dados. O tratamento desses dados deverá também ser autorizado por lei quando o titular dos dados tiver dado o seu acordo expresse, nos casos em que o tratamento de dados é particularmente intrusivo para o titular. Todavia, o consentimento do titular dos dados não deverá constituir em si mesmo fundamento jurídico do tratamento de dados pessoais pelas autoridades competentes.

- (38) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão que avalie aspetos pessoais que lhe digam respeito e se baseie exclusivamente no tratamento automatizado, com efeitos legais que lhe sejam adversos ou o afetem de forma significativa. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, incluindo informação específica ao titular dos dados e o direito de obter a intervenção humana e, em especial, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação ou de contestar a decisão. A definição de perfis que conduza a discriminação contra pessoas singulares com base em dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, deverá ser proibida, nas condições estabelecidas nos artigos 21.º e 52.º da Carta.
- (39) Para que os titulares de dados possam exercer os seus direitos, as informações que lhes sejam dirigidas, inclusive no sítio *web* do responsável pelo tratamento, deverão ser de fácil acesso e compreensão e formuladas em termos claros e simples. Essas informações deverão ser adaptadas às necessidades das pessoas vulneráveis, como as crianças.
- (40) Deverão ser previstas regras para facilitar o exercício, pelo titular dos dados, dos direitos que lhe são conferidos pelas disposições adotadas por força da presente diretiva, incluindo procedimentos para solicitar, a título gratuito, o acesso aos seus dados pessoais e a sua retificação e apagamento dos dados pessoais e a limitação do tratamento. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada, salvo se aplicar limitações aos direitos do mesmo em conformidade com a presente diretiva. Além disso, se os pedidos forem manifestamente infundados ou excessivos, por exemplo quando o titular dos dados solicitar informações de forma injustificada e repetida ou abusar do seu direito a receber informações, nomeadamente prestando informações falsas ou suscetíveis de induzir em erro, o responsável pelo tratamento deverá poder cobrar uma taxa razoável ou recusar dar seguimento ao pedido.
- (41) Caso o responsável pelo tratamento solicite que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados, essas informações deverão ser tratadas apenas para essa finalidade específica e não deverão ser conservadas durante mais tempo do que o necessário para o efeito.
- (42) Deverão ser facultadas ao titular dos dados pelo menos as seguintes informações: a identidade do responsável pelo tratamento, a existência da operação de tratamento, as finalidades do tratamento, o direito de apresentar reclamação e a existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais e a sua retificação ou apagamento ou a limitação do tratamento. Tal poderá ser efetuado no sítio *web* da autoridade competente. Além disso, em casos específicos e no intuito de que seja permitido o exercício dos seus direitos, o titular dos dados deverá ser informado sobre o fundamento jurídico do tratamento e a duração da conservação dos dados, na medida em que tais informações adicionais sejam necessárias, tendo em conta as circunstâncias específicas em que os dados são tratados, a fim de garantir a lealdade do tratamento no que respeita ao titular dos dados.
- (43) As pessoas singulares deverão ter o direito de aceder aos dados recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de tomar conhecimento do tratamento e verificar a sua licitude. Por conseguinte, cada titular de dados deverá ter o direito de ser informado das finalidades a que se destina o tratamento dos seus dados, da sua duração e de quem são os destinatários, inclusive em países terceiros. Nos casos em que essa comunicação inclua informações relativas à origem dos dados pessoais, tais informações não deverão revelar a identidade das pessoas singulares, em especial de fontes confidenciais. Para que esse direito seja respeitado, basta que o titular dos dados esteja na posse de um resumo completo desses dados num formulário inteligível, ou seja, um formulário que permita que o titular dos dados tome conhecimento desses

dados e verifique a sua exatidão e o seu tratamento em conformidade com a presente diretiva, de modo a que possa exercer os direitos que esta lhe confere. Esse resumo poderá ser concedido por via de uma cópia dos dados pessoais sujeitos a tratamento.

- (44) Os Estados-Membros deverão poder adotar medidas legislativas que visem atrasar, limitar ou recusar a informação prestada a titulares de dados ou restringir, total ou parcialmente, o acesso aos dados pessoais que lhes digam respeito, desde que tal 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, para não prejudicar os inquéritos, investigações ou procedimentos oficiais ou legais, procurar não prejudicar a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública ou a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros. O responsável pelo tratamento deverá avaliar, através de uma análise concreta de cada caso individualmente, se o direito de acesso deverá ser total ou parcialmente restringido.
- (45) As recusas ou restrições do acesso deverão, em princípio, ser comunicadas por escrito ao titular dos dados com os motivos de facto ou de direito que fundamentam a decisão.
- (46) As restrições dos direitos do titular dos dados devem respeitar a Carta e a CEDH, de acordo com a interpretação na jurisprudência do Tribunal de Justiça e do Tribunal Europeu dos Direitos do Homem, respetivamente, e devem respeitar, em particular, o conteúdo essencial desses direitos e liberdades.
- (47) As pessoas singulares deverão ter direito a que os dados inexatos que lhe dizem respeito sejam retificados, em especial no que diz respeito a factos, e a que sejam apagados, caso o seu tratamento não seja conforme com o disposto na presente diretiva. No entanto, o direito de retificação não deverá afetar, por exemplo, o conteúdo do depoimento de uma testemunha. As pessoas singulares deverão ter direito a que o tratamento seja limitado, sempre que conteste a exatidão dos dados pessoais e não possa ser apurado se os dados são exatos ou não ou, ainda, quando os dados pessoais tiverem de ser conservados para efeitos de prova. Em particular, os dados pessoais não deverão ser apagados, mas apenas limitados se, num dado caso, existirem motivos razoáveis para crer que o seu apagamento poderá prejudicar interesses legítimos do titular. Nesse caso, os dados limitados só deverão ser tratados para a finalidade que impediu o seu apagamento. Para limitar o tratamento de dados pessoais pode recorrer-se a métodos como a transferência de determinados dados para outro sistema de tratamento, nomeadamente para efeitos de arquivo, ou impedir o acesso a esses dados. Nos ficheiros automatizados, as limitações ao tratamento deverão, em princípio, ser impostas por meios técnicos; deverá ser indicado de forma bem clara no sistema que o tratamento dos dados pessoais está sujeito a limitações. Tal retificação ou apagamento dos dados pessoais ou a limitação do tratamento deverão ser comunicados aos destinatários a quem os dados tenham sido divulgados e às autoridades competentes que estão na origem dos dados inexatos. Os responsáveis pelo tratamento deverão igualmente abster-se de qualquer comunicação ulterior desses dados.
- (48) Caso o responsável pelo tratamento recuse ao titular dos dados o direito à informação, o acesso aos dados pessoais ou a sua retificação ou apagamento ou a limitação do tratamento, o titular dos dados deverá ter o direito de solicitar que a autoridade nacional de controlo verifique a licitude do tratamento. O titular dos dados deverá ser informado desse direito. Quando a autoridade de controlo agir em nome do titular dos dados, deverá, pelo menos, informá-lo de que foram realizadas todas as verificações ou revisões necessárias. A autoridade de controlo deverá também informar o titular de dados do seu direito de intentar ação judicial.
- (49) Caso os dados pessoais sejam tratados no âmbito de uma investigação criminal ou de um processo judicial em matéria penal, os Estados-Membros deverão poder dispor que o exercício do direito à informação, ao acesso aos dados pessoais e à sua retificação ou apagamento, bem como à limitação do tratamento, seja feito nos termos das regras nacionais aplicáveis aos processos judiciais.
- (50) Deverá ser estabelecida a responsabilidade do responsável pelo tratamento de dados pessoais realizado por si próprio ou em seu nome. Em especial, o responsável pelo tratamento deverá ficar obrigado a executar as medidas adequadas e eficazes e deverá estar em condições de demonstrar que as atividades de tratamento são efetuadas em conformidade com a presente diretiva. Tais medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento de dados, bem como o risco que possa implicar para os direitos e liberdades das pessoas singulares. As medidas tomadas pelo responsável pelo tratamento deverão incluir a elaboração e execução de garantias específicas para o tratamento de dados pessoais de pessoas singulares vulneráveis, como crianças.
- (51) Os riscos para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderão resultar de operações de tratamento de dados suscetíveis de causar danos físicos, materiais ou morais, em especial caso o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados protegidos por sigilo profissional, à

inversão não autorizada da pseudonimização, ou a outros prejuízos importantes de natureza económica ou social; ou caso os titulares dos dados possam ficar privados dos seus direitos e liberdades ou do exercício do controlo sobre os respetivos dados pessoais; caso sejam tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical; caso sejam tratados dados genéticos ou dados biométricos a fim de identificar uma pessoa de forma inequívoca ou caso sejam tratados dados relativos à saúde ou à vida sexual ou orientação sexual ou, ainda, a condenações e infrações penais ou medidas de segurança conexas; caso sejam avaliados aspetos de natureza pessoal, nomeadamente análises e 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; ou caso sejam tratados dados pessoais de pessoas singulares vulneráveis, em particular crianças; ou caso o tratamento incida sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

- (52) A probabilidade e a gravidade dos riscos deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento. Os riscos deverão ser aferidos com base numa avaliação objetiva, de modo a determinar se é provável que as operações de tratamento de dados impliquem um elevado risco. Entende-se por «elevado risco» um risco particular que prejudique os direitos e liberdades dos titulares de dados.
- (53) A proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige que sejam tomadas medidas técnicas e organizativas adequadas para assegurar o cumprimento dos requisitos da presente diretiva. A execução dessas medidas não poderá depender exclusivamente de considerações económicas. A fim de poder demonstrar a conformidade com a presente diretiva, o responsável pelo tratamento deverá adotar diretrizes internas e aplicar medidas que respeitem, em especial, os princípios da proteção de dados desde a conceção e da proteção de dados por defeito. Sempre que o responsável pelo tratamento tenha efetuado uma avaliação do impacto na proteção de dados nos termos da presente diretiva, os resultados da referida avaliação deverão ser tidos em conta para efeitos de desenvolvimento dessas medidas e procedimentos. As medidas poderão incluir, nomeadamente, o recurso à pseudonimização, efetuada o mais cedo possível. O recurso à pseudonimização para efeitos da presente diretiva poderá facilitar, designadamente, a livre circulação de dados pessoais no espaço de liberdade, segurança e justiça.
- (54) A proteção dos direitos e liberdades dos titulares de dados, bem como a responsabilidade dos responsáveis pelo tratamento e dos subcontratantes, inclusive no que diz respeito à supervisão e às medidas adotadas pelas autoridades de controlo, exigem uma clara repartição de responsabilidades nos termos da presente diretiva, designadamente caso o responsável pelo tratamento dos dados determine as finalidades e os meios do tratamento conjuntamente com outros responsáveis ou uma operação de tratamento de dados seja efetuada em nome de um responsável pelo tratamento.
- (55) O tratamento executado por um subcontratante deverá ser regido por um ato jurídico, que pode ser um contrato que vincule o subcontratante ao responsável pelo tratamento e estipule, nomeadamente, que o subcontratante só deverá agir segundo instruções do responsável pelo tratamento. O subcontratante deverá ter em consideração o princípio da proteção de dados desde a conceção e por defeito.
- (56) A fim de comprovar o cumprimento da presente diretiva, o responsável pelo tratamento ou o subcontratante deverá manter registos de todas as categorias de atividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento dos dados e os subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento. O responsável pelo tratamento ou o subcontratante que trate dados pessoais em sistemas de tratamento não automatizados deverá dispor de métodos eficazes, tais como registos cronológicos ou outros, para demonstrar a licitude do tratamento, permitir o autocontrolo e garantir a integridade e segurança dos dados.
- (57) Deverão ser conservados registos cronológicos pelo menos de operações em sistemas de tratamento automatizado, como a recolha, alteração, consulta, divulgação — incluindo transferências —, interconexão ou apagamento. A identificação da pessoa que consultou ou divulgou dados pessoais deverá ser registada e a partir dessa identificação será talvez possível determinar a justificação das operações de tratamento. Os registos cronológicos deverão ser utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo, garantia da integridade e segurança dos dados e ações penais. O autocontrolo abrange igualmente as ações disciplinares internas das autoridades competentes.
- (58) Deverá ser efetuada uma avaliação do impacto na proteção de dados pelo responsável pelo tratamento quando as operações de tratamento forem suscetíveis de constituir um elevado risco para os direitos e liberdades dos titulares dos dados devido à sua natureza, âmbito ou finalidades, a qual deverá incluir, em particular, as medidas previstas, as garantias e os mecanismos previstos para assegurar a proteção dos dados pessoais e demonstrar a conformidade com a presente diretiva. As avaliações de impacto deverão ter como objeto os sistemas e processos pertinentes das operações de tratamento, mas não casos individuais.

- (59) A fim de assegurar a proteção efetiva dos direitos e liberdades dos titulares dos dados, o responsável pelo tratamento ou o subcontratante deverá, em certos casos, consultar a autoridade de controlo antes do tratamento.
- (60) A fim de preservar a segurança e evitar o tratamento em violação da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e deverá aplicar medidas que os atenuem, como, por exemplo, a cifragem. Estas medidas deverão assegurar um nível de segurança adequado, nomeadamente no que respeita à confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função do risco 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, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados, de dados pessoais transmitidos, conservados ou tratados de outro modo, riscos esses que podem conduzir, em particular, a danos físicos, materiais ou morais. O responsável pelo tratamento e o subcontratante deverão assegurar que o tratamento de dados pessoais não seja efetuado por pessoas não autorizadas.
- (61) Se não forem tomadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, tais como a perda de controlo dos dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação de identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social importante para as pessoas singulares em causa. Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá comunicá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares. Se não for possível efetuar a comunicação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem mais demora injustificada.
- (62) Caso a violação de dados pessoais seja suscetível de criar um elevado risco para os direitos e liberdades das pessoas singulares, estas deverão ser informadas sem demora injustificada, a fim de permitir que tomem as precauções necessárias. Da comunicação deverá constar a natureza da violação de dados pessoais e recomendações destinadas à pessoa singular em causa para atenuar potenciais efeitos adversos. A comunicação aos titulares dos dados deverá ser feita o mais rapidamente possível, em estreita cooperação com a autoridade de controlo, e de acordo com as orientações fornecidas por esta ou por outras autoridades competentes. Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá que se envie uma comunicação rápida aos titulares dos dados, enquanto a necessidade de aplicar medidas adequadas contra violações de dados recorrentes ou similares poderá justificar um prazo maior para a comunicação. Se não for possível, através do atraso ou da restrição da comunicação à pessoa singular em causa de uma violação de dados pessoais, evitar criar entraves a inquéritos, investigações ou procedimentos oficiais ou legais, evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais, salvaguardar a segurança pública, preservar a segurança nacional ou ainda proteger os direitos e as liberdades de terceiros, essa comunicação poderá, em circunstâncias excecionais, ser omitida.
- (63) O responsável pelo tratamento deverá designar uma pessoa para o assistir no controlo do cumprimento, a nível interno, das disposições adotadas por força da presente diretiva. Os Estados-Membros poderão isentar desta obrigação os tribunais e outras autoridades judiciais independentes no exercício da sua função jurisdicional. Essa pessoa pode ser um membro do pessoal do responsável pelo tratamento, que tenha recebido uma formação específica no domínio da legislação e das práticas em matéria de proteção de dados a fim de adquirir conhecimentos especializados nesta matéria. O nível de conhecimentos especializados necessários deverá ser determinado, em particular, em função do tratamento de dados efetuado e da proteção exigida para os dados pessoais tratados pelo responsável pelo tratamento. As suas funções podem ser exercidas a tempo parcial ou a tempo inteiro. Um encarregado da proteção de dados poderá ser nomeado conjuntamente por vários responsáveis pelo tratamento, tendo em conta a dimensão e estrutura organizativa destes, por exemplo no caso de partilha de recursos em unidades centrais. Essa pessoa pode igualmente ser nomeada para diferentes funções no interior das estruturas responsáveis pelo tratamento. Essa pessoa deverá ajudar o responsável pelo tratamento e os empregados que tratem dados pessoais, informando-os e aconselhando-os a respeito do cumprimento das suas obrigações relevantes em matéria de proteção de dados. Essas pessoas encarregadas da proteção de dados deverão estar em condições de desempenhar as suas funções e cumprir os seus deveres de forma independente e de acordo com o direito dos Estados-Membros.
- (64) Os Estados-Membros deverão assegurar que as transferências para um país terceiro ou para uma organização internacional só possam ser realizadas se forem necessárias para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais — nomeadamente, a salvaguarda e a prevenção de

ameaças à segurança pública — e se o responsável pelo tratamento no país terceiro ou na organização internacional for uma autoridade competente na aceção da presente diretiva. Apenas as autoridades competentes, na qualidade de responsáveis pelo tratamento, podem efetuar transferências, salvo se os subcontratantes tiverem instruções explícitas para efetuar a transferência em causa por conta dos responsáveis pelo tratamento. Tal transferência pode ser efetuada caso a Comissão tenha decidido que o país terceiro ou a organização internacional em causa garante um nível de proteção adequado, ou quando tiverem sido apresentadas garantias adequadas ou forem aplicáveis derrogações em situações específicas. Caso os dados pessoais sejam transferidos da União para responsáveis pelo tratamento de dados, para subcontratantes ou para outros destinatários em países terceiros ou organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pela presente diretiva deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento de dados, ou subcontratantes desse país terceiro ou de outro, ou para uma organização internacional.

- (65) Caso sejam transferidos dados pessoais de um Estado-Membro para países terceiros ou organizações internacionais, essa transferência apenas deverá, em princípio, ser efetuada depois de o Estado-Membro de onde provêm os dados ter dado a sua autorização. O interesse de uma cooperação eficiente em matéria de aplicação da lei exige que, caso a natureza de uma ameaça à segurança pública de um Estado-Membro ou país terceiro ou aos interesses essenciais de um Estado-Membro seja tão iminente que impossibilite a obtenção de autorização prévia em tempo útil, a autoridade competente deva poder transferir os dados pessoais pertinentes para o país terceiro ou a organização internacional em causa sem essa autorização prévia. Os Estados-Membros deverão prever que sejam comunicadas aos países terceiros ou às organizações internacionais as condições específicas relativas à transferência. As transferências ulteriores de dados pessoais deverão ser submetidas a autorização prévia pela autoridade competente que realizou a transferência inicial. Ao decidir sobre um pedido de autorização para uma transferência ulterior, a autoridade competente que realizou a transferência inicial deverá ter devidamente em conta todos os fatores relevantes, designadamente a gravidade da infração penal, as condições específicas associadas e a finalidade para a qual os dados foram inicialmente transferidos, a natureza e as condições de execução da sanção penal e o nível de proteção de dados pessoais do país terceiro ou da organização internacional para os quais os dados pessoais são ulteriormente transferidos. A autoridade competente que realizou a transferência inicial poderá igualmente sujeitar a transferência ulterior a condições específicas. Tais condições específicas podem ser descritas, por exemplo, em códigos de tratamento.
- (66) A Comissão poderá decidir, com efeitos no conjunto da União, que determinados países terceiros, um território ou um ou vários setores especificados num país terceiro ou numa organização internacional asseguram um nível adequado de proteção de dados, garantindo assim a segurança jurídica e a uniformidade a nível da União relativamente a países terceiros ou organizações internacionais que sejam considerados aptos a assegurar tal nível de proteção. Nesses casos, poderão ser feitas transferências de dados pessoais para esses países sem necessidade de qualquer autorização específica, exceto se outro Estado-Membro de onde provêm os dados tiver de dar a sua autorização à transferência.
- (67) De acordo com os valores fundamentais em que a União assenta, particularmente a defesa dos direitos humanos, a Comissão deverá, na sua avaliação do país terceiro ou de um território ou de um setor específico num país terceiro, ter em consideração em que medida um determinado país respeita o primado do Estado de direito, o acesso à justiça, bem como as regras e normas internacionais no domínio dos direitos humanos e a sua legislação geral e setorial, nomeadamente a legislação relativa à segurança pública, à defesa e à segurança nacional, bem como a lei da ordem pública e a lei penal. A adoção de uma decisão de adequação relativa a um território ou um setor específico num país terceiro deverá ter em conta critérios claros e objetivos, tais como as atividades de tratamento específicas e o âmbito das normas jurídicas aplicáveis, bem como a legislação em vigor no país terceiro. Este deverá dar garantias de assegurar um nível adequado de proteção, essencialmente equivalente ao assegurado na União, em particular quando os dados são tratados num ou em vários setores específicos. Em especial, o país terceiro deverá garantir o controlo efetivo e independente da proteção dos dados e estabelecer mecanismos de cooperação com as autoridades de proteção de dados dos Estados-Membros, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.
- (68) Além dos compromissos internacionais assumidos pelo país terceiro ou pela organização internacional, a Comissão deverá também ter em conta as obrigações decorrentes da participação do país terceiro ou da organização internacional nos sistemas multilaterais ou regionais, em especial no que diz respeito à proteção dos dados pessoais, bem como o cumprimento de tais obrigações. Em especial, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, de 28 de janeiro de 1981, e respetivo Protocolo Adicional. A

Comissão deverá consultar o Comité Europeu para a Proteção de Dados criado pelo Regulamento (UE) 2016/679 («Comité») quando avalia o nível de proteção nos países terceiros ou organizações internacionais. A Comissão deverá ter igualmente em conta as decisões de adequação da Comissão pertinentes, adotadas em conformidade com o artigo 41.º do Regulamento (UE) 2016/679.

- (69) A Comissão deverá controlar a eficácia das decisões sobre o nível de proteção assegurado num país terceiro, num território ou num setor específico de um país terceiro, ou numa organização internacional. Nas suas decisões de adequação, a Comissão deverá prever um processo de avaliação periódica da aplicação destas. A avaliação periódica deverá ser feita em consulta com o país terceiro ou a organização internacional em questão e ter em conta todos os desenvolvimentos pertinentes verificados no país terceiro ou organização internacional.
- (70) A Comissão deverá igualmente poder reconhecer que um país terceiro, um território ou um setor específico de um país terceiro, ou uma organização internacional, deixou de assegurar um nível adequado de proteção de dados. Se for esse o caso, deverá ser proibida a transferência de dados pessoais para esse país terceiro ou organização internacional, a menos que sejam cumpridos os requisitos previstos na presente diretiva relativos às transferências sujeitas a garantias adequadas e às derrogações aplicáveis a situações específicas. É conveniente prever procedimentos de consulta entre a Comissão e esses países terceiros ou organizações internacionais. A Comissão deverá, em tempo útil, informar o país terceiro ou a organização internacional das razões de tal proibição e iniciar consultas com o país ou organização em causa a fim de corrigir a situação.
- (71) As transferências não baseadas numa decisão de adequação só deverão ser autorizadas caso sejam apresentadas garantias adequadas num instrumento juridicamente vinculativo que garanta a proteção dos dados pessoais ou o responsável pelo tratamento tenha avaliado todas as circunstâncias inerentes à transferência de dados e, com base nessa avaliação, considere que existem garantias adequadas no que diz respeito à proteção de dados pessoais. Tais instrumentos juridicamente vinculativos poderão ser, por exemplo, acordos bilaterais juridicamente vinculativos que os Estados-Membros tenham celebrado e integrado no seu ordenamento jurídico e que possam ser executados pelos titulares de dados desses Estados-Membros, assegurando a observância dos requisitos relativos à proteção de dados e dos direitos dos titulares dos dados, incluindo o direito de recurso administrativo ou judicial. Ao avaliar todas as circunstâncias relativas à transferência de dados, o responsável pelo tratamento poderá ter em conta os acordos de cooperação que tenham sido celebrados entre a Europol ou a Eurojust e países terceiros e que permitam o intercâmbio de dados pessoais. O responsável pelo tratamento poderá ainda ter em conta que a transferência de dados pessoais ficará sujeita a obrigações de confidencialidade e ao princípio da especificidade, assegurando que os dados não sejam tratados para efeitos que não sejam os da transferência. Além disso, o responsável pelo tratamento deverá ter em conta que os dados pessoais não serão utilizados para requerer, aplicar ou executar uma pena de morte ou qualquer forma de tratamento cruel ou desumano. Embora essas condições possam ser consideradas garantias adequadas para a transferência de dados, o responsável pelo tratamento pode exigir garantias adicionais.
- (72) Na falta de decisão de adequação ou de garantias adequadas, só poderão ser efetuadas transferências ou categorias de transferências em situações específicas, se necessário para: proteger os interesses vitais do titular dos dados ou de um terceiro ou salvaguardar os interesses legítimos do titular dos dados, desde que o direito do Estado-Membro que efetua a transferência dos dados assim o preveja; prevenir uma ameaça iminente e grave para a segurança pública de um Estado-Membro ou de um país terceiro; em determinados casos, para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a salvaguarda e prevenção de ameaças à segurança pública; em determinados casos, para efeitos de declaração, exercício ou defesa de um direito num processo judicial. Essas derrogações deverão ser interpretadas de forma restritiva e não permitir transferências frequentes, maciças e estruturais de dados pessoais nem transferências maciças de dados, devendo ser limitadas aos dados estritamente necessários. Tais transferências deverão ser documentadas e disponibilizadas, a pedido, à autoridade de controlo para verificar a licitude da transferência.
- (73) As autoridades competentes dos Estados-Membros aplicam os acordos internacionais bilaterais ou multilaterais vigentes celebrados com países terceiros no domínio da cooperação judiciária em matéria penal e da cooperação policial com vista ao intercâmbio de informações relevantes que lhes permitam exercer as atribuições previstas na lei. Em princípio, esse intercâmbio é efetuado em cooperação com as autoridades competentes dos países terceiros em causa ou, pelo menos, com a cooperação dessas autoridades, e por vezes até na falta de um acordo internacional bilateral ou multilateral. Todavia, em determinados casos específicos, os procedimentos normais que requerem contactar essa autoridade do país terceiro podem revelar-se ineficazes ou desadequados, nomeadamente devido à impossibilidade de a transferência ser efetuada em tempo útil ou devido ao facto de essa autoridade do país terceiro não respeitar o Estado de direito ou as regras e normas internacionais no domínio dos direitos humanos, de tal modo que as autoridades competentes dos Estados-Membros poderão decidir transferir os dados pessoais diretamente para os destinatários estabelecidos em países terceiros. Poderá ser o caso se houver necessidade urgente de transferir dados pessoais para salvar a vida de uma pessoa que corra o risco de ser vítima de uma infração penal ou prevenir a prática iminente de um crime, incluindo o terrorismo. Mesmo que essa

transferência entre autoridades competentes e destinatários estabelecidos em países terceiros só deva ter lugar em determinados casos específicos, a presente diretiva deverá prever condições para regular tais casos. Essas disposições não deverão ser consideradas derrogações aos acordos internacionais bilaterais ou multilaterais vigentes no domínio da cooperação judiciária em matéria penal e da cooperação policial. Essas regras deverão complementar a aplicação das demais regras da presente diretiva, especialmente as que dizem respeito à licitude do tratamento e as que estabelece o Capítulo V.

- (74) Quando os dados pessoais atravessam fronteiras há um risco acrescido de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se proteger da utilização ilícita ou da divulgação dessas informações. Paralelamente, as autoridades de controlo podem ser incapazes de dar seguimento a reclamações ou conduzir investigações relacionadas com atividades exercidas fora das suas fronteiras. Os seus esforços para colaborar no contexto transfronteiriço podem ser também prejudicados pela falta de poderes para tomar medidas preventivas ou de reparação, bem como pela incoerência e insuficiência dos regimes jurídicos aplicáveis. Por conseguinte, revela-se necessário promover uma cooperação mais estreita entre as autoridades de controlo da proteção de dados a fim de que possam efetuar o intercâmbio de informações com as suas homólogas internacionais.
- (75) A criação de autoridades de controlo nos Estados-Membros, com total independência no exercício das suas atribuições, constitui um elemento essencial da proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais. As autoridades de controlo deverão fiscalizar a aplicação das disposições adotadas por força da presente diretiva e deverão contribuir para a sua aplicação coerente em toda a União, a fim de proteger as pessoas singulares relativamente ao tratamento dos seus dados pessoais. Para esse efeito, as autoridades de controlo deverão cooperar entre si e com a Comissão.
- (76) Os Estados Membros podem confiar a uma autoridade de controlo já criada nos termos do Regulamento (UE) 2016/679 o exercício das atribuições das autoridades nacionais de controlo criadas por força da presente diretiva.
- (77) Os Estados-Membros deverão poder criar várias autoridades de controlo de modo a refletir a sua estrutura constitucional, organizativa e administrativa. Deverão ser dados às autoridades de controlo os meios financeiros e humanos, as instalações e as infraestruturas necessárias ao exercício eficaz das suas atribuições, incluindo as relacionadas com a assistência e a cooperação mútuas com outras autoridades de controlo da União. As autoridades de controlo deverão ter orçamentos anuais públicos separados, que poderão estar integrados no orçamento geral do estado ou do orçamento nacional.
- (78) As autoridades de controlo deverão ficar sujeitas a procedimentos de controlo ou fiscalização independentes no que diz respeito às suas despesas financeiras, desde que tal não afete a sua independência.
- (79) As condições gerais aplicáveis aos membros da autoridade de controlo deverão ser definidas pelo direito do Estado-Membro e deverão prever, em especial, que os referidos membros sejam nomeados por procedimento transparente pelo Parlamento, pelo Governo nacional ou pelo Chefe de Estado do Estado-Membro, com base numa proposta do governo ou de um dos seus membros ou do parlamento ou da sua câmara competente, ou por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro. A fim de assegurar a independência da autoridade de controlo, os membros que a integram deverão atuar com integridade, abster-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não deverão exercer nenhuma ocupação, seja ou não remunerada, que com elas seja incompatível. A fim de assegurar a independência da autoridade de controlo, o pessoal deverá ser selecionado pela autoridade de controlo, eventualmente com a intervenção de um organismo independente incumbido nos termos do direito do Estado-Membro.
- (80) Embora a presente diretiva se aplique também às atividades dos tribunais nacionais e outras autoridades judiciais, a competência das autoridades de controlo não deverá abranger o tratamento de dados pessoais efetuado pelos tribunais no exercício da sua função jurisdicional, a fim de assegurar a independência dos juízes no desempenho das suas funções jurisdicionais. Esta exceção deverá ser estritamente limitada às atividades judiciais relativas a processos judiciais, não se aplicando a outras atividades a que os juízes possam estar associados por força do direito do Estado-Membro. Os Estados-Membros podem também prever a possibilidade de a competência das autoridades de controlo não abranger o tratamento de dados pessoais efetuado por outras autoridades judiciais independentes no exercício da sua função jurisdicional, nomeadamente o Ministério Público. Em todo o caso, o cumprimento das regras da presente diretiva pelos tribunais e outras autoridades judiciais independentes deverá ficar sempre sujeito a uma fiscalização independente nos termos do artigo 8.º, n.º 3, da Carta.

- (81) Cada autoridade de controlo deverá tratar as reclamações apresentadas por qualquer titular de dados e investigar o assunto ou transmiti-lo à autoridade de controlo competente. A investigação decorrente de uma reclamação deverá ser realizada, sob reserva de controlo jurisdicional, na medida adequada ao caso específico. A autoridade de controlo deverá informar o titular dos dados da evolução e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser fornecidas informações intermédias ao titular dos dados.
- (82) A fim de assegurar o controlo eficaz, fiável e coerente da conformidade com a presente diretiva e da sua aplicação em toda a União e nos termos do TFUE, conforme interpretado pelo Tribunal de Justiça, as autoridades de controlo deverão ter, em cada Estado-Membro, as mesmas atribuições e poderes, incluindo poderes de investigação e de correção, bem como funções consultivas, que constituem meios necessários no exercício das suas atribuições. Os seus poderes não deverão, contudo, interferir com as regras específicas aplicáveis ao processo penal, nomeadamente à investigação e repressão de infração penais, nem com a independência do poder judicial. Sem prejuízo dos poderes das autoridades responsáveis pela aplicação da lei nos termos do direito do Estado-Membro, as autoridades de controlo deverão ainda dispor do poder de levar as violações à presente diretiva ao conhecimento das autoridades judiciais e de intentar processos judiciais. Os poderes das autoridades de controlo deverão ser exercidos em conformidade com as garantias processuais adequadas previstas pelo direito da União e dos Estados-Membros, com imparcialidade e equidade e num prazo razoável. Em particular, cada medida deverá ser adequada, necessária e proporcionada a fim de garantir a conformidade com a presente diretiva, tendo em conta as circunstâncias de cada caso concreto, respeitar o direito de qualquer pessoa a ser ouvida antes de a seu respeito ser tomada qualquer medida individual que a afete desfavoravelmente e evitar custos supérfluos e inconvenientes excessivos para a pessoa em causa. Os poderes de investigação em matéria de acesso às instalações deverão ser exercidos em conformidade com os requisitos específicos do direito do Estado-Membro, como, por exemplo, a obrigação de obter autorização judicial prévia. A adoção de uma decisão juridicamente vinculativa deverá ficar sujeita a controlo jurisdicional no Estado-Membro da autoridade de controlo que tenha adotado a decisão.
- (83) As autoridades de controlo deverão prestar-se mutuamente assistência no exercício das suas atribuições, por forma a assegurar a execução e aplicação coerentes das disposições adotadas por força da presente diretiva.
- (84) O Comité deverá contribuir para a aplicação coerente da presente diretiva em toda a União, nomeadamente aconselhando a Comissão e promovendo a cooperação das autoridades de controlo em toda a União.
- (85) Os titulares de dados deverão ter direito a apresentar reclamação a uma autoridade de controlo única e a intentar uma ação judicial, nos termos do artigo 47.º da Carta, se considerarem que os direitos que lhes são conferidos por disposições adotadas por força da presente diretiva foram violados ou a autoridade de controlo não responder à reclamação, a recusar ou rejeitar, total ou parcialmente, ou não tomar as iniciativas 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 de controlo competente deverá informar o titular dos dados da evolução e do resultado da reclamação num prazo razoável. Se o caso exigir maior investigação ou a coordenação com outra autoridade de controlo, deverão ser fornecidas informações intermédias ao titular dos dados. As autoridades de controlo deverão tomar medidas para facilitar a apresentação de reclamações, como, por exemplo, fornecer formulários para apresentação de reclamações que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.
- (86) Todas as pessoas, singulares ou coletivas, deverão ter direito a intentar uma ação judicial perante os tribunais nacionais competentes contra as decisões das autoridades de controlo que produzam efeitos jurídicos que lhes digam respeito. Tais decisões prendem-se, em especial, com o exercício de poderes de investigação, correção e autorização pelas autoridades de controlo ou com a recusa ou rejeição de reclamações. Porém, este direito não abrange outras medidas das autoridades de controlo que não sejam juridicamente vinculativas, como os pareceres emitidos ou o aconselhamento prestado pela autoridade de controlo. As ações contra as autoridades de controlo deverão ser instauradas nos tribunais do Estado-Membro em cujo território a autoridade de controlo esteja estabelecida e deverão ser conduzidas nos termos do direito desse Estado-Membro. Estes tribunais deverão ter jurisdição plena, incluindo o poder de analisar todas as questões de facto e de direito relevantes para o litígio.
- (87) Se considerar que os direitos que lhe são conferidos pela presente diretiva foram violados, o titular dos dados deverá ter o direito de mandatatar um organismo que vise proteger os direitos e interesses dos titulares de dados



no que respeita à proteção dos seus dados pessoais, e que seja constituído ao abrigo do direito de um Estado-Membro, para apresentar reclamação em seu nome a uma autoridade de controlo e exercer o direito de intentar ação judicial. O direito de representação dos titulares dos dados não deverá prejudicar o direito processual do Estado-Membro, que poderá exigir que estes se façam obrigatoriamente representar perante os tribunais nacionais por um advogado, tal como previsto na Diretiva 77/249/CEE do Conselho <sup>(1)</sup>.

- (88) Os danos sofridos por uma pessoa em virtude de um tratamento em violação da presente diretiva deverão ser ressarcidos pelo responsável pelo tratamento dos dados ou por qualquer outra autoridade competente nos termos do direito do Estado-Membro. O conceito de «dano» deverá ser interpretado em sentido lato à luz da jurisprudência do Tribunal de Justiça de uma forma que reflita plenamente os objetivos da presente diretiva. Tal não prejudica os pedidos de indemnização por danos provocados pela violação de outras regras constantes do direito da União ou dos Estados-Membros. Quando se faça referência a tratamentos ilícitos ou a tratamentos que violem disposições adotadas por força da presente diretiva, ficam igualmente abrangidos os tratamentos que violem os atos de execução adotados nos termos da presente diretiva. Os titulares dos dados deverão ser integral e efetivamente indemnizados pelos danos que tenham sofrido.
- (89) Deverão ser aplicadas sanções às pessoas singulares ou às pessoas coletivas, de direito privado ou público, que violem a presente diretiva. Os Estados-Membros deverão assegurar que as sanções sejam efetivas, proporcionadas e dissuasivas e tomar todas as medidas necessárias à sua aplicação.
- (90) A fim de assegurar condições uniformes para a execução da presente diretiva, deverão ser conferidas competências de execução à Comissão no que diz respeito ao nível de proteção adequado garantido por um país terceiro, um território ou um setor específico desse país terceiro, ou por uma organização internacional, e o formato e os procedimentos de assistência mútua, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho <sup>(2)</sup>.
- (91) Deverá ser utilizado o procedimento de exame para a adoção de atos de execução sobre o nível de proteção adequado garantido por um país terceiro, um território ou um setor específico desse país terceiro, ou por uma organização internacional, o formato e os procedimentos de assistência mútua, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité, atendendo a que se trata de atos de alcance geral.
- (92) A Comissão deverá adotar atos de execução imediatamente aplicáveis quando imperativos urgentes assim o exijam, em casos devidamente fundamentados relacionados com um país terceiro, um território ou um setor específico desse país terceiro ou uma organização internacional que tenha deixado de assegurar um nível de proteção adequado.
- (93) Atendendo a que os objetivos da presente diretiva, a saber, proteger os direitos e liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção de dados pessoais, e assegurar o livre intercâmbio desses dados pelas autoridades competentes na União, não podem ser suficientemente alcançados pelos Estados-Membros, mas podem, devido à dimensão e aos efeitos da ação, ser mais bem alcançados ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, a presente diretiva não excede o necessário para atingir esses objetivos.
- (94) Não deverão ser afetadas as disposições específicas dos atos, adotados pela União no domínio da cooperação judiciária em matéria penal e da cooperação policial antes da data de adoção da presente diretiva, que regulem o

<sup>(1)</sup> Diretiva 77/249/CEE do Conselho, de 22 de março de 1977, tendente a facilitar o exercício efetivo da livre prestação de serviços pelos advogados (JO L 78 de 26.3.1977, p. 17).

<sup>(2)</sup> Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

tratamento de dados pessoais entre Estados-Membros ou o acesso das autoridades designadas dos Estados-Membros aos sistemas de informação criados nos termos dos Tratados, como, por exemplo, as disposições específicas relativas à proteção dos dados pessoais aplicadas por força da Decisão 2008/615/JAI do Conselho <sup>(1)</sup> ou o artigo 23.º da Convenção relativa ao Auxílio Judiciário Mútuo em Matéria Penal entre os Estados-Membros da União Europeia <sup>(2)</sup>. Dado que o artigo 8.º da Carta e o artigo 16.º do TFUE exigem que o direito fundamental à proteção de dados pessoais seja garantido de forma coerente em toda a União, a Comissão deverá examinar a situação quanto à relação entre a presente diretiva e os atos adotados anteriormente à data de adoção da presente diretiva que regulem o tratamento de dados pessoais entre Estados-Membros ou o acesso de autoridades designadas dos Estados-Membros a sistemas de informação criados por força dos Tratados, a fim de avaliar a necessidade de adaptar essas disposições específicas à presente diretiva. Sempre que apropriado, a Comissão deverá apresentar propostas para assegurar regras jurídicas coerentes relacionadas com o tratamento de dados pessoais.

- (95) A fim de assegurar uma proteção global e coerente dos dados pessoais na União, os acordos internacionais celebrados pelos Estados-Membros antes de a presente diretiva entrar em vigor que sejam conformes com o direito da União aplicável antes dessa data deverão continuar a vigorar até serem alterados, substituídos ou revogados.
- (96) Os Estados-Membros deverão dispor de um prazo, não superior a dois anos, a contar da data de entrada em vigor da presente diretiva para a transpor. Os tratamentos de dados que se encontrem já em curso à data de entrada em vigor da presente diretiva deverão passar a cumprir as disposições da presente diretiva no prazo de dois anos após a data da respetiva entrada em vigor. Todavia, caso tal tratamento cumpra o disposto no direito da União aplicável antes da entrada em vigor da presente diretiva, os requisitos por ela estabelecidos no que respeita à consulta prévia da autoridade de controlo não deverão ser aplicáveis às operações de tratamento já em curso antes da entrada em vigor da presente diretiva, uma vez que, pela sua natureza, tais requisitos deverão ser cumpridos antes do início do tratamento. Caso os Estados-Membros utilizem o período de transposição mais longo, que termina setes anos a contar da data de entrada em vigor da presente diretiva, para cumprir as obrigações de registo cronológico no que respeita a sistemas de tratamento automatizado criados antes da data de entrada em vigor da presente diretiva, o responsável pelo tratamento, ou o subcontratante, deverá dispor de métodos eficazes para demonstrar a licitude do tratamento dos dados, permitir o autocontrolo e garantir a integridade e a segurança dos dados, tais como registos cronológicos ou outros.
- (97) A presente diretiva não prejudica as disposições relativas à luta contra o abuso sexual, a exploração sexual de crianças e a pornografia infantil, previstas na Diretiva 2011/93/UE do Parlamento Europeu e do Conselho <sup>(3)</sup>.
- (98) Por conseguinte, a Decisão-Quadro 2008/977/JAI deverá ser revogada.
- (99) Nos termos do artigo 6.º-A do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, o Reino Unido e a Irlanda não ficam vinculados pelas regras estabelecidas na presente diretiva que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação da Parte III, Título V, Capítulos 4 ou 5, do TFUE, caso não estejam vinculados por regras que regulem formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devam ser observadas as disposições definidas com base no artigo 16.º do TFUE.
- (100) Nos termos dos artigos 2.º e 2.º-A do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não fica vinculada nem sujeita à aplicação das regras da presente diretiva que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação da Parte III, Título V, Capítulos 4 ou 5, do TFUE. Uma vez que a presente diretiva constitui um desenvolvimento do acervo de Schengen, por força do disposto na Parte III, Título V, do TFUE, cabe à Dinamarca decidir, nos termos do artigo 4.º do referido Protocolo, no prazo de seis meses a contar da data de adoção da presente diretiva, se procederá à transposição da presente diretiva para o seu direito nacional.
- (101) No que diz respeito à Islândia e à Noruega, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo celebrado pelo Conselho da União Europeia e a República da Islândia e o Reino da Noruega relativo à associação destes Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen <sup>(4)</sup>.

<sup>(1)</sup> Decisão 2008/615/JAI do Conselho, de 23 de junho de 2008, relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e a criminalidade transfronteiras (JO L 210 de 6.8.2008, p. 1).

<sup>(2)</sup> Ato do Conselho, de 29 de maio de 2000, que estabelece, nos termos do artigo 34.º do Tratado da União Europeia, a Convenção relativa ao auxílio judiciário mútuo em matéria penal entre os Estados-Membros da União Europeia (JO C 197 de 12.7.2000, p. 1).

<sup>(3)</sup> Diretiva 2011/93/UE do Parlamento Europeu e do Conselho, de 13 de dezembro de 2011, relativa à luta contra o abuso sexual e a exploração sexual de crianças e a pornografia infantil, e que substitui a Decisão-Quadro 2004/68/JAI do Conselho (JO L 335 de 17.12.2011, p. 1).

<sup>(4)</sup> JO L 176 de 10.7.1999, p. 36.

- (102) No que diz respeito à Suíça, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen <sup>(1)</sup>.
- (103) No que diz respeito ao Liechtenstein, a presente diretiva constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Liechtenstein relativo à adesão do Principado do Liechtenstein ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen <sup>(2)</sup>.
- (104) A presente diretiva respeita os direitos fundamentais e observa os princípios reconhecidos na Carta, consagrados pelo TFUE, nomeadamente o direito ao respeito da vida privada e familiar, o direito à proteção dos dados pessoais e o direito à ação e a um tribunal imparcial. As restrições introduzidas em relação a estes direitos são conformes com o artigo 52.º, n.º 1, da Carta, uma vez que são necessárias para cumprir os objetivos de interesse geral reconhecidos pela União ou para satisfazer a necessidade de proteger os direitos e as liberdades de outrem.
- (105) De acordo com a declaração política conjunta dos Estados-Membros e da Comissão, de 28 de setembro de 2011, sobre os documentos explicativos, os Estados-Membros assumiram o compromisso de fazer acompanhar a notificação das suas medidas de transposição, nos casos em que tal se justifique, de um ou mais documentos que expliquem a relação entre as componentes de uma diretiva e as partes correspondentes das disposições nacionais de transposição. Em relação à presente diretiva, o legislador considera que a transmissão desses documentos se justifica.
- (106) 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 7 de março de 2012 <sup>(3)</sup>.
- (107) A presente diretiva não obsta a que os Estados-Membros possam aplicar disposições respeitantes ao exercício dos direitos dos titulares de dados em matéria de informação, de acesso e de retificação ou apagamento dos dados pessoais e de limitação do tratamento no âmbito de uma ação penal, bem como eventuais restrições desses direitos, na legislação processual penal nacional,

ADOTARAM A PRESENTE DIRETIVA:

#### CAPÍTULO I

#### **Disposições gerais**

##### Artigo 1.º

#### **Objeto e objetivos**

1. A presente diretiva estabelece as regras relativas 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, incluindo a salvaguarda e prevenção de ameaças à segurança pública.
2. Nos termos da presente diretiva, os Estados-Membros asseguram:
  - a) A proteção dos direitos e das liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais; e
  - b) Que o intercâmbio de dados pessoais entre autoridades competentes na União, caso seja previsto pelo direito da União ou do Estado-Membro, não seja limitado nem proibido por razões relacionadas com a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

<sup>(1)</sup> JO L 53 de 27.2.2008, p. 52.

<sup>(2)</sup> JO L 160 de 18.6.2011, p. 21.

<sup>(3)</sup> JO C 192 de 30.6.2012, p. 7.

3. A presente diretiva não obsta a que os Estados-Membros prevejam garantias mais elevadas do que as nela estabelecidas para a proteção dos direitos e liberdades do titular dos dados no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes.

#### Artigo 2.º

##### Âmbito de aplicação

1. A presente diretiva aplica-se ao tratamento de dados pessoais pelas autoridades competentes para os efeitos estabelecidos no artigo 1.º, n.º 1.
2. A presente diretiva aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento de dados pessoais contidos num ficheiro ou a ele destinados por meios não automatizados.
3. A presente diretiva não se aplica ao tratamento de dados pessoais:
  - a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
  - b) Efetuado pelas instituições, organismos, serviços e agências da União.

#### Artigo 3.º

##### Definições

Para efeitos da presente diretiva, entende-se por:

- 1) «Dados pessoais», informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;
- 2) «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, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;
- 3) «Limitação do tratamento», a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;
- 4) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de 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;
- 5) «Pseudonimização», o tratamento de dados pessoais de forma a que deixem de poder ser atribuídos a um titular de dados específico sem recurso a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável;
- 6) «Ficheiro», um conjunto estruturado de dados pessoais acessíveis segundo critérios específicos, centralizado, descentralizado ou repartido de modo funcional ou geográfico;
- 7) «Autoridade competente»:
  - a) Uma autoridade pública competente 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; ou
  - b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer a autoridade pública e os poderes públicos 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;

- 8) «Responsável pelo tratamento», a autoridade competente que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento dos dados pessoais; caso as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou pelo direito de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro;
- 9) «Subcontratante», uma pessoa singular ou coletiva, uma autoridade pública, uma agência ou outro organismo que tratam dados pessoais por conta do responsável pelo tratamento;
- 10) «Destinatário», uma pessoa singular ou coletiva, uma autoridade pública, uma agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito de um Estado-Membro não são consideradas como destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento;
- 11) «Violação de dados pessoais», uma violação da segurança que provoca, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação não autorizada de dados pessoais transmitidos, conservados ou tratados de outro modo, ou o acesso não autorizado a esses dados;
- 12) «Dados genéticos», dados pessoais, relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular, que dão informações únicas sobre a sua fisiologia ou sobre a sua saúde e que resultam, designadamente, da análise de uma amostra biológica da pessoa singular em causa;
- 13) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitem ou confirmam a sua identificação única, tais como imagens faciais ou dados dactiloscópicos;
- 14) «Dados relativos à saúde», dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde;
- 15) «Autoridade de controlo», uma autoridade pública independente criada por um Estado-Membro nos termos do artigo 41.º;
- 16) «Organização internacional», uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza.

## CAPÍTULO II

### **Princípios**

#### *Artigo 4.º*

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

1. Os Estados-Membros preveem que os dados pessoais sejam:
  - a) Objeto de um tratamento lícito e leal;
  - b) Recolhidos para finalidades determinadas, explícitas e legítimas, e não tratados de uma forma incompatível com essas finalidades;
  - c) Adequados, pertinentes e limitados ao mínimo necessário relativamente às finalidades para as quais são tratados;
  - d) Exatos e atualizados sempre que necessário; devem ser tomadas todas as medidas razoáveis para que os dados inexatos, tendo em conta as finalidades para as quais são tratados, sejam apagados ou retificados sem demora;
  - 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;
  - f) Tratados de uma forma que garanta a sua segurança adequada, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas;

2. É permitido o tratamento pelo mesmo ou por outro responsável pelo tratamento para as finalidades previstas no artigo 1.º, n.º 1, diferentes da finalidade para a qual os dados pessoais foram recolhidos, desde que:
  - a) O responsável pelo tratamento esteja autorizado a tratar esses dados pessoais com essa finalidade, nos termos do direito da União ou dos Estados-Membros; e
  - b) O tratamento seja necessário e proporcionado para essa outra finalidade, nos termos do direito da União ou dos Estados-Membros.
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 artigo 1.º, n.º 1, sob reserva de garantias adequadas dos direitos e liberdades do titular dos dados.
4. O responsável pelo tratamento é responsável pelo cumprimento do disposto nos n.ºs 1, 2 e 3 e deve poder comprovar esse cumprimento.

#### Artigo 5.º

##### **Prazos para a conservação e avaliação**

Os Estados-Membros preveem prazos adequados para o apagamento dos dados pessoais ou para a avaliação periódica da necessidade de os conservar. Devem ser previstas regras processuais que garantam o cumprimento desses prazos.

#### Artigo 6.º

##### **Distinção entre diferentes categorias de titulares de dados**

Os Estados-Membros preveem que o responsável pelo tratamento estabeleça, se aplicável, e na medida do possível, uma distinção clara entre os dados pessoais de diferentes categorias de titulares de dados, tais como:

- a) Pessoas relativamente às quais existem motivos fundados para crer que cometeram ou estão prestes a cometer uma infração penal;
- b) Pessoas condenadas por uma infração penal;
- c) Vítimas de uma infração penal ou pessoas relativamente às quais certos factos levam a crer que possam vir a ser vítimas de uma infração penal; e
- d) Terceiros envolvidos numa infração penal, tais como pessoas que possam ser chamadas a testemunhar em investigações penais relacionadas com infrações penais ou em processos penais subsequentes, pessoas que possam fornecer informações sobre infrações penais, ou contactos ou associados de uma das pessoas a que se referem as alíneas a) e b).

#### Artigo 7.º

##### **Distinção entre dados pessoais e verificação da qualidade dos dados pessoais**

1. Os Estados-Membros preveem que os dados pessoais baseados em factos sejam, na medida do possível, distinguidos dos dados pessoais baseados em apreciações pessoais.
2. Os Estados-Membros preveem que as autoridades competentes tomem todas as medidas razoáveis para assegurar que os dados pessoais inexatos, incompletos ou desatualizados não possam ser transmitidos nem disponibilizados. Para o efeito, as autoridades competentes verificam, na medida do possível, a qualidade dos dados pessoais antes de estes serem transmitidos ou disponibilizados. Em todas as transmissões de dados pessoais devem ser fornecidas, na medida do possível, as informações necessárias para que a autoridade competente que as recebe possa apreciar até que ponto os dados são exatos, completos e fiáveis, e estão atualizados.
3. Se se verificar que foram transmitidos dados inexatos ou que foram transmitidos dados pessoais de forma ilícita, o destinatário deve ser informado sem demora. Neste caso, os dados pessoais são retificados ou apagados, ou o tratamento é limitado nos termos do artigo 16.º.

*Artigo 8.º***Licitude do tratamento**

1. Os Estados-Membros preveem que o tratamento só seja lícito se e na medida em que for necessário para o exercício de uma atribuição pela autoridade competente para os efeitos previstos no artigo 1.º, n.º 1, e tiver por base o direito da União ou de um Estado-Membro.
2. O direito de um Estado-Membro que rege o tratamento no âmbito da presente diretiva especifica pelo menos os objetivos do tratamento, os dados pessoais a tratar e as finalidades do tratamento.

*Artigo 9.º***Condições específicas do tratamento**

1. Os dados pessoais recolhidos pelas autoridades competentes para os fins do artigo 1.º, n.º 1, não podem ser tratados para fins diferentes dos previstos no artigo 1.º, n.º 1, a não ser que esse tratamento seja autorizado pelo direito da União ou de um Estado-Membro. Caso os dados pessoais sejam tratados para esses outros fins, é aplicável o Regulamento (UE) 2016/679, salvo se tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União.
2. Caso o direito dos Estados-Membros confie às autoridades competentes o exercício de atribuições diferentes das exercidas para os fins do artigo 1.º, n.º 1, o Regulamento (UE) 2016/679 é aplicável ao tratamento para esses fins, inclusive para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, salvo se o tratamento for efetuado no âmbito de uma atividade não sujeita à aplicação do direito da União.
3. Caso o direito da União ou dos Estados-Membros aplicável à autoridade transmissora competente preveja condições específicas para o tratamento, os Estados-Membros preveem que a autoridade transmissora competente informe o destinatário dos dados pessoais dessas condições e da obrigação de as cumprir.
4. Os Estados-Membros preveem que a autoridade transmissora competente não aplique condições ao abrigo do n.º 3 a destinatários situados noutros Estados-Membros nem a agências, organismos e órgãos criados nos termos do Título V, Capítulos 4 e 5, do TFUE, diferentes das aplicáveis a transmissões de dados similares no Estado-Membro da autoridade transmissora competente.

*Artigo 10.º***Tratamento de categorias especiais de dados pessoais**

O tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, o tratamento de dados genéticos, dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou à orientação sexual, só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se:

- a) For autorizado pelo direito da União ou de um Estado-Membro;
- b) Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou
- c) Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados.

*Artigo 11.º***Decisões individuais automatizadas**

1. Os Estados-Membros preveem a proibição de decisões tomadas exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produzam efeitos adversos na esfera jurídica do titular dos dados ou que o afetem de forma significativa, a menos que sejam autorizadas pelo direito da União ou do Estado-Membro ao qual o responsável pelo tratamento está sujeito, e que o direito da União ou desse Estado-Membro preveja garantias adequadas dos direitos e 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 8.º, a não ser que sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

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 10.º.

### *CAPÍTULO III*

#### ***Direitos do titular dos dados***

##### *Artigo 12.º*

#### **Comunicação e regras de exercício dos direitos dos titulares dos dados**

1. Os Estados-Membros preveem que o responsável pelo tratamento tome todas as medidas razoáveis para fornecer ao titular dos dados as informações a que se refere o artigo 13.º e efetue as comunicações relativas aos artigos 11.º, 14.º a 18.º e 31.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. Os Estados-Membros preveem que o responsável pelo tratamento facilite o exercício dos direitos do titular dos dados nos termos dos artigos 11.º e 14.º a 18.º.

3. Os Estados-Membros preveem que o responsável pelo tratamento informe por escrito, sem demora injustificada, o titular dos dados do seguimento dado ao seu pedido.

4. Os Estados-Membros preveem que as informações fornecidas nos termos do artigo 13.º e as comunicações efetuadas ou as medidas tomadas previstas nos termos dos artigos 11.º, 14.º a 18.º e 31.º, sejam gratuitas. Caso os pedidos de um titular dos dados sejam manifestamente infundados ou excessivos, particularmente devido ao seu carácter recorrente, o responsável pelo tratamento pode:

- a) Exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos da prestação das informações ou da comunicação ou da tomada das medidas solicitadas; ou
- b) Recusar dar seguimento ao pedido.

Nesses casos, cabe ao responsável pelo tratamento demonstrar o carácter manifestamente infundado ou excessivo dos pedidos.

5. Se tiver dúvidas razoáveis quanto à identidade da pessoa singular que apresenta o pedido a que se referem os artigos 14.º e 16.º, o responsável pelo tratamento pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.

##### *Artigo 13.º*

#### **Informações a facultar ou a fornecer ao titular dos dados**

1. Os Estados-Membros preveem que o responsável pelo tratamento faculte ao titular dos dados pelo menos as seguintes informações:

- a) A identidade e os contactos do responsável pelo tratamento;
- b) Os contactos do encarregado da proteção de dados, se for caso disso;
- c) As finalidades do tratamento a que os dados pessoais se destinam;
- d) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade;
- e) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que dizem respeito ao titular, bem como a sua retificação ou o seu apagamento e a limitação do tratamento.

2. Para além das informações a que se refere o n.º 1, os Estados-Membros preveem por lei que o responsável pelo tratamento forneça ao titular dos dados, em determinados casos, 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 ou, se tal não for possível, os critérios usados para definir esse período;



- c) Se aplicável, as categorias de destinatários dos dados pessoais, inclusive nos países terceiros ou nas organizações internacionais;
  - d) Se for caso disso, informações adicionais, especialmente se os dados pessoais forem recolhidos sem conhecimento do seu titular.
3. Os Estados-Membros podem adotar medidas legislativas que prevejam o adiamento, a limitação ou a não prestação aos titulares dos dados das informações a que se refere o n.º 2 se e enquanto tais 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;
  - d) Proteger a segurança nacional;
  - e) Proteger os direitos e as liberdades de terceiros.
4. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, por uma das alíneas do n.º 3.

#### Artigo 14.º

##### **Direito de acesso do titular dos dados aos seus dados pessoais**

Sem prejuízo do artigo 15.º, os Estados-Membros preveem que o titular dos dados tenha o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe dizem respeito estão ou não a ser objeto de tratamento e, em caso afirmativo, acesso aos seus dados pessoais e às seguintes informações:

- a) As finalidades e o fundamento jurídico do tratamento;
- b) As categorias dos dados pessoais em causa;
- c) Os destinatários ou as categorias de destinatários aos quais os dados pessoais foram divulgados, especialmente se se tratar de destinatários de países terceiros ou de organizações internacionais;
- d) Sempre que possível, o prazo previsto de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para fixar esse prazo;
- e) A existência do direito de solicitar ao responsável pelo tratamento a retificação ou o apagamento dos dados pessoais ou a limitação do tratamento dos dados pessoais que dizem respeito ao titular dos dados;
- f) O direito de apresentar reclamação à autoridade de controlo e de obter os contactos dessa autoridade;
- g) A comunicação dos dados pessoais sujeitos a tratamento e as informações disponíveis sobre a origem dos dados.

#### Artigo 15.º

##### **Limitações do direito de acesso**

1. Os Estados-Membros podem adotar medidas legislativas para limitar, total ou parcialmente, o direito de acesso do titular dos dados, se e enquanto tal limitação, total ou parcial, constituir uma medida necessária e proporcionada 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;

- d) Proteger a segurança nacional;
  - e) Proteger os direitos e as liberdades de terceiros.
2. Os Estados-Membros podem adotar medidas legislativas a fim de determinar as categorias de tratamento suscetíveis de ser abrangidas, total ou parcialmente, por uma das categorias previstas no n.º 1.
3. Nos casos a que se referem os n.ºs 1 e 2, os Estados-Membros preveem que o responsável pelo tratamento informe por escrito o titular dos dados, sem demora injustificada, 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. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados do direito que lhe assiste de apresentar reclamação à autoridade de controlo ou de intentar uma ação judicial.
4. Os Estados-Membros preveem que o responsável pelo tratamento detalhe os motivos de facto ou de direito em que a sua decisão se baseou. Essa informação deve ser facultada às autoridades de controlo.

#### Artigo 16.º

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

1. Os Estados-Membros preveem que o titular dos dados tenha o direito de obter sem demora injustificada do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta a finalidade do tratamento, os Estados-Membros preveem que o titular dos dados tenha direito a que os seus dados pessoais incompletos sejam completados, inclusive por meio de declaração adicional.
2. Os Estados-Membros exigem que o responsável pelo tratamento apague os dados pessoais sem demora injustificada e preveem que o titular dos dados tenha o direito de obter sem demora injustificada do responsável pelo tratamento o apagamento dos dados pessoais que lhe digam respeito caso o tratamento infrinja as disposições adotadas nos termos dos artigos 4.º, 8.º ou 10.º, ou caso os dados pessoais tenham de ser apagados a fim de cumprir 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 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 anular a limitação do tratamento.
4. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados, por escrito, de todos os casos de recusa da retificação ou do apagamento de dados pessoais ou da limitação do tratamento, e dos motivos da recusa. Os Estados-Membros podem adotar medidas legislativas que limitem, total ou parcialmente, a obrigação de fornecer essas 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 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;
  - d) Proteger a segurança nacional;
  - e) Proteger os direitos e as liberdades de terceiros.

Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados do direito de apresentar reclamação à autoridade de controlo ou de intentar ação judicial.

5. Os Estados-Membros preveem que o responsável pelo tratamento de dados comunique a retificação de dados pessoais inexatos à autoridade competente que está na origem dos dados pessoais inexatos.

6. Os Estados-Membros preveem que, caso os dados pessoais tenham sido retificados ou apagados ou o tratamento tenha sido limitado nos termos dos n.ºs 1, 2 e 3, o responsável pelo tratamento notifique os destinatários e estes retifiquem ou apaguem os dados pessoais ou limitem o tratamento de dados pessoais sob a sua responsabilidade.

#### *Artigo 17.º*

##### **Exercício dos direitos do titular dos dados e verificação pela autoridade de controlo**

1. Nos casos referidos no artigo 13.º, n.º 3, no artigo 15.º, n.º 3 e no artigo 16.º, n.º 4, os Estados-Membros adotam medidas que prevejam a possibilidade de os direitos do titular dos dados serem igualmente exercidos através da autoridade de controlo competente.

2. Os Estados-Membros preveem que o responsável pelo tratamento informe o titular dos dados que os seus direitos podem ser exercidos através da autoridade de controlo nos termos do n.º 1.

3. Se for exercido o direito referido no n.º 1, a autoridade de controlo informa, pelo menos, o titular dos dados de que procedeu a todas as verificações necessárias ou a um reexame. A autoridade de controlo informa também o titular dos dados acerca do seu direito de intentar ação judicial.

#### *Artigo 18.º*

##### **Direitos do titular dos dados no âmbito de investigações e ações penais**

Os Estados-Membros podem prever que os direitos referidos nos artigos 13.º, 14.º e 16.º sejam exercidos nos termos do direito dos Estados-Membros se os dados pessoais constarem de uma decisão judicial ou registo criminal ou de um processo objeto de tratamento no âmbito de uma investigação ou ação penal.

#### *CAPÍTULO IV*

##### **Responsável pelo tratamento e subcontratante**

#### *Secção 1*

##### **Obrigações gerais**

#### *Artigo 19.º*

##### **Obrigações do responsável pelo tratamento**

1. Os Estados-Membros preveem que o responsável pelo tratamento, 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 liberdades das pessoas singulares, aplique as medidas técnicas e organizativas adequadas para assegurar e poder comprovar que o tratamento é realizado em conformidade com a presente diretiva. Estas medidas são avaliadas e atualizadas, se necessário.

2. Caso sejam proporcionadas em relação às atividades de tratamento de dados, as medidas referidas no n.º 1 incluem a aplicação, pelo responsável pelo tratamento, de políticas adequadas em matéria de proteção de dados.

#### *Artigo 20.º*

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

1. Os Estados-Membros preveem que o responsável pelo tratamento, tendo em conta as técnicas mais avançadas e os custos da sua aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis que representa para os direitos e liberdades das pessoas singulares, aplique, tanto no momento da definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas — como a pseudonimização — concebidas para aplicar de forma eficaz os princípios da proteção de dados, como a minimização dos dados, e para integrar as garantias necessárias no tratamento de dados a fim de satisfazer os requisitos da presente diretiva e de proteger os direitos dos titulares dos dados.

2. Os Estados-Membros preveem que o responsável pelo tratamento aplique as medidas técnicas e organizativas adequadas que assegurem, por defeito, que apenas são tratados os dados pessoais necessários para cada finalidade específica do tratamento; tal aplica-se ao volume de dados pessoais recolhidos, à extensão do seu tratamento, ao prazo de conservação e à sua acessibilidade. Em especial, estas medidas asseguram que, por defeito, os dados pessoais não são disponibilizados a um número indeterminado de pessoas sem a intervenção da pessoa singular em causa.

#### Artigo 21.º

### Responsáveis conjuntos pelo tratamento

1. Os Estados-Membros preveem que, quando dois ou mais responsáveis pelo tratamento de dados determinam conjuntamente as finalidades e os meios do tratamento, ambos são responsáveis conjuntos pelo tratamento. Ambos determinam as respetivas responsabilidades por acordo entre si e de modo transparente, a fim de garantir o cumprimento da presente diretiva, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados, e os respetivos deveres de fornecer as informações referidas no artigo 13.º, a menos e na medida em que as suas responsabilidades respetivas sejam determinadas pelo direito da União ou do Estado-Membro a que estejam sujeitos. Desse acordo deve constar o ponto de contacto dos titulares dos dados. Os Estados-Membros podem determinar qual dos dois responsáveis conjuntos fica habilitado a agir como o ponto de contacto único para que os titulares dos dados exerçam os seus direitos.

2. Independentemente do acordo a que se refere o n.º 1, os Estados-Membros podem prever que o titular dos dados exerça, em relação a cada um dos responsáveis pelo tratamento de dados, os direitos que lhe conferem as disposições adotadas por força da presente diretiva.

#### Artigo 22.º

### Subcontratante

1. Os Estados-Membros preveem que, caso o tratamento de dados seja efetuado por conta do responsável pelo tratamento, este recorra apenas a subcontratantes que apresentem garantias suficientes de executar medidas técnicas e organizativas adequadas, de modo a que o tratamento satisfaça os requisitos estabelecidos na presente diretiva e assegure a proteção dos direitos do titular dos dados.

2. Os Estados-Membros preveem que o subcontratante não contrate outro subcontratante sem a autorização prévia específica ou geral por escrito do responsável pelo tratamento. Em caso de autorização geral por escrito, o subcontratante informa o responsável pelo tratamento de quaisquer alterações pretendidas quanto ao aditamento ou substituição de outros subcontratantes, dando, assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações.

3. Os Estados-Membros preveem que o tratamento em subcontratação seja regulada por um contrato ou outro ato normativo sujeito ao direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento e que estabeleça o objeto e a duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias de titulares de dados, as obrigações e os direitos do responsável pelo tratamento. Esse contrato ou outro ato normativo prevê, designadamente, 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 assumiram um compromisso de confidencialidade ou se encontram sujeitas às obrigações legais de confidencialidade adequada;
- 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) Apaga todos os dados pessoais ou devolve-os ao responsável pelo tratamento, consoante a escolha deste, depois de concluir os serviços de tratamento de dados, e apaga as cópias existentes, a menos que a sua conservação seja exigida pelo direito da União ou do Estado-Membro;

- e) Disponibiliza ao responsável pelo tratamento dos dados todas as informações necessárias para demonstrar o cumprimento do presente artigo;
  - f) Respeita as condições referidas nos n.ºs 2 e 3 na contratação de outro subcontratante.
4. O contrato ou outro ato normativo a que se refere o n.º 3 é feito por escrito, inclusivamente em formato eletrónico.
5. Se, em violação da presente diretiva, um subcontratante determinar as finalidades e os meios do tratamento, esse mesmo subcontratante é considerado responsável pelo tratamento em relação ao referido tratamento.

#### Artigo 23.º

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

Os Estados-Membros preveem que o subcontratante, bem como qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, não possa efetuar o seu tratamento sem instruções do responsável pelo tratamento, salvo se tal for previsto pelo direito da União ou de um Estado-Membro.

#### Artigo 24.º

### **Registos das atividades de tratamento**

1. Os Estados-Membros preveem que os responsáveis pelo tratamento conservem um registo de todas as categorias de atividades de tratamento sob a sua responsabilidade. Desse registo deve constar:
- a) O nome e contactos do responsável pelo tratamento de dados e, se for caso disso, do responsável conjunto pelo tratamento de dados e do encarregado da proteção de dados;
  - b) As finalidades do tratamento;
  - c) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros ou organizações internacionais;
  - d) A descrição das categorias de titulares de dados e das categorias de dados pessoais;
  - e) Se for caso disso, a utilização da definição de perfis;
  - f) Se for caso disso, as categorias de transferências de dados pessoais para um país terceiro ou uma organização internacional;
  - g) Uma indicação da fundamento jurídico da operação de tratamento, incluindo transferências, a que os dados pessoais se destinam;
  - h) Se possível, os prazos fixados para o apagamento das diferentes categorias de dados pessoais;
  - i) Se possível, uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 29.º, n.º 1.
2. Os Estados-Membros preveem que os subcontratantes conservem um registo de todas as categorias de atividades de tratamento realizadas em nome de um responsável pelo tratamento, do qual constem:
- a) O nome e contactos do subcontratante ou subcontratantes, de cada responsável pelo tratamento em nome do qual atua o subcontratante, bem como do encarregado da proteção de dados, se for caso disso;
  - b) As categorias de tratamentos de dados efetuados em nome de cada responsável pelo tratamento;
  - c) Se for caso disso, as transferências de dados pessoais para um país terceiro ou uma organização internacional se o responsável pelo tratamento der instruções explícitas nesse sentido, incluindo a identificação desse país terceiro ou dessa organização internacional;
  - d) Se possível, uma descrição geral das medidas técnicas e organizativas em matéria de segurança referidas no artigo 29.º, n.º 1.

3. Os registos a que se referem os n.ºs 1 e 2 são conservados por escrito, inclusivamente em formato eletrónico.

O responsável pelo tratamento e o subcontratante facultam o registo à autoridade de controlo, a pedido desta.

#### *Artigo 25.º*

##### **Registo cronológico**

1. Os Estados-Membros preveem que sejam conservados em sistemas de tratamento automatizado registos cronológicos pelo menos das seguintes operações de tratamento: recolha, alteração, consulta, divulgação — incluindo transferências —, interconexão e apagamento. Os registos cronológicos das operações de consulta e divulgação permitem determinar o motivo, a data e a hora dessas operações e, na medida do possível, a identificação da pessoa que consultou ou divulgou dados pessoais, e a identidade dos destinatários desses dados pessoais.
2. Os registos cronológicos são utilizados exclusivamente para efeitos de verificação da licitude do tratamento, autocontrolo e garantia da integridade e segurança dos dados pessoais, bem como para ações penais.
3. O responsável pelo tratamento e o subcontratante disponibilizam os registos cronológicos à autoridade de controlo, a pedido desta.

#### *Artigo 26.º*

##### **Cooperação com a autoridade de controlo**

Os Estados-Membros preveem que o responsável pelo tratamento e o subcontratante cooperem, a pedido, com a autoridade de controlo no exercício das suas atribuições.

#### *Artigo 27.º*

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

1. Caso um tipo de tratamento, em particular que utilize novas tecnologias, e tendo em conta a sua natureza, âmbito, contexto e finalidades, seja suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, os Estados-Membros preveem que o responsável efetue, antes de iniciar o tratamento, uma avaliação do impacto das operações de tratamento previstas na proteção dos dados pessoais.
2. A avaliação a que se refere o n.º 1 inclui pelo menos uma descrição geral das operações de tratamento de dados previstas, uma avaliação dos riscos para os direitos e liberdades dos titulares dos dados, as medidas previstas para fazer face a esses riscos, as garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade com a presente diretiva, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.

#### *Artigo 28.º*

##### **Consulta prévia da autoridade de controlo**

1. Os Estados-Membros preveem que o responsável pelo tratamento ou o subcontratante consulte a autoridade de controlo antes de proceder ao tratamento de dados pessoais que farão parte de um novo ficheiro a criar caso:
  - a) A avaliação de impacto sobre a proteção de dados prevista no artigo 27.º indique que o tratamento resultaria num elevado risco na ausência das medidas a tomar pelo responsável pelo tratamento para atenuar o risco; ou
  - b) O tipo de tratamento envolva, especialmente no caso de se utilizarem novas tecnologias, mecanismos ou procedimentos, um elevado risco para os direitos e liberdades dos titulares dos dados.
2. Os Estados-Membros preveem que a autoridade de controlo seja consultada durante a elaboração de propostas de medidas legislativas a adotar por um parlamento nacional ou de medidas regulamentares baseadas nessas medidas legislativas, quando tais propostas estejam relacionadas com o tratamento.
3. Os Estados-Membros preveem que a autoridade de controlo possa estabelecer uma lista das operações de tratamento de dados sujeitas a consulta prévia nos termos do n.º 1.

4. Os Estados-Membros preveem que o responsável pelo tratamento forneça à autoridade de controlo a avaliação de impacto sobre a proteção de dados nos termos do artigo 27.º e, quando solicitado, qualquer outra informação que permita à autoridade de controlo avaliar a conformidade do tratamento e, nomeadamente, os riscos para a proteção dos dados pessoais do titular dos dados e as respetivas garantias.

5. Os Estados-Membros preveem que, caso considere que o tratamento previsto referido no n.º 1 do presente artigo violaria as disposições adotadas nos termos da presente diretiva, especialmente se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, no prazo de seis semanas a contar da receção do pedido de consulta, dê orientações, por escrito, ao responsável pelo tratamento e, se aplicável, ao subcontratante e possa recorrer a todos os seus poderes referidos no artigo 47.º. Esse prazo pode ser prorrogado por um mês, tendo em conta a complexidade do tratamento previsto. A autoridade de controlo informa o responsável pelo tratamento e, se for caso disso, o subcontratante dessa prorrogação e dos seus fundamentos no prazo de um mês a contar da data de receção do pedido de consulta.

## Secção 2

### Segurança dos dados pessoais

#### Artigo 29.º

#### Segurança do tratamento

1. Os Estados-Membros preveem que o responsável pelo tratamento e o subcontratante, 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 de probabilidade e gravidade variáveis que este tratamento representa para os direitos e liberdades das pessoas singulares, apliquem medidas técnicas e organizativas adequadas a fim de assegurar um nível de segurança adequado ao risco, em especial no que respeita ao tratamento das categorias especiais de dados pessoais a que se refere o artigo 10.º.

2. No que respeita ao tratamento automatizado de dados, cada Estado-Membro prevê que o responsável pelo tratamento ou o subcontratante, na sequência de uma avaliação dos riscos, aplique medidas para os seguintes efeitos:

- a) Impedir o acesso de pessoas não autorizadas ao equipamento utilizado para o tratamento («controlo de acesso ao equipamento»);
- b) Impedir que os suportes de dados sejam lidos, copiados, alterados ou retirados sem autorização («controlo dos suportes de dados»);
- c) Impedir a introdução não autorizada de dados pessoais, bem como qualquer inspeção, alteração ou apagamento não autorizados de dados pessoais conservados («controlo da conservação»);
- d) Impedir que os sistemas de tratamento automatizado sejam utilizados por pessoas não autorizadas por meio de equipamento de comunicação de dados («controlo dos utilizadores»);
- e) Assegurar que as pessoas autorizadas a utilizar um sistema de tratamento automatizado só tenham acesso aos dados pessoais abrangidos pela sua autorização de acesso («controlo do acesso aos dados»);
- f) Assegurar que possa ser verificado e determinado a organismos os dados pessoais foram ou podem ser transmitidos ou facultados utilizando equipamento de comunicação de dados («controlo da comunicação»);
- g) Assegurar que possa ser verificado e determinado *a posteriori* quais os dados pessoais introduzidos nos sistemas de tratamento automatizado, quando e por quem («controlo da introdução»);
- h) Impedir que, durante as transferências de dados pessoais ou o transporte de suportes de dados, os dados pessoais possam ser lidos, copiados, alterados ou suprimidos sem autorização («controlo do transporte»);
- 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 conservados não possam ser falseados por um disfuncionamento do sistema («integridade»).

*Artigo 30.º***Notificação de uma violação de dados pessoais à autoridade de controlo**

1. Os Estados-Membros preveem que, em caso de violação de dados pessoais, o responsável pelo tratamento notifique desse facto a autoridade de controlo sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação da autoridade de controlo não for feita no prazo de 72 horas, é acompanhada dos motivos do atraso.
2. O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais.
3. A notificação referida no n.º 1 deve, pelo menos:
  - a) Descrever a natureza da violação de dados pessoais incluindo, se possível e adequado, as categorias e número aproximados de titulares dos dados afetados, bem como 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 ou de outro ponto de contacto onde possam ser obtidas informações adicionais;
  - 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, inclusive, se for caso disso, para atenuar os seus eventuais efeitos negativos.
4. Caso, e na medida em que, não seja possível fornecer as informações ao mesmo tempo, estas podem ser fornecidas por fases sem demora injustificada.
5. Os Estados-Membros preveem que o responsável pelo tratamento documente qualquer violação de dados pessoais referida no n.º 1, compreendendo os factos relacionados com a violação de dados pessoais, os seus efeitos e as medidas de reparação adotadas. Essa documentação deve permitir à autoridade de controlo verificar o cumprimento do disposto no presente artigo.
6. Os Estados-Membros preveem que, caso a violação de dados pessoais envolva dados pessoais que tenham sido transmitidos pelo ou ao responsável pelo tratamento de outro Estado-Membro, as informações referidas no n.º 3 sejam comunicadas sem demora injustificada ao responsável pelo tratamento deste último Estado-Membro.

*Artigo 31.º***Comunicação de uma violação de dados pessoais ao titular dos dados**

1. Os Estados-Membros preveem que, quando a violação dos dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunique a violação de dados pessoais ao titular dos dados sem demora injustificada.
2. A comunicação ao titular dos dados referida no n.º 1 do presente artigo descreve numa linguagem clara e simples a natureza da violação dos dados pessoais e inclui, pelo menos, as informações e as medidas referidas no artigo 30.º, n.º 3, alíneas b), c) e d).
3. A comunicação ao titular dos dados referida no n.º 1 não é exigida se:
  - a) O responsável pelo tratamento de dados tiver aplicado medidas de proteção adequadas, tanto tecnológicas como organizativas, e essas medidas tiverem sido aplicadas aos dados afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, como, por exemplo, a cifragem; ou
  - b) O responsável pelo tratamento de dados tiver tomado medidas subsequentes capazes de assegurar que a ocorrência de elevado risco para os direitos e liberdades dos titulares referida no n.º 1 deixou de ser provável; ou
  - c) Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.



4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controlo, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir que o referido responsável proceda a essa notificação, ou pode decidir que se encontra preenchida uma das condições referidas no n.º 3.

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 enunciados no artigo 13.º, n.º 3.

### Secção 3

## **Encarregado da proteção de dados**

### *Artigo 32.º*

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

1. Os Estados-Membros preveem que o responsável pelo tratamento designe um encarregado da proteção de dados. Os Estados-Membros podem isentar dessa obrigação os tribunais e outras autoridades judiciais independentes no exercício da sua função jurisdicional.
2. O encarregado da proteção de dados é designado com base nas suas qualidades profissionais e, em especial, nos seus conhecimentos especializados no domínio da legislação e práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 34.º.
3. Pode ser designado um único encarregado da proteção de dados para várias autoridades competentes, tendo em conta a sua dimensão e estrutura organizativa.
4. Os Estados-Membros preveem que o responsável pelo tratamento dos dados publique os contactos do encarregado da proteção de dados e os comunique à autoridade de controlo.

### *Artigo 33.º*

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

1. Os Estados-Membros preveem que o responsável pelo tratamento assegure que o encarregado da proteção de dados seja envolvido, de forma adequada e em tempo útil, em todas as questões relacionadas com a proteção de dados pessoais.
2. O responsável pelo tratamento dos dados apoia o encarregado da proteção de dados no desempenho das funções a que se refere o artigo 34.º, fornecendo-lhe os recursos necessários para o efeito e para a manutenção dos seus conhecimentos, e dando-lhe acesso aos dados pessoais e às operações de tratamento.

### *Artigo 34.º*

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

Os Estados-Membros preveem que o responsável pelo tratamento confie ao encarregado da proteção de dados, pelo menos, as seguintes funções:

- a) Informar e aconselhar o responsável pelo tratamento dos dados e os empregados que efetuem o tratamento quanto às obrigações que lhes incumbem por força da presente diretiva e a outras disposições da União ou dos Estados-Membros de proteção de dados;
- b) Fiscalizar a conformidade com a presente diretiva, com outras disposições da União ou dos Estados-Membros de proteção de dados e com as políticas do responsável pelo tratamento de dados em matéria de proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados e as auditorias correspondentes;
- c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controlar a sua realização nos termos do artigo 27.º;
- d) Cooperar com a autoridade de controlo;
- e) Ponto de contacto para a autoridade de controlo em assuntos relacionados com o tratamento, incluindo a consulta prévia referida no artigo 28.º, e aconselhar esta autoridade, se for caso disso, sobre qualquer outro assunto.

## CAPÍTULO V

***Transferências de dados pessoais para países terceiros ou organizações internacionais*****Artigo 35.º****Princípios gerais das transferências de dados pessoais**

1. Os Estados-Membros preveem que qualquer transferência, por parte das autoridades competentes, de dados pessoais que sejam ou se destinem a ser objeto de tratamento após transferência para um país terceiro ou uma organização internacional, inclusivamente que se destinem a transferências ulteriores para outro país terceiro ou outra organização internacional, só possa ser efetuada nos termos das disposições nacionais adotadas por força de outras disposições da presente diretiva, se forem preenchidas as condições previstas neste capítulo, a saber:

- a) A transferência se necessária para a consecução das finalidades estabelecidas no artigo 1.º, n.º 1;
- b) Os dados pessoais serem transferidos para um responsável pelo tratamento no país terceiro ou na organização internacional que seja uma autoridade competente para as finalidades referidas no artigo 1.º, n.º 1;
- c) Caso os dados pessoais sejam transmitidos ou disponibilizados por outro Estado-Membro, esse Estado ter dado o seu consentimento prévio à transferência nos termos do seu direito nacional;
- d) A Comissão ter adotado uma decisão de adequação nos termos do artigo 36.º ou, na falta dessa decisão de adequação, terem sido apresentadas ou existirem garantias adequadas nos termos do artigo 37.º, ou, na falta de decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, se forem aplicáveis derrogações a situações específicas nos termos do artigo 38.º; e
- e) No caso de uma transferência ulterior para um país terceiro ou uma organização internacional, a autoridade competente que realizou a transferência inicial, ou outra autoridade competente do mesmo Estado-Membro, autorizar a transferência ulterior após ter em conta todos os fatores pertinentes, incluindo a gravidade da infração penal, a finalidade para que os dados pessoais foram transferidos inicialmente e o nível de proteção dos dados pessoais no país terceiro ou na organização internacional para os quais os dados pessoais são ulteriormente transferidos.

2. Os Estados-Membros preveem que as transferências sem consentimento prévio de outro Estado-Membro nos termos do n.º 1, alínea c), só sejam permitidas se a transferência de dados pessoais for necessária para prevenir uma ameaça imediata e grave à segurança pública de um Estado-Membro ou de um país terceiro ou aos interesses essenciais de um Estado-Membro e o consentimento prévio não puder ser obtido em tempo útil. A autoridade responsável por dar o consentimento prévio é informada sem demora.

3. Todas as disposições do presente capítulo são aplicadas de forma a assegurar que não fique comprometido o nível de proteção das pessoas singulares assegurado pela presente diretiva.

**Artigo 36.º****Transferências com base numa decisão de adequação**

1. Os Estados-Membros preveem que uma transferência de dados pessoais para um país terceiro ou uma organização internacional possa ser efetuada se a Comissão tiver determinado que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Esta transferência não exige autorização específica.

2. Ao avaliar a adequação do nível de proteção, a Comissão tem particularmente em conta os seguintes elementos:

- a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação desta legislação, das regras de proteção de dados, das regras profissionais e das medidas de segurança relativas à proteção de dados, incluindo as regras para transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e meios efetivos de recurso administrativo e judicial para os titulares dos dados cujos dados pessoais sejam objeto de transferência;
- b) A existência e o funcionamento efetivo de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e fazer cumprir as regras de proteção de dados e dotadas de poderes sancionatórios adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e por cooperar com as autoridades de controlo dos Estados-Membros; e

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

3. Uma vez avaliada a adequação do nível de proteção, a Comissão pode decidir, por meio de um ato de execução, que um país terceiro, um território, um ou mais setores específicos desse país terceiro, ou uma organização internacional, assegura um nível de proteção adequado na aceção do n.º 2 do presente artigo. O ato de execução prevê um processo de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. O ato de execução especifica o âmbito de aplicação territorial e setorial e, se existir, identifica a autoridade ou autoridades de controlo a que se refere o n.º 2, alínea b) do presente artigo. O ato de execução é adotado pelo procedimento de exame a que se refere o artigo 58.º, n.º 2.

4. A Comissão controla, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar o funcionamento das decisões adotadas nos termos do n.º 3.

5. A Comissão, sempre que a informação disponível revelar, nomeadamente na sequência da revisão a que se refere o n.º 3 do presente artigo, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, deixou de assegurar um nível de proteção adequado na aceção do n.º 2 do presente artigo, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3 do presente artigo, por meio de atos de execução sem efeitos retroativos. Esses atos de execução são adotados pelo procedimento de exame a que se refere o artigo 58.º, n.º 2.

Por imperativos de urgência devidamente justificados, a Comissão adota atos de execução imediatamente aplicáveis pelo procedimento a que se refere o artigo 58.º, n.º 3.

6. A Comissão inicia consultas com o país terceiro ou a organização internacional com vista a remediar a situação que tiver dado origem à decisão adotada nos termos do n.º 5.

7. Os Estados-Membros preveem que as decisões adotadas nos termos do n.º 5 não prejudicam as transferências de dados pessoais para o país terceiro, o território ou o setor específico desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 37.º e 38.º.

8. A Comissão publica no *Jornal Oficial da União Europeia* e no seu sítio *web* uma lista dos países terceiros, territórios e setores específicos de um país terceiro e de organizações internacionais relativamente aos quais tenha declarado, mediante decisão, se asseguram ou não um nível de proteção adequado.

#### Artigo 37.º

#### Transferências sujeitas a garantias adequadas

1. Na falta de uma decisão nos termos do artigo 36.º, n.º 3, os Estados-Membros preveem a possibilidade de se transferirem dados pessoais para um país terceiro ou organização internacional se:

- a) Tiverem sido apresentadas garantias adequadas no que diz respeito à proteção de dados pessoais mediante um instrumento juridicamente vinculativo; ou
- b) O responsável pelo tratamento de dados tiver avaliado todas as circunstâncias inerentes à transferência de dados pessoais e concluído que existem garantias adequadas no que diz respeito à proteção desses dados.

2. O responsável pelo tratamento informa a autoridade de controlo sobre as categorias de transferências abrangidas pelo n.º 1, alínea b).

3. As transferências baseadas no n.º 1, alínea b), são documentadas, devendo a documentação ser disponibilizada à autoridade de controlo, a pedido desta, incluindo a data e hora da transferência, informações acerca da autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

*Artigo 38.º***Derrogações aplicáveis a situações específicas**

1. Na falta de uma decisão de adequação nos termos do artigo 36.º ou de garantias adequadas nos termos do artigo 37.º, os Estados-Membros preveem que só se possa efetuar uma transferência ou uma categoria de transferências de dados pessoais para um país terceiro ou uma organização internacional se a transferência for necessária:
  - a) Para proteger os interesses vitais do titular dos dados ou de outra pessoa;
  - b) Para salvaguardar os legítimos interesses do titular dos dados caso a legislação do Estado-Membro que transfere os dados pessoais o preveja;
  - c) Para prevenir uma ameaça imediata e grave contra a segurança pública de um Estado-Membro ou de um país terceiro;
  - d) Em determinados casos, para a consecução das finalidades estabelecidas no artigo 1.º, n.º 1; ou
  - e) Num dado caso, para declarar, exercer ou defender num processo judicial um direito relacionado com as finalidades estabelecidas no artigo 1.º, n.º 1.
2. Os dados pessoais não são transferidos se a autoridade competente que procede à transferência determinar que, aquando da transferência referida no n.º 1, alíneas d) e e), os direitos e liberdades fundamentais do titular dos dados em causa primam sobre o interesse público.
3. As transferências baseadas no n.º 1 são documentadas, devendo a documentação ser disponibilizada à autoridade de controlo, a pedido desta, incluindo a data e hora da transferência, informações acerca da autoridade competente que as recebe, a justificação da transferência e os dados pessoais transferidos.

*Artigo 39.º***Transferências de dados pessoais para destinatários estabelecidos em países terceiros**

1. Em derrogação do artigo 35.º, n.º 1, alínea b), e sem prejuízo de qualquer acordo internacional referido no n.º 2 do presente artigo, o direito da União ou dos Estados-Membros pode prever a possibilidade de, em determinados casos específicos, as autoridades competentes referidas no artigo 3.º, ponto 7), alínea a), transferirem dados pessoais diretamente para destinatários estabelecidos em países terceiros unicamente no caso de serem cumpridas as demais disposições da presente diretiva e preenchidas todas as seguintes condições:
  - a) A transferência é estritamente necessária a uma função desempenhada pela autoridade competente que efetua a transferência e prevista pelo direito da União ou dos Estados-Membros tendo em vista a consecução das finalidades estabelecidas no artigo 1.º, n.º 1;
  - b) A autoridade competente que efetua a transferência determina que nenhum direito ou liberdade fundamental do titular dos dados em causa prevalece sobre o interesse público que exige a transferência no caso em apreço;
  - c) A autoridade competente que efetua a transferência considera que a transferência para uma autoridade que é competente para os efeitos referidos no artigo 1.º, n.º 1, no país terceiro se revela ineficaz ou desadequada, nomeadamente por não ser possível efetua-la em tempo útil;
  - d) A autoridade que é competente para os efeitos referidos no artigo 1.º, n.º 1, no país terceiro é informada sem demora injustificada, a menos que tal se revele ineficaz ou inadequado; e
  - e) A autoridade competente que efetua a transferência informa o destinatário da finalidade ou finalidades específicas para as quais o destinatário apenas pode tratar os dados pessoais, desde que o tratamento seja necessário.
2. Por «acordo internacional» a que se refere o n.º 1 entende-se um acordo internacional bilateral ou multilateral em vigor entre os Estados-Membros e países terceiros no domínio da cooperação judiciária em matéria penal e da cooperação policial.
3. A autoridade competente que efetua a transferência informa a autoridade de controlo sobre as transferências abrangidas pelo presente artigo.
4. As transferências efetuadas nos termos do n.º 1 devem ser documentadas.

*Artigo 40.º***Cooperação internacional no domínio da proteção de dados pessoais**

Em relação a países terceiros e a organizações internacionais, a Comissão e os Estados-Membros adotam as medidas necessárias destinadas a:

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

*CAPÍTULO VI****Autoridades de controlo independentes****Secção 1***Estatuto independente***Artigo 41.º***Autoridade de controlo**

1. Cada Estado-Membro prevê que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação da presente diretiva, a fim de proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e de facilitar a livre circulação desses dados na União («autoridade de controlo»).
2. Cada autoridade de controlo contribui para a aplicação coerente da presente diretiva em toda a União. Para esse efeito, as autoridades de controlo cooperam entre si e com a Comissão nos termos do Capítulo VII.
3. Os Estados-Membros podem prever que uma autoridade de controlo criada pelo Regulamento (UE) 2016/679 seja a autoridade de controlo a que se refere a presente diretiva e assuma as funções de autoridade de controlo a definir nos termos do n.º 1 do presente artigo.
4. Se for criada mais do que uma autoridade de controlo num Estado-Membro, o Estado-Membro em questão designa a autoridade de controlo que representa as demais no Comité a que se refere o artigo 51.º.

*Artigo 42.º***Independência**

1. Os Estados-Membros preveem que cada autoridade de controlo aja com total independência no exercício das suas atribuições e dos poderes que lhe forem atribuídos nos termos da presente diretiva.
2. Os Estados-Membros preveem que os membros das autoridades de controlo, no desempenho das suas funções e no exercício dos poderes nos termos da presente diretiva, não estejam sujeitos a influências externas, diretas ou indiretas, e não solicitem nem recebam instruções de outrem.
3. Os membros das autoridades de controlo dos Estados-Membros abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar qualquer atividade profissional incompatível, remunerada ou não.
4. Os Estados-Membros asseguram que as suas autoridades de controlo disponham dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários ao exercício eficaz das suas atribuições e dos seus poderes, designadamente no contexto da assistência mútua, da cooperação e da participação no Comité.

5. Os Estados-Membros asseguram que as suas autoridades de controlo escolham e disponham do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controlo interessadas.

6. Os Estados-Membros asseguram que as suas autoridades de controlo fiquem sujeitas a um controlo financeiro que não afete a sua independência e que disponham de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou no orçamento nacional.

#### Artigo 43.º

##### **Condições gerais aplicáveis aos membros da autoridade de controlo**

1. Os Estados-Membros preveem que cada membro das respetivas autoridades de controlo seja nomeado por procedimento transparente:

- pelo Parlamento,
- pelo Governo,
- pelo Chefe de Estado, ou
- por um organismo independente incumbido da nomeação nos termos do direito do Estado-Membro.

2. Cada membro possui as habilitações, a experiência e os conhecimentos técnicos necessários, nomeadamente no domínio da proteção de dados pessoais, ao desempenho das suas funções e ao exercício dos seus poderes.

3. As funções de membro da autoridade de controlo cessam findo o seu mandato, com a sua exoneração ou aposentação compulsiva, nos termos do direito do Estado-Membro em causa.

4. Um membro pode ser exonerado apenas se tiver cometido uma falta grave ou se tiver deixado de cumprir os requisitos previstos para o exercício das suas funções.

#### Artigo 44.º

##### **Regras aplicáveis à criação da autoridade de controlo**

1. Cada Estado-Membro estabelece por lei:

- a) A criação da respetiva autoridade de controlo;
- b) As qualificações e condições de elegibilidade necessárias para a nomeação dos membros da respetiva autoridade de controlo;
- c) As regras e procedimentos aplicáveis à nomeação dos membros da respetiva autoridade de controlo;
- d) A duração do mandato dos membros da respetiva autoridade de controlo, que não deve ser inferior a quatro anos, salvo no caso do primeiro mandato após 6 de maio de 2016, que pode ser mais curta caso seja necessário preservar a independência da autoridade de controlo através de um procedimento de nomeações escalonadas;
- e) Se for caso disso, o número máximo, de mandatos dos membros da respetiva autoridade de controlo;
- f) As condições que regem as obrigações dos membros e do pessoal da respetiva autoridade de controlo, a proibição das ações, funções e benefícios que com elas são incompatíveis durante o mandato e após o seu termo e as normas que regem a cessação da relação de trabalho.

2. Os membros e o pessoal de cada autoridade de controlo ficam sujeitos, nos termos do direito da União ou dos Estados-Membros, à obrigação de sigilo profissional, tanto durante o seu mandato como após o seu termo, no que respeita a quaisquer informações confidenciais a que tenham tido acesso no desempenho das suas funções ou no exercício dos seus poderes. Durante o seu mandato, essa obrigação de sigilo profissional aplica-se, em especial, à comunicação por pessoas singulares das violações da presente diretiva.

## Secção 2

**Competência, atribuições e poderes***Artigo 45.º***Competência**

1. Os Estados-Membros preveem que a respetiva autoridade de controlo seja competente para, no respetivo território, exercer as atribuições e os poderes que lhe são conferidos pela presente diretiva.
2. Os Estados-Membros preveem que a respetiva autoridade de controlo não seja responsável pela supervisão de operações de tratamento efetuadas pelos tribunais no exercício da sua função jurisdicional. Os Estados-Membros podem estabelecer que a respetiva autoridade de controlo não tenha competência para supervisionar operações de tratamento efetuadas por outras autoridades judiciais independentes no exercício da sua função jurisdicional

*Artigo 46.º***Atribuições**

1. Os Estados-Membros preveem que, no território respetivo, cada autoridade de controlo:
  - a) Fiscalize e faça aplicar a presente diretiva e as suas medidas de execução;
  - b) Promova a sensibilização e a compreensão do público relativamente aos riscos, regras, garantias e direitos associados ao tratamento;
  - c) Aconselhe, nos termos do direito do Estado-Membro, o Parlamento nacional, o Governo e outras instituições e organismos quanto às medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades das pessoas singulares em matéria de tratamento;
  - d) Promova a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as obrigações que lhes incumbem nos termos da presente diretiva;
  - e) Se tal lhe for solicitado, preste informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos da presente diretiva e, se adequado, coopere para esse efeito com as autoridades de controlo de outros Estados-Membros;
  - f) Trate de reclamações apresentadas pelos titulares de dados ou por um organismo, organização ou associação, nos termos do artigo 55.º, e investigue, na medida do necessário, o conteúdo da reclamação, informando o autor da reclamação do andamento e do resultado da investigação num prazo razoável, especialmente se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;
  - g) Verifique a licitude do tratamento nos termos do artigo 17.º e, num prazo razoável, informe o respetivo titular do resultado da verificação, conforme previsto no n.º 3 desse artigo, ou dos motivos que impediram a sua realização;
  - h) Coopere, nomeadamente partilhando informações, e preste assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução da presente diretiva;
  - i) Conduza investigações sobre a aplicação da presente diretiva, nomeadamente com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;
  - j) Acompanhe factos novos relevantes na medida em que tenham incidência na proteção de dados pessoais, particularmente a evolução a nível das tecnologias da informação e comunicação;
  - k) Preste aconselhamento sobre as operações de tratamento referidas no artigo 28.º;
  - l) Contribua para as atividades do Comité.
2. As autoridades de controlo facilitam a apresentação das reclamações previstas no n.º 1, alínea f), tomando certas medidas, como, por exemplo, fornecer formulários para apresentação de reclamações que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.

3. O exercício das atribuições de cada autoridade de controlo é gratuito para o titular dos dados e para o encarregado da proteção de dados.
4. Caso os pedidos sejam manifestamente infundados ou excessivos, particularmente devido ao seu carácter recorrente, a autoridade de controlo pode exigir o pagamento de uma taxa razoável, com base nos custos administrativos, ou indeferir-lhes. Cabe à autoridade de controlo demonstrar o carácter manifestamente infundado ou excessivo do pedido.

#### Artigo 47.º

##### **Poderes**

1. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo detenha poderes de investigação efetivos. Esses poderes incluem, pelo menos, o poder de obter do responsável pelo tratamento de dados e do subcontratante autorização de acesso a todos os dados pessoais objeto de tratamento e a todas as informações necessárias ao exercício das suas atribuições.
2. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha poderes de correção efetivos, como, por exemplo:
  - a) Advertir o responsável pelo tratamento de dados ou o subcontratante de que as operações de tratamento previstas são suscetíveis de violar as disposições adotadas por força da presente diretiva;
  - b) Ordenar ao responsável pelo tratamento de dados ou ao subcontratante que, na medida do necessário, proceda por forma a que as operações de tratamento cumpram as disposições adotadas por força da presente diretiva, de determinada forma e num prazo determinado; em especial, ordenar a retificação ou apagamento dos dados pessoais ou a limitação tratamento nos termos do artigo 16.º;
  - c) Impor uma limitação temporária ou definitiva, inclusive uma proibição, ao tratamento.
3. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha poderes consultivos efetivos para aconselhar o responsável pelo tratamento de dados pelo procedimento de consulta prévia previsto no artigo 28.º e emitir, por iniciativa própria ou a pedido, pareceres dirigidos ao seu Parlamento nacional, ao seu Governo ou, nos termos do direito do Estado-Membro, a outras instituições e organismos, bem como ao público, sobre qualquer questão relacionada com a proteção de dados pessoais.
4. O exercício dos poderes conferidos à autoridade de controlo nos termos do presente artigo está sujeito a garantias adequadas, incluindo o direito à ação judicial e a um processo equitativo, previstas no direito da União e dos Estados-Membros em conformidade com a Carta.
5. Cada Estado-Membro prevê, por lei, que a sua autoridade de controlo tenha o poder de apresentar as violações das disposições adotadas por força da presente diretiva ao conhecimento das autoridades judiciais e, se adequado, de intentar ou de outro modo intervir em processos judiciais, a fim de fazer aplicar as disposições adotadas por força da presente diretiva.

#### Artigo 48.º

##### **Comunicação das violações**

Os Estados-Membros preveem que as autoridades competentes aplicam procedimentos eficazes para incentivar a comunicação confidencial das violações da presente diretiva.

#### Artigo 49.º

##### **Relatório de atividades**

Cada autoridade de controlo elabora um relatório anual de atividades, que pode incluir uma lista dos tipos de violações notificadas e dos tipos de sanções aplicadas. Esses relatórios são apresentados ao Parlamento nacional, ao Governo e às outras autoridades designadas pelo direito do Estado-Membro. Os relatórios são disponibilizados ao público, à Comissão e ao Comité.



## CAPÍTULO VII

**Cooperação**

## Artigo 50.º

**Assistência mútua**

1. Os Estados-Membros preveem que as suas autoridades de controlo prestem entre si informações relevantes e assistência mútua a fim de executar e aplicar a presente diretiva de forma coerente, e ponham em prática medidas para cooperar eficazmente entre si. A assistência mútua abrange, em especial, os pedidos de informação e as medidas de controlo, como os pedidos de consulta, inspeção e investigação.
2. Os Estados-Membros preveem que cada autoridade de controlo tome todas as medidas adequadas para responder aos pedidos de outra autoridade de controlo sem demora injustificada e, o mais tardar, um mês após a receção do pedido. Essas medidas podem incluir, particularmente, a transmissão de informações úteis sobre a condução de uma investigação.
3. Os pedidos de assistência inclui todas as informações necessárias, nomeadamente a finalidade e os motivos do pedido. As informações trocadas só são utilizadas para a finalidade para que tenham sido solicitadas.
4. A autoridade de controlo requerida não pode indeferir um pedido, salvo se:
  - a) Não for competente em razão do objeto do pedido ou das medidas cuja execução lhe é solicitada; ou
  - b) O deferimento do pedido viole a presente diretiva ou o direito da União ou do Estado-Membro ao qual a autoridade de controlo que recebe o pedido esteja sujeita.
5. A autoridade de controlo requerida informa a autoridade de controlo requerente dos resultados obtidos ou, consoante o caso, do andamento do pedido ou das medidas tomadas para lhe dar resposta. A autoridade de controlo requerida deve fundamentar a decisão de indeferir o pedido nos termos do n.º 4.
6. As autoridades de controlo requeridas fornecem, em regra, as informações solicitadas por outras autoridades de controlo por meios eletrónicos, utilizando um formato normalizado.
7. As autoridades de controlo requeridas não cobram taxas pelas medidas por elas tomadas por força de pedidos de assistência mútua. As autoridades de controlo podem acordar regras para a indemnização recíproca de despesas específicas decorrentes da prestação de assistência mútua em circunstâncias excecionais.
8. A Comissão pode especificar, por atos de execução, o formato e os procedimentos de assistência mútua referidos no presente artigo, bem como as regras de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 58.º, n.º 2.

## Artigo 51.º

**Atribuições do Comité**

1. O Comité criado pelo Regulamento (UE) 2016/679 exerce as seguintes atribuições no que diz respeito ao tratamento no âmbito de aplicação da presente diretiva:
  - a) Aconselhar a Comissão em todas as questões relacionadas com a proteção de dados pessoais na União, nomeadamente em qualquer projeto de alteração da presente diretiva;
  - b) Analisar, por iniciativa própria ou a pedido de um dos seus membros ou da Comissão, qualquer questão relativa à aplicação da presente diretiva e emitir diretrizes, recomendações e boas práticas a fim de incentivar a aplicação coerente da presente diretiva;
  - c) Elaborar diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas referidas no artigo 47.º, n.ºs 1 e 3;
  - d) Emitir diretrizes, recomendações e boas práticas em conformidade com a alínea b) do presente parágrafo, aplicáveis à determinação das violações de dados pessoais e da demora injustificada referidas no artigo 30.º, n.ºs 1 e 2, e às circunstâncias particulares em que um responsável pelo tratamento ou um subcontratante é obrigado a notificar a violação de dados pessoais;

- e) Emitir diretrizes, recomendações e boas práticas em conformidade com a alínea b) do presente parágrafo em relação às circunstâncias em que uma violação de dados pessoais é suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares a que se refere o artigo 31.º, n.º 1;
- f) Examinar a aplicação prática das diretrizes, recomendações e boas práticas referidas nas alíneas b) e c);
- g) Dar parecer à Comissão tendo em vista avaliar a adequação do nível de proteção num país terceiro ou organização internacional e também avaliar se um país terceiro, o território ou a organização internacional ou o setor específico deixou de garantir um nível de proteção adequado;
- h) Promover a cooperação e o intercâmbio bilateral e multilateral efetivo de informações e melhores práticas entre as autoridades de controlo;
- i) Promover programas de formação comuns e facilitar o intercâmbio de pessoal entre autoridades de controlo, bem como, se necessário, com as autoridades de controlo de países terceiros ou organizações internacionais;
- j) Promover o intercâmbio de conhecimentos e documentação sobre direito e práticas de proteção de dados com autoridades de controlo de todo o mundo.

Para efeitos do primeiro parágrafo, da alínea g), a Comissão fornece ao Comité toda a documentação necessária, incluindo a correspondência com o governo do país terceiro, o território ou o setor específico nesse país terceiro, ou com a organização internacional.

2. Se consultar o Comité, a Comissão pode fixar um prazo para tal, tendo em conta a urgência do assunto.

3. O Comité transmite os seus pareceres, diretrizes, recomendações e melhores práticas à Comissão e ao comité referido no artigo 58.º, n.º 1, e procede à sua publicação.

4. A Comissão informa o Comité das medidas tomadas na sequência dos pareceres, diretrizes, recomendações e melhores práticas por ele emitidos.

## CAPÍTULO VIII

### ***Vias de recurso, responsabilidade e sanções***

#### *Artigo 52.º*

#### **Direito de apresentar reclamação a uma autoridade de controlo**

- 1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, os Estados-Membros preveem que todos os titulares de dados têm o direito de apresentar reclamação a uma autoridade de controlo única, se o titular dos dados considerar que o tratamento dos dados pessoais que lhe diz respeito viola as disposições adotadas por força da presente diretiva.
- 2. Os Estados-Membros preveem que, se a reclamação não for apresentada à autoridade de controlo competente nos termos do artigo 45.º, n.º 1, a autoridade de controlo a que é apresentada a transmita, sem demora injustificada, à autoridade de controlo competente. O titular dos dados é informado dessa transmissão.
- 3. Os Estados-Membros preveem que a autoridade de controlo à qual a reclamação é apresentada preste assistência complementar a pedido do titular dos dados.
- 4. O titular dos dados é informado pela autoridade de controlo competente do andamento e do resultado da reclamação apresentada, nomeadamente da possibilidade de intentar ação judicial nos termos do artigo 53.º.

#### *Artigo 53.º*

#### **Direito de intentar ação judicial contra uma autoridade de controlo**

- 1. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, os Estados-Membros preveem que as pessoas singulares ou coletivas tenham o direito de intentar ação judicial contra qualquer decisão juridicamente vinculativa tomada por uma autoridade de controlo que lhes diga respeito.

2. Sem prejuízo de qualquer outra via de recurso administrativo ou extrajudicial, todos os titulares de dados têm o direito de intentar ação judicial se a autoridade de controlo competente nos termos do artigo 45.º, n.º 1, não atender à reclamação ou não informar o titular dos dados, no prazo de três meses, do andamento ou do resultado da reclamação apresentada nos termos do artigo 52.º.
3. Os Estados-Membros preveem que os recursos contra uma autoridade de controlo sejam interpostos nos tribunais do Estado-Membro em cujo território essa autoridade se encontre estabelecida.

#### *Artigo 54.º*

### **Direito de intentar uma ação judicial contra um responsável pelo tratamento de dados ou um subcontratante**

Sem prejuízo de qualquer via de recurso administrativo ou extrajudicial disponível, nomeadamente o direito de apresentar reclamação junto de uma autoridade de controlo nos termos do artigo 52.º, os Estados-Membros preveem que os titulares dos dados têm o direito de intentar ação judicial se considerarem ter havido violação dos direitos que lhes assistem nos termos das disposições adotadas por força da presente diretiva na sequência de um tratamento dos seus dados pessoais que não cumpra tais disposições.

#### *Artigo 55.º*

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

Os Estados-Membros preveem, nos termos do direito processual dos Estados-Membros, que o titular dos dados tem o direito de mandar um organismo, organização ou associação, sem fins lucrativos, devidamente constituído nos termos do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a proteção dos direitos e liberdades dos titulares de dados no que respeita à proteção dos seus dados pessoais, para apresentar reclamação em seu nome e exercer também em seu nome os direitos previstos nos artigos 52.º, 53.º e 54.º.

#### *Artigo 56.º*

### **Direito de indemnização**

Os Estados-Membros preveem que qualquer pessoa que tenha sofrido danos materiais ou morais causados por uma operação de tratamento ilícito de dados ou por qualquer outro ato que viole as disposições nacionais adotadas por força da presente diretiva tem direito a receber do responsável pelo tratamento de dados ou de qualquer outra autoridade competente nos termos do direito dos Estados-Membros uma indemnização pelos danos sofridos.

#### *Artigo 57.º*

### **Sanções**

Os Estados-Membros estabelecem regras respeitantes às sanções aplicáveis às violações das disposições adotadas por força da presente diretiva e tomam todas as medidas necessárias para assegurar a sua aplicação. As sanções previstas devem ser eficazes, proporcionadas e dissuasivas.

## **CAPÍTULO IX**

### **Atos de execução**

#### *Artigo 58.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.
3. Caso se remeta para o presente número, aplica-se o artigo 8.º do Regulamento (UE) n.º 182/2011, em conjugação com o seu artigo 5.º.

## CAPÍTULO X

**Disposições finais**

## Artigo 59.º

**Revogação da Decisão-Quadro 2008/977/JAI**

1. A Decisão-Quadro 2008/977/JAI é revogada com efeitos a partir de 6 de maio de 2018.
2. As remissões para a decisão revogada a que se refere o n.º 1 entendem-se como sendo feitas para a presente diretiva.

## Artigo 60.º

**Atos jurídicos da União em vigor**

As disposições específicas de proteção de dados pessoais, previstas em atos jurídicos da União adotados antes de 6 de maio de 2016 no domínio da cooperação judiciária em matéria penal e da cooperação policial, que regulam o tratamento entre os Estados-Membros e o acesso das autoridades designadas dos Estados-Membros aos sistemas de informação criados, por força dos Tratados, no âmbito da presente diretiva mantêm-se inalteradas.

## Artigo 61.º

**Relação com acordos internacionais celebrados anteriormente no domínio da cooperação judiciária em matéria penal e da cooperação policial**

Os acordos internacionais que impliquem a transferência de dados pessoais para países terceiros ou para organizações internacionais, celebrados pelos Estados-Membros antes de 6 de maio de 2016, e que sejam conformes com o direito da União tal como aplicável antes dessa data, continuam a vigorar até serem alterados, substituídos ou revogados.

## Artigo 62.º

**Relatórios da Comissão**

1. Até 6 de maio de 2022 e, posteriormente, de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão da presente diretiva. Os relatórios devem ser tornados públicos.
2. No âmbito das avaliações e revisões a que se refere o n.º 1, a Comissão examina, em particular, a aplicação e o funcionamento do Capítulo V sobre a transferência de dados pessoais para países terceiros ou organizações internacionais, em especial no que diz respeito às decisões adotadas nos termos do artigo 36.º, n.º 3, e do artigo 39.º.
3. Para os efeitos dos n.ºs 1 e 2, a Comissão pode solicitar informações aos Estados-Membros e às autoridades de controlo.
4. Ao proceder às avaliações e revisões a que se referem os n.ºs 1 e 2, a Comissão tem em consideração as posições e conclusões a que tenham chegado o Parlamento Europeu, o Conselho e outros organismos e fontes pertinentes.
5. Se necessário, a Comissão apresenta propostas adequadas com vista à alteração da presente diretiva atendendo, em especial, à evolução das tecnologias da informação e aos progressos da sociedade da informação e à harmonização de outros instrumentos jurídicos.
6. Até 6 de maio de 2019, a Comissão reexamina outros atos jurídicos adotados pela União que regulam o tratamento pelas autoridades competentes para efeitos do artigo 1.º, n.º 1, designadamente os referidos no artigo 60.º, a fim de avaliar a necessidade de os harmonizar com a presente diretiva e apresenta, se for caso disso, as propostas necessárias à alteração desses atos de forma a assegurar uma abordagem coerente da proteção de dados pessoais no âmbito da presente diretiva.

*Artigo 63.º***Transposição**

1. Os Estados-Membros adotam e publicam, até 6 de maio de 2018, as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva. Os Estados-Membros comunicam imediatamente à Comissão o texto dessas disposições. Os Estados-Membros aplicam as referidas disposições a partir de 6 de maio de 2018.

Quando os Estados-Membros adotarem essas disposições, estas incluem uma referência à presente diretiva ou são acompanhadas dessa referência aquando da sua publicação oficial. As modalidades dessa referência são estabelecidas pelos Estados-Membros.

2. Em derrogação do n.º 1, um Estado-Membro pode estabelecer que, excecionalmente, quando o esforço envolvido for desproporcionado, os sistemas de tratamento automatizado estabelecidos antes de 6 de maio de 2016 seja tornado conforme com o artigo 25.º, n.º 1, até 6 de maio de 2023.

3. Em derrogação dos n.ºs 1 e 2 do presente artigo, um Estado-Membro pode, em circunstâncias excecionais, tornar um sistema de tratamento automatizado, referido no n.º 2 do presente artigo, conforme com o artigo 25.º, n.º 1, num prazo fixado após o período a que se refere o n.º 2 do presente artigo, caso, de outra forma, sejam causadas graves dificuldades ao funcionamento desse sistema de tratamento automatizado. O Estado-Membro em causa notifica a Comissão dos motivos para essas graves dificuldades e dos motivos para o prazo especificado em que tornará esse particular sistema de tratamento automatizado conforme com o artigo 25.º, n.º 1. O prazo fixado não pode, em caso algum, ir além de 6 de maio de 2026.

4. Os Estados-Membros comunicam à Comissão o texto das principais disposições de direito interno que adotarem no domínio abrangido pela presente diretiva.

*Artigo 64.º***Entrada em vigor**

A presente diretiva entra em vigor no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

*Artigo 65.º***Destinatários**

Os destinatários da presente diretiva são os Estados-Membros.

Feito em Bruxelas, em 27 de abril de 2016.

*Pelo Parlamento Europeu*  
O Presidente  
M. SCHULZ

*Pelo Conselho*  
A Presidente  
J.A. HENNIS-PLASSCHAERT

**DIRETIVA (UE) 2016/681 DO PARLAMENTO EUROPEU E DO CONSELHO****de 27 de abril de 2016****relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave**

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 82.º, n.º 1, alínea d), e o artigo 87.º, n.º 2, alínea a),

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu <sup>(1)</sup>,

Após consulta ao Comité das Regiões,

Deliberando de acordo com o processo legislativo ordinário <sup>(2)</sup>,

Considerando o seguinte:

- (1) Em 6 de novembro de 2007, a Comissão adotou uma proposta de decisão-quadro do Conselho relativa à utilização dos dados dos registos de identificação dos passageiros (*passenger name record* — PNR) para fins policiais. No entanto, com a entrada em vigor do Tratado de Lisboa em 1 de dezembro de 2009, a proposta, que não fora adotada pelo Conselho até essa data, tornou-se obsoleta.
- (2) O «Programa de Estocolmo — Uma Europa aberta e segura que sirva e proteja os cidadãos» <sup>(3)</sup> convidou a Comissão a apresentar uma proposta relativa à utilização de dados PNR para fins de prevenção, deteção, investigação e repressão do terrorismo e da criminalidade grave.
- (3) Na sua comunicação intitulada «Abordagem global relativa à transferência dos dados do registo de identificação dos passageiros (PNR) para países terceiros», de 21 de setembro de 2010, a Comissão expôs vários elementos centrais de uma política da União neste domínio.
- (4) A Diretiva 2004/82/CE do Conselho <sup>(4)</sup> regula a transmissão antecipada de dados referentes a informações prévias sobre passageiros (API — *advance passenger information*) pelas transportadoras aéreas às autoridades nacionais competentes, a fim de melhorar os controlos nas fronteiras e combater a imigração ilegal.
- (5) A presente diretiva tem nomeadamente por objetivos garantir a segurança e proteger a vida e a segurança das pessoas e criar um regime jurídico aplicável à proteção dos dados PNR no que respeita ao seu tratamento pelas autoridades competentes.
- (6) A utilização eficaz de dados PNR, nomeadamente mediante a sua comparação com várias bases de dados sobre as pessoas e os objetos procurados a fim de obter provas e, se for caso disso, detetar cúmplices de criminosos e dismantelar redes criminosas, é necessária para prevenir, detetar, investigar e reprimir infrações terroristas e a criminalidade grave e, assim, reforçar a segurança interna.
- (7) A avaliação dos dados PNR permite identificar pessoas insuspeitas de envolvimento em infrações terroristas ou criminalidade grave antes de tal avaliação e que deverão ser sujeitas a um controlo mais minucioso pelas

<sup>(1)</sup> JO C 218 de 23.7.2011, p. 107.

<sup>(2)</sup> Posição do Parlamento Europeu de 14 de abril de 2016 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 21 de abril de 2016.

<sup>(3)</sup> JO C 115 de 4.5.2010, p. 1.

<sup>(4)</sup> Diretiva 2004/82/CE do Conselho, de 29 de abril de 2004, relativa à obrigação de comunicação de dados dos passageiros pelas transportadoras (JO L 261 de 6.8.2004, p. 24).

autoridades competentes. Através da utilização dos dados PNR é possível fazer face à ameaça que representam as infrações terroristas e a criminalidade grave numa perspetiva diferente da do tratamento de outras categorias de dados pessoais. Contudo, a fim de assegurar que o tratamento de dados PNR se continua a restringir ao necessário, a fixação e a aplicação de critérios de avaliação deverão limitar-se a infrações terroristas e à criminalidade grave para as quais a utilização de tais critérios seja relevante. Além disso, os critérios de avaliação deverão ser definidos de modo a reduzir ao mínimo o número de pessoas inocentes incorretamente identificadas pelo sistema.

- (8) As transportadoras aéreas já fazem a recolha e o tratamento dos dados PNR dos seus passageiros para fins comerciais. A presente diretiva não deverá impor às transportadoras aéreas a obrigação de recolherem ou conservarem dados adicionais dos passageiros, nem a estes últimos a obrigação de fornecerem outros dados para além dos que já são fornecidos às transportadoras aéreas.
- (9) Algumas transportadoras aéreas conservam os dados API que recolhem como parte dos dados PNR, enquanto outras não o fazem. A utilização dos dados PNR em conjunto com os dados API contribui para ajudar os Estados-Membros a verificar a identidade dos indivíduos, reforçando, assim, a utilidade desse resultado para fins policiais e minimizando o risco de controlar e investigar pessoas inocentes. Importa, pois, garantir que, caso recolham dados API, as transportadoras aéreas procedam à sua transferência, independentemente de os conservarem por meios técnicos distintos dos utilizados para outros dados PNR.
- (10) A fim de prevenir, detetar, investigar e reprimir as infrações terroristas e a criminalidade grave, é essencial que todos os Estados-Membros adotem disposições que prevejam a obrigação de as transportadoras aéreas que operam voos extra-UE transferirem os dados PNR que recolham, incluindo os dados API. Os Estados-Membros deverão ter igualmente a possibilidade de alargar esta obrigação às transportadoras aéreas que operam voos intra-UE. Essas disposições deverão aplicar-se sem prejuízo do disposto na Diretiva 2004/82/CE.
- (11) O tratamento de dados pessoais deverá ser proporcionado em relação aos objetivos específicos de segurança visados pela presente diretiva.
- (12) A definição de «infrações terroristas» utilizada na presente diretiva deverá ser idêntica à que consta da Decisão-Quadro 2002/475/JAI do Conselho <sup>(1)</sup>. A definição de «criminalidade grave» deverá abranger as categorias de infrações enumeradas no anexo II da presente diretiva.
- (13) Os dados PNR deverão ser transferidos para uma única unidade de informações de passageiros (UIP) designada no Estado-Membro em causa, de modo a assegurar a clareza e a reduzir os custos para as transportadoras aéreas. A UIP pode ter diversas secções num Estado-Membro, podendo também os Estados-Membros criar conjuntamente uma UIP. Os Estados-Membros deverão trocar informações entre si através de redes apropriadas de intercâmbio de informações, de modo a facilitar a partilha de informações e a garantir a interoperabilidade.
- (14) Caberá aos Estados-Membros suportar os custos da utilização, da conservação e do intercâmbio de dados PNR.
- (15) Uma lista de dados PNR, a obter por uma UIP, deverá ser elaborada com o objetivo de refletir as exigências legítimas das autoridades públicas a fim de prevenir, detetarem, investigarem e reprimirem as infrações terroristas ou a criminalidade grave, aumentando assim a segurança interna na União e salvaguardando os direitos fundamentais, nomeadamente o direito à privacidade e à proteção dos dados pessoais. Para o efeito, deverão ser aplicadas normas exigentes, de acordo com a Carta dos Direitos Fundamentais da União Europeia (a «Carta»), a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (a «Convenção n.º 108») e a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais (a «CEDH»). Essa lista não deverá basear-se na raça ou origem étnica, na religião ou nas convicções da pessoa, nem nas suas opiniões, políticas ou outras, na sua filiação sindical nem na sua saúde, vida ou orientação sexual. Os dados PNR deverão incluir unicamente informações pormenorizadas sobre as reservas e os itinerários do passageiro que permitam às autoridades competentes identificar os passageiros aéreos que representem uma ameaça para a segurança interna.
- (16) Existem atualmente dois métodos possíveis para a transferência de dados: o método de transferência por extração (*pull*), pelo qual as autoridades competentes do Estado-Membro que solicita os dados PNR podem aceder ao sistema de reservas da transportadora aérea e extrair uma cópia dos dados PNR requeridos, e o método de transferência por exportação (*push*), pelo qual as transportadoras aéreas transmitem (exportam) os dados PNR requeridos para a autoridade que os solicita, o que permite às transportadoras aéreas manter o controlo sobre os dados transmitidos. Considera-se que o método de transferência por exportação (*push*) proporciona um nível mais elevado de proteção dos dados e que deverá ser obrigatório para todas as transportadoras aéreas.

<sup>(1)</sup> Decisão-Quadro 2002/475/JAI do Conselho, de 13 de junho de 2002, relativa à luta contra o terrorismo (JO L 164 de 22.6.2002, p. 3).

- (17) A Comissão apoia as orientações da Organização da Aviação Civil Internacional (OACI) em matéria de dados PNR. Essas orientações deverão, portanto, servir de base para a adoção de formatos de dados reconhecidos para as transferências de dados PNR pelas transportadoras aéreas para os Estados-Membros. A fim de assegurar condições uniformes de execução de tais formatos de dados reconhecidos e dos protocolos relevantes aplicáveis à transferência de dados das transportadoras aéreas, 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 <sup>(1)</sup>.
- (18) Os Estados-Membros deverão adotar todas as medidas necessárias para permitir que as transportadoras aéreas cumpram as obrigações que lhes incumbem por força da presente diretiva. Os Estados-Membros deverão estabelecer sanções efetivas, proporcionadas e dissuasivas, incluindo sanções financeiras, contra as transportadoras aéreas que não cumpram as suas obrigações no que respeita à transferência de dados PNR.
- (19) Cada Estado-Membro deverá ser responsável pela avaliação das ameaças potenciais relacionadas com infrações terroristas e criminalidade grave.
- (20) Tendo plenamente em conta o direito à proteção dos dados pessoais e à não discriminação, não deverá ser tomada qualquer decisão que produza efeitos jurídicos que prejudiquem uma pessoa ou que a afete significativamente apenas com base no tratamento automatizado dos dados PNR. Além disso, nos termos dos artigos 8.º e 21.º da Carta, nenhuma decisão dessa natureza deverá introduzir uma discriminação em razão do sexo, da raça, da cor ou origem étnica ou social, das características genéticas, da língua, da religião ou das convicções, das opiniões políticas ou outras, da pertença a uma minoria nacional, da riqueza, do nascimento, da deficiência, da idade ou da orientação sexual. A Comissão deverá igualmente ter em conta estes princípios quando proceder ao reexame da aplicação da presente diretiva.
- (21) O resultado do tratamento dos dados PNR não deverá, em circunstância alguma, ser utilizado pelos Estados-Membros como motivo para contornar as obrigações internacionais que lhes incumbem por força da Convenção de 28 de julho de 1951 relativa ao Estatuto dos Refugiados conforme alterada pelo Protocolo de 31 de janeiro de 1967, nem para negar aos requerentes de asilo vias legais seguras e eficazes para aceder ao território da União a fim de exercerem o seu direito à proteção internacional.
- (22) Tendo plenamente em conta os princípios enunciados na recente jurisprudência do Tribunal de Justiça da União Europeia na matéria, a aplicação da presente diretiva deverá garantir o pleno respeito dos direitos fundamentais, do direito à privacidade e do princípio da proporcionalidade. Deverá também cumprir efetivamente os objetivos da necessidade e proporcionalidade a fim de respeitar os interesses gerais reconhecidos pela União e atender à necessidade de proteger os direitos e as liberdades de terceiros na luta contra as infrações terroristas e a criminalidade grave. A aplicação da presente diretiva deverá ser devidamente justificada e deverão ser criadas as garantias necessárias para assegurar a legalidade da conservação, análise, transferência ou utilização de dados PNR.
- (23) Os Estados-Membros deverão partilhar entre si, e com a Europol, os dados PNR que recebem caso tal seja considerado necessário para efeitos de prevenção, deteção, investigação ou repressão de infrações terroristas ou da criminalidade grave. Se necessário, as UIP deverão transmitir sem demora o resultado do tratamento dos dados PNR às UIP de outros Estados-Membros, para efeitos de investigação complementar. As disposições da presente diretiva deverão aplicar-se sem prejuízo da aplicação de outros instrumentos da União em matéria de intercâmbio de informações entre as autoridades policiais, outras autoridades responsáveis pela aplicação da lei e autoridades judiciais, incluindo a Decisão 2009/371/JAI do Conselho <sup>(2)</sup> e a Decisão-Quadro 2006/960/JAI do Conselho <sup>(3)</sup>. Tal intercâmbio de dados PNR deverá reger-se pelas disposições em matéria de cooperação policial e judiciária e não atentar contra o elevado nível de proteção da privacidade e dos dados pessoais exigido pela Carta, pela Convenção n.º 108 e pela CEDH.
- (24) Deverá ser garantida a segurança do intercâmbio de informações sobre dados PNR entre os Estados-Membros, através de qualquer dos canais de cooperação existentes entre as respetivas autoridades competentes, e, em especial, com a Europol, através da rede de intercâmbio seguro de informações (SIENA) da Europol.

<sup>(1)</sup> Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

<sup>(2)</sup> Decisão 2009/371/JAI do Conselho, de 6 de abril de 2009, que cria o Serviço Europeu de Polícia (Europol) (JO L 121 de 15.5.2009, p. 37).

<sup>(3)</sup> Decisão-Quadro 2006/960/JAI do Conselho, de 18 de dezembro de 2006, relativa à simplificação do intercâmbio de dados e informações entre as autoridades de aplicação da lei dos Estados-Membros da União Europeia (JO L 386 de 29.12.2006, p. 89).



- (25) O prazo durante ao qual deverão ser conservados os dados PNR deverá ser tão longo quanto necessário e proporcionado à consecução dos objetivos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Atendendo à natureza dos dados e à sua utilização, é necessário que os dados PNR sejam conservados durante um prazo suficientemente longo para permitir a realização de análises e a sua utilização no âmbito de investigações. A fim de evitar uma utilização desproporcionada, após o prazo inicial de conservação, os dados PNR deverão ser anonimizados mediante o mascaramento de elementos dos dados. A fim de assegurar o nível mais elevado de proteção de dados, o acesso aos dados PNR integrais, que permitem a identificação direta do seu titular, só deverá ser concedido em condições muito estritas e limitadas após aquele prazo inicial.
- (26) Caso tenham sido transferidos dados PNR específicos para uma autoridade competente e estes sejam utilizados no quadro de determinadas investigações ou processos penais, o prazo de conservação dos dados por essa autoridade deverá reger-se pelo direito nacional, independentemente dos prazos de conservação dos dados estabelecidos na presente diretiva.
- (27) Em cada Estado-Membro, o tratamento dos dados PNR pela UIP e pelas autoridades competentes deverá estar sujeito a uma norma de proteção de dados pessoais, prevista pelo direito nacional, que seja conforme com a Decisão-Quadro 2008/977/JAI do Conselho <sup>(1)</sup>, e com os requisitos específicos em matéria de proteção de dados estabelecidos na presente diretiva. As remissões para a Decisão-Quadro 2008/977/JAI deverão ser entendidas como remissões para a legislação atualmente em vigor e para a legislação que a substitua.
- (28) Tendo em conta o direito à proteção dos dados pessoais, os direitos dos titulares dos dados no que se refere ao tratamento dos dados PNR que lhes dizem respeito, nomeadamente os direitos de acesso, retificação, apagamento ou limitação, e os direitos a indemnização e a recurso judicial, deverão ser conformes com a Decisão-Quadro 2008/977/JAI e com o elevado nível de proteção conferido pela Carta e pela CEDH.
- (29) Tendo em conta o direito que assiste aos passageiros de serem informados do tratamento dos seus dados pessoais, os Estados-Membros deverão assegurar que estes recebem informações precisas, de fácil acesso e compreensão, sobre a recolha de dados PNR, a sua transferência para a UIP e os seus direitos enquanto titulares dos dados.
- (30) A presente diretiva é aplicável sem prejuízo do direito da União e nacional sobre o princípio do direito de acesso do público aos documentos oficiais.
- (31) As transferências de dados PNR dos Estados-Membros para países terceiros só deverão ser autorizadas caso a caso e no pleno respeito das disposições adotadas pelos Estados-Membros em aplicação da Decisão-Quadro 2008/977/JAI. Para assegurar a proteção dos dados pessoais, essas transferências deverão ficar sujeitas a requisitos adicionais no que respeita à finalidade destas. Deverão ainda respeitar os princípios da necessidade e da proporcionalidade, e o elevado nível de proteção conferido pela Carta e pela CEDH.
- (32) As autoridades nacionais de controlo criadas em aplicação da Decisão-Quadro 2008/977/JAI deverão ter igualmente a responsabilidade de prestar aconselhamento e monitorizar a aplicação das disposições adotadas pelos Estados-Membros em aplicação da presente diretiva.
- (33) A presente diretiva não obsta a que os Estados-Membros prevejam, no âmbito do respetivo direito nacional, um sistema de recolha e tratamento dos dados PNR provenientes de operadores económicos que não sejam as transportadoras, tais como agências de viagem e operadores turísticos que prestam serviços afins, incluindo a reserva de voos, para os quais procedem à recolha e ao tratamento de dados PNR, ou de fornecedores de serviços de transporte que não sejam os especificados na presente diretiva, desde que esse direito nacional seja conforme com o acervo da União.
- (34) A presente diretiva é aplicável sem prejuízo das atuais regras da União sobre a forma como são efetuados os controlos nas fronteiras, nem das regras da União que regem a entrada e a saída do território da União.
- (35) Dadas as diferenças jurídicas e técnicas entre as disposições nacionais aplicáveis ao tratamento de dados pessoais, incluindo dados PNR, as transportadoras aéreas já são, e continuarão a ser, confrontadas com exigências diferentes relativamente ao tipo de informações a transmitir e às condições em que estas devem ser fornecidas às

<sup>(1)</sup> Decisão-Quadro 2008/977/JAI do Conselho, de 27 de novembro de 2008, relativa à proteção dos dados pessoais tratados no âmbito da cooperação policial e judiciária em matéria penal (JO L 350 de 30.12.2008, p. 60).

autoridades nacionais competentes. Essas diferenças podem ser prejudiciais à cooperação efetiva entre essas autoridades para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave. Por conseguinte, é necessário prever, a nível da União, um regime jurídico comum para a transferência e o tratamento de dados PNR.

- (36) A presente diretiva respeita os direitos fundamentais e os princípios enunciados na Carta, em especial o direito à proteção de dados pessoais, o direito ao respeito pela vida privada e o direito à não discriminação, consagrados nos artigos 8.º, 7.º e 21.º da mesma, e deverá, assim, ser aplicada em conformidade. A presente diretiva é compatível com os princípios da proteção de dados e as suas disposições são conformes com a Decisão-Quadro 2008/977/JAI. Além disso, a fim de respeitar o princípio da proporcionalidade, a presente diretiva prevê, em relação a determinadas matérias, normas de proteção de dados mais estritas do que as estabelecidas na Decisão-Quadro 2008/977/JAI.
- (37) O âmbito de aplicação da presente diretiva é o mais limitado possível, uma vez que: prevê que os dados PNR sejam conservados nas UIP durante um prazo não superior a cinco anos, após o qual tais dados deverão ser apagados; prevê que os dados sejam anonimizados mediante mascaramento de elementos de dados após o decurso de um prazo inicial de seis meses; e proíbe recolher e utilizar dados sensíveis. A fim de assegurar a eficácia do sistema e um elevado nível de proteção dos dados, os Estados-Membros deverão garantir que uma autoridade de controlo independente a nível nacional e, especificamente, um responsável pela proteção de dados, sejam incumbidos de prestar aconselhamento sobre a forma como os dados PNR são tratados e de a monitorizar. Qualquer tratamento de dados PNR deverá ser registado ou documentado para efeitos de verificação da sua legalidade, autocontrolo e garantia da integridade dos dados e da segurança do seu tratamento. Os Estados-Membros deverão também assegurar que os passageiros sejam informados de forma clara e precisa sobre a recolha de dados PNR e sobre os seus direitos.
- (38) Atendendo a que os objetivos da presente diretiva, a saber, a transferência de dados PNR pelas transportadoras aéreas e o tratamento desses dados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, não podem ser suficientemente alcançados pelos Estados-Membros mas podem ser mais bem alcançados ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade, consagrado no mesmo artigo, a presente diretiva não excede o necessário para alcançar esses objetivos.
- (39) Nos termos do artigo 3.º do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, estes Estados-Membros notificaram a sua intenção de participar na adoção e na aplicação da presente diretiva.
- (40) Nos termos dos artigos 1.º e 2.º do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participa na adoção da presente diretiva e não fica a ela vinculada nem sujeita à sua aplicação.
- (41) 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 do Parlamento Europeu e do Conselho <sup>(1)</sup> e emitiu um parecer em 25 de março de 2011,

ADOTARAM A PRESENTE DIRETIVA:

## CAPÍTULO I

### *Disposições gerais*

#### *Artigo 1.º*

### **Objeto e âmbito de aplicação**

1. A presente diretiva prevê:
  - a) A transferência, pelas transportadoras aéreas, dos dados dos registos de identificação dos passageiros (PNR) de voos extra-UE;
  - b) O tratamento dos dados referidos na alínea a), inclusive a sua recolha, utilização e conservação pelos Estados-Membros, e o respetivo intercâmbio entre Estados-Membros.

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

2. Os dados PNR recolhidos nos termos da presente diretiva só podem ser tratados para fins de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave, conforme previsto no artigo 6.º, n.º 2, alíneas a), b) e c).

#### Artigo 2.º

##### **Aplicação da presente diretiva aos voos intra-UE**

1. Se decidirem aplicar a presente diretiva aos voos intra-UE, os Estados-Membros notificam a Comissão por escrito. Os Estados-Membros podem efetuar ou revogar essa notificação a todo o tempo. A Comissão publica essa notificação ou uma eventual revogação da mesma no *Jornal Oficial da União Europeia*.

2. Caso seja efetuada a notificação a que se refere o n.º 1, todas as disposições da presente diretiva são aplicáveis aos voos intra-UE como se se tratassem de voos extra-UE e aos dados PNR respeitantes aos voos intra-UE como se se tratassem de dados referentes a voos extra-UE.

3. Os Estados-Membros podem decidir aplicar a presente diretiva apenas a voos intra-UE selecionados. Ao tomarem essa decisão, selecionam os voos que considerem necessário a fim de prosseguir os objetivos da presente diretiva. Os Estados-Membros podem decidir alterar a seleção de voos intra-UE, a todo o tempo.

#### Artigo 3.º

##### **Definições**

Para efeitos da presente diretiva, entende-se por:

- 1) «Transportadora aérea», uma empresa de transporte aéreo titular de uma licença de exploração válida ou equivalente que lhe permite transportar passageiros por via aérea;
- 2) «Voo extra-UE», um voo regular ou não regular efetuado por uma transportadora aérea a partir de um país terceiro e programado para aterrar no território de um Estado-Membro, ou a partir do território de um Estado-Membro e programado para aterrar num país terceiro, incluindo, em ambos os casos, os voos com escala no território de Estados-Membros ou de países terceiros;
- 3) «Voo intra-UE», um voo regular ou não regular efetuado por uma transportadora aérea a partir do território de um Estado-Membro, programado para aterrar no território de um ou mais Estados-Membros, sem escala no território de um país terceiro;
- 4) «Passageiro», uma pessoa, incluindo pessoas em trânsito ou em correspondência e excluindo membros da tripulação, transportada ou a transportar numa aeronave com o consentimento da transportadora aérea, decorrendo esse consentimento do registo dessa pessoa na lista de passageiros;
- 5) «Registo de identificação dos passageiros» ou «PNR» (*Passenger Name Record*), um registo das formalidades de viagem impostas a cada passageiro que contém as informações necessárias para permitir o tratamento e o controlo das reservas feitas pelas transportadoras aéreas participantes relativamente a cada viagem reservada por uma pessoa ou em seu nome, quer o registo conste dos sistemas de reserva, dos sistemas de controlo das partidas utilizado para efetuar o controlo dos passageiros embarcados nos voos, ou de sistemas equivalentes que ofereçam as mesmas funcionalidades;
- 6) «Sistema de reservas», o sistema interno da transportadora aérea, no qual são recolhidos dados PNR para o tratamento das reservas;
- 7) «Método de transferência por exportação», o método através do qual as transportadoras aéreas transferem os dados PNR enumerados no anexo I para a base de dados da autoridade requerente;

- 8) «Infrações terroristas», as infrações definidas no direito nacional a que se referem os artigos 1.º a 4.º da Decisão-Quadro 2002/475/JAI;
- 9) «Criminalidade grave», as infrações enumeradas no anexo II puníveis com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos nos termos do direito nacional de um Estado-Membro;
- 10) «Anonimizar mediante mascaramento de elementos de dados», tornar invisíveis para os utilizadores os elementos dos dados suscetíveis de identificar diretamente o seu titular.

## CAPÍTULO II

### **Responsabilidades dos estados-membros**

#### *Artigo 4.º*

#### **Unidade de informações de passageiros**

1. Cada Estado-Membro cria ou designa uma autoridade competente para efeitos de prevenção, deteção, investigação ou repressão das infrações terroristas e da criminalidade grave, ou cria ou designa uma secção de tal autoridade, para agir na qualidade da sua «unidade de informações de passageiros» (UIP).
2. A UIP é responsável:
  - a) Pela recolha dos dados PNR junto das transportadoras aéreas, pela conservação e pelo tratamento desses dados e pela transferência desses dados ou dos resultados do seu tratamento às autoridades competentes referidas no artigo 7.º;
  - b) Pelo intercâmbio de dados PNR e dos resultados do seu tratamento com as UIP de outros Estados-Membros e com a Europol, nos termos dos artigos 9.º e 10.º.
3. Os membros do pessoal das UIP podem ser agentes destacados pelas autoridades competentes. Os Estados-Membros dotam as UIP dos recursos adequados para o exercício das suas funções.
4. Dois ou mais Estados-Membros («Estados-Membros participantes») podem criar ou designar uma única autoridade como a sua UIP. Essa UIP fica estabelecida num dos Estados-Membros participantes, e é considerada a UIP nacional de todos os Estados-Membros participantes. Estes determinam de comum acordo as regras pormenorizadas de funcionamento da UIP, respeitando os requisitos previstos na presente diretiva.
5. Cada Estado-Membro notifica a constituição da sua UIP à Comissão no prazo de um mês a contar da mesma e pode alterar a sua notificação a todo o tempo. A Comissão publica a notificação, bem como as respetivas alterações, no *Jornal Oficial da União Europeia*.

#### *Artigo 5.º*

#### **Responsável pela proteção de dados na UIP**

1. A UIP nomeia um responsável pela proteção de dados incumbido de controlar o tratamento dos dados PNR e de aplicar as salvaguardas relevantes.
2. Os Estados-Membros dotam os responsáveis pela proteção de dados dos meios necessários ao desempenho dos deveres e das funções que lhes incumbem nos termos do presente artigo, de forma eficaz e independente.
3. Os Estados-Membros asseguram que o titular dos dados tenha o direito de contactar o responsável pela proteção de dados, enquanto ponto de contacto único, para todos os assuntos respeitantes ao tratamento dos dados PNR de que é titular.

## Artigo 6.º

**Tratamento dos dados PNR**

1. Os dados PNR transferidos pelas transportadoras aéreas são recolhidos pela UIP do Estado-Membro em causa, conforme previsto no artigo 8.º. Caso os dados PNR transferidos pelas transportadoras aéreas incluam dados distintos dos enumerados no anexo I, a UIP apaga imediata e definitivamente esses dados assim que os receber.
2. A UIP procede ao tratamento dos dados PNR exclusivamente para os seguintes fins:
  - a) Proceder a uma avaliação dos passageiros antes da sua chegada prevista ao Estado-Membro ou da sua partida prevista desse Estado-Membro, a fim de identificar as pessoas que, pelo facto de poderem estar implicadas numa infração terrorista ou numa forma de criminalidade grave, devem ser sujeitas a um controlo mais minucioso pelas autoridades competentes a que se refere o artigo 7.º e, se for caso disso, pela Europol, nos termos do artigo 10.º;
  - b) Responder, caso a caso, aos pedidos devidamente fundamentados, baseados em motivos suficientes, apresentados pelas autoridades competentes, para fornecer e tratar dados PNR, em casos específicos, para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas ou da criminalidade grave, e para disponibilizar às autoridades competentes ou, se for caso disso, à Europol os resultados desse tratamento; e
  - c) Analisar os dados PNR com o objetivo de atualizar ou criar novos critérios a utilizar nas avaliações realizadas nos termos do n.º 3, alínea b), a fim de identificar pessoas que possam estar implicadas em infrações terroristas ou em formas de criminalidade grave.
3. Ao realizar a avaliação a que se refere o n.º 2, alínea a), a UIP pode:
  - a) Comparar os dados PNR com os que constam das bases de dados relevantes para efeitos de prevenção, deteção, investigação e repressão de infrações terroristas e da criminalidade grave, incluindo bases de dados sobre pessoas ou objetos procurados ou alvo de um alerta, de acordo com as regras da União, internacionais e nacionais, aplicáveis a essas bases de dados; ou
  - b) Proceder ao tratamento dos dados PNR de acordo com critérios pré-estabelecidos.
4. Qualquer avaliação dos passageiros antes da sua chegada prevista ao Estado-Membro ou da sua partida prevista do Estado-Membro, feita nos termos do n.º 3, alínea b), de acordo com os critérios pré-estabelecidos, é realizada de forma não discriminatória. Os referidos critérios pré-estabelecidos devem ser orientados em função dos objetivos, proporcionados e específicos. Os Estados-Membros asseguram que esses critérios sejam fixados e revistos regularmente pelas UIP, em cooperação com as autoridades competentes a que se refere o artigo 7.º. Esses critérios não podem, em caso algum, basear-se na raça ou na origem étnica de uma pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, na sua filiação sindical, na sua saúde, vida ou orientação sexual.
5. Os Estados-Membros asseguram que qualquer resultado positivo obtido através do tratamento automatizado dos dados PNR efetuado ao abrigo n.º 2, alínea a), seja verificado individualmente por meios não automatizados, para aferir se é ou não necessário que a autoridade competente referida no artigo 7.º intervenha, de acordo com o direito nacional.
6. A UIP de um Estado-Membro transmite os dados PNR das pessoas identificadas nos termos do n.º 2, alínea a), ou os resultados do tratamento desses dados, às autoridades competentes referidas no artigo 7.º desse mesmo Estado-Membro, para efeitos de um controlo mais minucioso. Essas transferências de dados só podem ser feitas caso a caso e, se houver tratamento automatizado dos dados PNR, após verificação individual por meios não automatizados.
7. Os Estados-Membros asseguram que o responsável pela proteção de dados tenha acesso a todos os dados tratados pela UIP. Se o responsável pela proteção de dados considerar que o tratamento dos dados não foi efetuado em conformidade com a lei, pode remeter a questão para a autoridade nacional de controlo.
8. Os dados PNR só podem ser conservados, tratados e analisados pela UIP em local ou locais seguros no território dos Estados-Membros.

9. As consequências das avaliações dos passageiros, referidas no n.º 2, alínea a), do presente artigo, não põem em causa o direito das pessoas que gozam do direito de livre circulação da União de entrarem no território do Estado-Membro em causa, tal como estabelecido na Diretiva 2004/38/CE do Parlamento Europeu e do Conselho <sup>(1)</sup>. Além disso, quando as avaliações sejam efetuadas em relação a voos intra-UE operados entre Estados-Membros aos quais seja aplicável o Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho <sup>(2)</sup>, as consequências de tais avaliações devem observar o referido regulamento.

#### Artigo 7.º

##### **Autoridades competentes**

1. Cada Estado-Membro adota uma lista das autoridades competentes habilitadas a solicitar às UIP ou a delas receber dados PNR ou o resultado do tratamento de tais dados, a fim de analisar mais minuciosamente essas informações ou de tomar medidas apropriadas para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave.
2. As autoridades referidas no n.º 1 são as autoridades competentes para fins de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave.
3. Para efeitos do artigo 9.º, n.º 3, cada Estado-Membro notifica a Comissão da lista das respetivas autoridades competentes até 25 de maio de 2017, podendo alterar a sua notificação a todo o tempo. A Comissão publica a notificação, bem como as suas eventuais alterações, no *Jornal Oficial da União Europeia*.
4. Os dados PNR e o resultado do tratamento de tais dados recebidos pela UIP podem ser objeto de tratamento ulterior pelas autoridades competentes dos Estados-Membros exclusivamente para efeitos específicos de prevenção, deteção, investigação ou repressão das infrações terroristas ou da criminalidade grave.
5. O disposto no n.º 4 é aplicável sem prejuízo das competências das autoridades policiais ou judiciárias nacionais quando forem detetadas outras infrações ou indícios de outras infrações no decurso de ações repressivas desencadeadas na sequência do referido tratamento.
6. As autoridades competentes abstêm-se de tomar qualquer decisão que produza efeitos jurídicos adversos para uma pessoa ou que a afete de forma grave apenas com base no tratamento automatizado dos dados PNR. Tais decisões não podem basear-se na raça ou origem étnica da pessoa, nas suas opiniões políticas, religião ou convicções filosóficas, filiação sindical nem na sua saúde, vida ou orientação sexual.

#### Artigo 8.º

##### **Obrigações impostas às transportadoras aéreas em matéria de transferência de dados**

1. Os Estados-Membros adotam as medidas necessárias para assegurar que as transportadoras aéreas transfiram, pelo método de exportação, os dados PNR enumerados no anexo I, na medida em que já tenham recolhido esses dados no exercício normal das suas atividades, para a base de dados da UIP do Estado-Membro em cujo território o voo aterrará ou do qual descolará. Caso um voo seja explorado por uma ou mais transportadoras aéreas em regime de partilha de código, a obrigação de transferir os dados PNR de todos os passageiros do voo cabe à transportadora aérea que o opera. Caso os voos extra-UE incluam uma ou mais escalas em aeroportos de diferentes Estados-Membros, as transportadoras aéreas transferem os dados PNR da totalidade dos passageiros para as UIP de todos os Estados-Membros em causa. O mesmo se aplica aos voos intra-UE com uma ou mais escalas nos aeroportos de diferentes Estados-Membros, mas só em relação aos Estados-Membros que recolhem dados PNR de voos intra-UE.

<sup>(1)</sup> Diretiva 2004/38/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao direito de livre circulação e residência dos cidadãos da União e dos membros das suas famílias no território dos Estados-Membros, que altera o Regulamento (CEE) n.º 1612/68 e que revoga as Diretivas 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE e 93/96/CEE (JO L 158 de 30.4.2004, p. 77).

<sup>(2)</sup> Regulamento (CE) n.º 562/2006 do Parlamento Europeu e do Conselho, de 15 de março de 2006, que estabelece o código comunitário relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen) (JO L 105 de 13.4.2006, p. 1).

2. Caso as transportadoras aéreas tenham recolhido dados referentes a informações prévias sobre passageiros (API) enumeradas no ponto 18 do anexo I, mas não os conservem pelos mesmos meios técnicos que os dados PNR, os Estados-Membros adotam as medidas necessárias para garantir que as transportadoras aéreas também transfiram, pelo método de exportação, esses dados para a UIP do Estado-Membro a que se refere o n.º 1. Em caso de tal transferência, todas as disposições da presente diretiva são aplicáveis aos dados API em causa.
3. As transportadoras aéreas transferem os dados PNR por via eletrónica, utilizando protocolos comuns e formatos de dados reconhecidos, adotados pelo procedimento de exame a que se refere o artigo 17.º, n.º 2, ou, em caso de avaria técnica, por quaisquer outros meios apropriados que assegurem um nível adequado de segurança dos dados:
  - a) 24 a 48 horas antes da hora programada da partida do voo; e
  - b) Imediatamente após o encerramento do voo, ou seja, logo que os passageiros se encontrem a bordo do avião preparados para partir e o embarque ou desembarque já não seja possível.
4. Os Estados-Membros autorizam as transportadoras aéreas a limitar as transferências referidas no n.º 3, alínea b), às atualizações das transferências referidas na alínea a) desse número.
5. Caso seja necessário aceder aos dados PNR para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou criminalidade grave, as transportadoras aéreas transmitem os dados PNR noutros momentos que não os mencionados no n.º 3, caso a caso e mediante pedido apresentado por uma UIP, nos termos do direito nacional.

#### Artigo 9.º

### Intercâmbio de informações entre Estados-Membros

1. Os Estados-Membros asseguram que, no que respeita a pessoas identificadas por uma UIP nos termos do artigo 6.º, n.º 2, todos os dados PNR relevantes e necessários, ou o resultado do seu tratamento, sejam transmitidos por essa UIP às UIP correspondentes dos outros Estados-Membros. Nos termos do artigo 6.º, n.º 6, as UIP dos Estados-Membros destinatários transmitem as informações recebidas às respetivas autoridades competentes.
2. A UIP de um Estado-Membro tem o direito de solicitar, se necessário, à UIP de qualquer outro Estado-Membro que lhe forneça dados PNR conservados na sua base de dados e ainda não anonimizados mediante mascaramento de elementos de dados, nos termos do artigo 12.º, n.º 2, e, se necessário, também o resultado do tratamento desses dados, se este já tiver sido efetuado nos termos do artigo 6.º, n.º 2, alínea a). Esse pedido é devidamente fundamentado e pode basear-se num elemento de dados ou numa combinação de tais elementos, consoante o que a UIP requerente entenda como adequado no âmbito de um caso específico de prevenção, deteção, investigação ou repressão de infrações terroristas ou de criminalidade grave. As UIP fornecem as informações requeridas logo que possível. Caso os dados solicitados tenham sido anonimizados mediante mascaramento de elementos de dados, nos termos do artigo 12.º, n.º 2, a UIP só fornece os dados PNR na íntegra se for razoável considerar que tal é necessário para o fim referido no artigo 6.º, n.º 2, alínea b), e apenas se para tal for autorizada por uma autoridade a que se refere o artigo 12.º, n.º 3, alínea b).
3. As autoridades competentes de um Estado-Membro só podem solicitar diretamente à UIP de qualquer outro Estado-Membro que lhes forneça dados PNR conservados na sua base de dados se necessário, em casos de emergência, e nas condições previstas no n.º 2. Os pedidos das autoridades competentes devem ser devidamente fundamentados. Deve ser sempre enviada uma cópia do pedido à UIP do Estado-Membro requerente. Em todos os outros casos, as autoridades competentes encaminham os seus pedidos através da UIP do seu próprio Estado-Membro.
4. Em circunstâncias excecionais, quando seja necessário aceder a dados PNR para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com a criminalidade grave, a UIP de um Estado-Membro tem o direito de solicitar à UIP de outro Estado-Membro que obtenha dados PNR, nos termos do artigo 8.º, n.º 5, e os forneça à UIP requerente.
5. O intercâmbio de informações previsto no presente artigo pode ser feito através de qualquer canal de cooperação existente entre as autoridades competentes dos Estados-Membros. A língua utilizada para o pedido e para o intercâmbio

de informações é a que for aplicável ao canal usado. Ao proceder às notificações nos termos do artigo 4.º, n.º 5, os Estados-Membros comunicam igualmente à Comissão os dados relativos aos pontos de contacto aos quais os pedidos podem ser enviados em caso de emergência. A Comissão comunica tais dados aos Estados-Membros.

#### Artigo 10.º

##### **Condições de acesso da Europol aos dados PNR**

1. A Europol está habilitada a solicitar dados PNR ou o resultado do seu tratamento às UIP dos Estados-Membros, nos limites das suas competências e para o exercício das suas funções.
2. A Europol pode apresentar, caso a caso, à UIP de qualquer Estado-Membro através da sua unidade nacional, um pedido eletrónico devidamente fundamentado de transmissão de dados PNR específicos ou dos resultados do tratamento desses dados. A Europol pode apresentar esse pedido quando tal for estritamente necessário para apoiar e reforçar a ação dos Estados-Membros na prevenção, deteção ou investigação de uma infração terrorista específica ou uma forma de criminalidade grave, na medida em que essa infração ou forma de criminalidade estejam abrangidas pelas competências da Europol nos termos da Decisão 2009/371/JAI. Esse pedido fundamentado indica os motivos razoáveis com base nos quais a Europol considera que a transmissão dos dados PNR ou dos resultados do tratamento dos dados PNR constitui um contributo substancial para a prevenção, deteção ou investigação da infração penal em causa.
3. A Europol comunica ao responsável pela proteção de dados, nomeado nos termos do artigo 28.º da Decisão 2009/371/JAI, todos os intercâmbios de informações realizados ao abrigo do presente artigo.
4. O intercâmbio de informações ao abrigo do presente artigo é feito através da rede SIENA, nos termos da Decisão 2009/371/JAI. A língua utilizada para o pedido e para o intercâmbio de informações é a que for aplicável na rede SIENA.

#### Artigo 11.º

##### **Transferência de dados para países terceiros**

1. Os Estados-Membros só podem transferir para um país terceiro os dados PNR e os resultados do seu tratamento que tenham sido armazenados pela UIP, nos termos do artigo 12.º, caso a caso e se:
  - a) Estiverem preenchidas as condições estabelecidas no artigo 13.º da Decisão-Quadro 2008/977/JAI;
  - b) A transferência for necessária para os fins prosseguidos pela presente diretiva referidos no artigo 1.º, n.º 2;
  - c) O país terceiro só aceitar transferir os dados para outro país terceiro caso tal seja estritamente necessário para os fins da presente diretiva referidos no artigo 1.º, n.º 2, e unicamente mediante autorização expressa desse Estado-Membro; e
  - d) Estiverem preenchidas as mesmas condições que as estabelecidas no artigo 9.º, n.º 2.
2. Sem prejuízo do artigo 13.º, n.º 2, da Decisão-Quadro 2008/977/JAI, a transferência de dados PNR sem autorização prévia do Estado-Membro a partir do qual foram obtidos os dados é permitida em circunstâncias excecionais e apenas se:
  - a) Essa transferência for essencial para dar resposta a uma ameaça específica e concreta relacionada com infrações terroristas ou com criminalidade grave num Estado-Membro ou um país terceiro; e
  - b) A autorização prévia não puder ser obtida em tempo útil.

A autoridade responsável por conceder a autorização é informada sem demora e a transferência é devidamente registada e sujeita a uma verificação *ex-post*.

3. Os Estados-Membros só podem transferir os dados PNR para as autoridades competentes de países terceiros em condições compatíveis com a presente diretiva, e apenas depois de se terem certificado de que o destinatário os tenciona utilizar de forma compatível com essas condições e salvaguardas.
4. O responsável pela proteção de dados da UIP do Estado-Membro que transfere os dados PNR é informado sempre que o Estado-Membro transfira dados PNR nos termos do presente artigo.



## Artigo 12.º

**Prazo de conservação e anonimização dos dados**

1. Os Estados-Membros asseguram que os dados PNR fornecidos pelas transportadoras aéreas à UIP sejam conservados numa base de dados dessa UIP por um prazo de cinco anos contados a partir da sua transferência para a UIP do Estado-Membro em cujo território o voo aterre ou de cujo território descole.
2. Decorrido um prazo de seis meses após a transferência dos dados PNR referida no n.º 1, todos os dados PNR são anonimizados mediante mascaramento dos seguintes elementos de dados suscetíveis de identificar diretamente o passageiro ao qual dizem respeito os dados PNR:
  - a) Nome(s), incluindo os nomes de outros passageiros mencionados nos PNR, bem como o número de passageiros nos PNR que viajam em conjunto;
  - b) Endereço e informações de contacto;
  - c) Todas as informações sobre os meios de pagamento, incluindo o endereço de faturação, na medida em que contenham informações suscetíveis de identificar diretamente o passageiro ao qual os PNR dizem respeito ou quaisquer outras pessoas;
  - d) Informação de passageiro frequente;
  - e) Observações gerais, na medida em que contenham informações suscetíveis de permitir identificar diretamente o passageiro ao qual os PNR dizem respeito; e
  - f) Quaisquer dados API que tenham sido recolhidos.
3. Decorrido o prazo de seis meses referido no n.º 2, só é permitida a divulgação dos dados PNR integrais caso essa divulgação seja:
  - a) Considerada necessária, com base em motivos razoáveis, para os fins referidos no artigo 6.º, n.º 2, alínea b); e
  - b) Autorizada por:
    - i) uma autoridade judiciária, ou
    - ii) outra autoridade nacional competente, nos termos do direito nacional, para verificar se estão reunidas as condições de divulgação, sob reserva de o responsável pela proteção de dados da UIP ser informado e proceder a uma verificação *ex-post*.
4. Os Estados-Membros asseguram que os dados PNR sejam apagados de forma definitiva no termo do prazo referido no n.º 1. Esta obrigação aplica-se sem prejuízo dos casos em que dados PNR específicos tenham sido transferidos para uma autoridade competente e sejam utilizados no âmbito de um caso específico para efeitos de prevenção, deteção, investigação ou repressão de infrações terroristas ou criminalidade grave; nesse caso a conservação dos dados pela autoridade competente rege-se pelo direito nacional.

5. O resultado do tratamento a que se refere o artigo 6.º, n.º 2, alínea a), só é conservado pela UIP durante o período necessário para informar as autoridades competentes e, nos termos do artigo 9.º, n.º 1, as UIP de outros Estados-Membros, de um resultado positivo. Caso se constate, na sequência de uma verificação individual por meios não automatizados referida no artigo 6.º, n.º 5, alínea a), que o resultado do tratamento automatizado é negativo, este pode, ainda assim, ser conservado a fim de evitar «falsos» resultados positivos no futuro, desde que os dados de base não sejam apagados, nos termos do n.º 4 do presente artigo.

## Artigo 13.º

**Proteção de dados pessoais**

1. Os Estados-Membros asseguram que, em qualquer tratamento de dados pessoais nos termos da presente diretiva, todos os passageiros tenham o mesmo direito à proteção dos seus dados pessoais, os direitos de acesso, retificação, apagamento e limitação, e os direitos a indemnização e recurso judicial, nos termos do direito da União e do direito nacional, e em aplicação dos artigos 17.º, 18.º, 19.º e 20.º da Decisão-Quadro 2008/977/JAI. Esses artigos são, por conseguinte, aplicáveis.

2. Os Estados-Membros prevêm que as disposições adotadas nos termos do direito nacional em aplicação dos artigos 21.º e 22.º da Decisão-Quadro 2008/977/JAI, respeitantes à confidencialidade do tratamento e à segurança dos dados, sejam igualmente aplicáveis a qualquer tratamento de dados pessoais efetuado nos termos da presente diretiva.

3. A presente diretiva não prejudica a aplicabilidade da Diretiva 95/46/CE do Parlamento Europeu e do Conselho <sup>(1)</sup> ao tratamento dos dados pessoais pelas transportadoras aéreas, em especial as suas obrigações de tomarem as medidas técnicas e organizativas adequadas para proteger a segurança e confidencialidade dos dados pessoais.

4. Os Estados-Membros proíbem o tratamento de dados PNR que revelem a raça ou origem étnica da pessoa, as suas opiniões políticas, religião ou convicções filosóficas, filiação sindical saúde, vida ou orientação sexual. Se receber dados PNR que revelem tais informações, a UIP apaga-os imediatamente.

5. Os Estados-Membros asseguram que a UIP conserve a documentação relativa a todos os sistemas e procedimentos de tratamento sob a sua responsabilidade. Essa documentação deve conter, no mínimo:

- a) O nome e os contactos da organização e do pessoal da UIP a quem é confiado o tratamento de dados PNR e os diferentes níveis de autorização de acesso;
- b) Os pedidos apresentados pelas autoridades competentes e pelas UIP de outros Estados-Membros;
- c) Todos os pedidos e transferências de dados PNR para um país terceiro.

A UIP disponibiliza toda a documentação existente à autoridade nacional de controlo, a pedido desta.

6. Os Estados-Membros asseguram que a UIP conserve registos, pelo menos, das seguintes operações de tratamento: recolha, consulta, divulgação e apagamento. Os registos das operações de consulta e de divulgação indicam, em especial, a finalidade, a data e a hora dessas operações e, se possível, a identidade da pessoa que consultou ou divulgou os dados PNR e a identidade dos destinatários desses dados. Os registos só podem ser utilizados para efeitos de verificação e de autocontrolo, para garantir a integridade e a segurança dos dados e para auditoria. A UIP disponibiliza os registos à autoridade nacional de controlo, a pedido desta.

Esses registos são conservados durante um prazo de cinco anos.

7. Os Estados-Membros asseguram que a respetiva UIP aplique medidas técnicas e organizativas e procedimentos adequados para garantir um elevado nível de segurança, adaptado aos riscos que o tratamento representa e à natureza dos dados PNR.

8. Os Estados-Membros asseguram que, caso a violação de dados pessoais seja suscetível de resultar num elevado risco para a proteção dos dados pessoais ou de prejudicar a privacidade do titular dos dados, a UIP comunique tal violação de dados ao titular dos dados e à autoridade nacional de controlo sem demora injustificada.

#### Artigo 14.º

#### Sanções

O Estados-Membros estabelecem as regras relativas às sanções aplicáveis à violação das disposições nacionais adotadas em aplicação da presente diretiva e tomam todas as medidas necessárias para assegurar a sua aplicação.

Em especial, os Estados-Membros estabelecem as regras relativas às sanções, incluindo sanções financeiras, a aplicar às transportadoras aéreas que não transmitam dados conforme previsto no artigo 8.º ou não os transmitam no formato requerido.

As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

<sup>(1)</sup> Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (JO L 281 de 23.11.1995, p. 31).

*Artigo 15.º***Autoridade nacional de controlo**

1. Cada Estado-Membro estabelece que a autoridade nacional de controlo referida no artigo 25.º da Decisão-Quadro 2008/977/JAI seja responsável por prestar aconselhamento e monitorizar a aplicação, no seu território, das disposições adotadas pelos Estados-Membros por força da presente diretiva. É aplicável o artigo 25.º da Decisão-Quadro 2008/977/JAI.
2. As referidas autoridades nacionais de controlo exercem as atividades previstas no n.º 1, tendo em vista a proteção dos direitos fundamentais no âmbito do tratamento de dados pessoais.
3. Cabe a cada autoridade nacional de controlo:
  - a) Analisar as reclamações apresentadas por qualquer titular de dados, investigar a questão e informar os titulares dos dados sobre os progressos e os resultados da reclamação num prazo razoável;
  - b) Verificar a legalidade do tratamento de dados, proceder a investigações, inspeções e auditorias nos termos do direito nacional, por sua própria iniciativa ou com base numa reclamação a que se refere a alínea a).
4. A autoridade nacional de controlo aconselha, mediante pedido, os titulares de dados sobre o exercício dos direitos previstos em disposições adotadas em aplicação da presente diretiva.

*CAPÍTULO III****Medidas de execução****Artigo 16.º***Protocolos comuns e formatos de dados reconhecidos**

1. Todas as transferências de dados PNR das transportadoras aéreas para as UIP para efeitos da presente diretiva são efetuadas por meios eletrónicos, que ofereçam garantias suficientes no que respeita às medidas técnicas de segurança e às medidas organizativas que regulam o tratamento a efetuar. Em caso de avaria técnica, os dados PNR podem ser transferidos por qualquer outro meio adequado, desde que o mesmo nível de segurança seja mantido e o direito da União em matéria de proteção de dados seja plenamente respeitado.
2. Um ano após a data em que a Comissão adotar, nos termos do n.º 3, pela primeira vez, os protocolos comuns e os formatos de dados reconhecidos, todas as transferências de dados PNR pelas transportadoras aéreas para as UIP para efeitos da presente diretiva são efetuadas eletronicamente através de métodos seguros, conformes com esses protocolos comuns. Tais protocolos são idênticos para todas as transferências, a fim de garantir a segurança dos dados PNR durante a transferência. Os dados PNR são transferidos num formato de dados reconhecido, a fim de assegurar a sua legibilidade por todas as partes envolvidas. Todas as transportadoras aéreas são obrigadas a selecionar e a identificar junto da UIP o protocolo comum e o formato de dados que tencionam utilizar para as suas transferências.
3. A Comissão elabora a lista dos protocolos comuns e dos formatos de dados reconhecidos e, se necessário, adapta-a por meio de atos de execução. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 17.º, n.º 2.
4. É aplicável o n.º 1 enquanto os protocolos comuns aceites e os formatos de dados reconhecidos referidos nos n.ºs 2 e 3 não estiverem disponíveis
5. No prazo de um ano a contar da data de adoção dos protocolos comuns e dos formatos de dados reconhecidos referidos no n.º 2, os Estados-Membros asseguram que sejam adotadas as medidas técnicas necessárias para permitir a utilização desses protocolos comuns e formatos de dados.

*Artigo 17.º***Procedimento de comité**

1. A Comissão é assistida por um comité. 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.

Na falta de parecer do Comité, a Comissão não adota o projeto de ato de execução, aplicando-se o artigo 5.º, n.º 4, terceiro parágrafo, do Regulamento (UE) n.º 182/2011.

*CAPÍTULO IV***Disposições finais***Artigo 18.º***Transposição**

1. Os Estados-Membros põem em vigor as disposições legislativas, regulamentares e administrativas necessárias para dar cumprimento à presente diretiva até 25 de maio de 2018. Comunicam imediatamente à Comissão o texto dessas disposições.

Quando os Estados-Membros adotarem essas disposições, estas incluem uma remissão para a presente diretiva ou são acompanhadas dessa remissão aquando da sua publicação oficial. Os Estados-Membros estabelecem o modo como deve ser feita a remissão e formulada a menção.

2. Os Estados-Membros comunicam à Comissão o texto das principais disposições de direito interno que adotarem no domínio regulado pela presente diretiva.

*Artigo 19.º***Reexame**

1. Com base nas informações prestadas pelos Estados-Membros, incluindo as informações estatísticas referidas no artigo 20.º, n.º 2, a Comissão procede, até 25 de maio de 2020, a um reexame de todos os elementos da presente diretiva e apresenta um relatório ao Parlamento Europeu e ao Conselho.

2. Ao proceder ao reexame, a Comissão presta especial atenção:

- a) Ao cumprimento das normas aplicáveis de proteção de dados pessoais;
- b) À necessidade e proporcionalidade da recolha e do tratamento dos dados PNR para cada um dos fins fixados na presente diretiva;
- c) À duração do prazo de conservação dos dados;
- d) À eficácia do intercâmbio de informações entre os Estados-Membros; e
- e) À qualidade das avaliações, nomeadamente no que respeita às informações estatísticas recolhidas nos termos do artigo 20.º.

3. O relatório referido no n.º 1 inclui também um reexame da necessidade, proporcionalidade e eficácia da inclusão, no âmbito de aplicação da presente diretiva, da recolha e transferência obrigatórias de dados PNR, no que respeita a todos os voos intra-UE ou a uma seleção destes. A Comissão tem em conta a experiência adquirida pelos Estados-Membros, especialmente por aqueles que aplicam a presente diretiva a voos intra-UE, nos termos do artigo 2.º. O relatório considera também a necessidade de incluir no âmbito de aplicação da presente diretiva operadores económicos que não sejam transportadoras, tais como agências de viagem e operadores turísticos que prestam serviços afins, incluindo a reserva de voos.

4. À luz do reexame efetuado nos termos do presente artigo, a Comissão apresenta, se necessário, ao Parlamento Europeu e ao Conselho uma proposta legislativa destinada a alterar a presente diretiva.

#### *Artigo 20.º*

##### **Dados estatísticos**

1. Os Estados-Membros fornecem anualmente à Comissão um conjunto de informações estatísticas sobre os dados PNR comunicados às UIP. As referidas estatísticas não podem incluir dados pessoais.
2. As estatísticas indicam, pelo menos:
  - a) O número total de passageiros cujos dados PNR foram objeto de recolha e de intercâmbio;
  - b) O número de passageiros identificados sujeitos a um controlo mais minucioso.

#### *Artigo 21.º*

##### **Relação com outros instrumentos**

1. Os Estados-Membros podem continuar a aplicar entre si os acordos ou convénios bilaterais ou multilaterais em matéria de intercâmbio de informações entre autoridades competentes que estejam em vigor em 24 de maio de 2016, na medida em que tais acordos ou convénios sejam compatíveis com esta última.
2. A presente diretiva não prejudica a aplicabilidade da Diretiva 95/46/CE ao tratamento de dados pessoais pelas transportadoras aéreas.
3. A presente diretiva aplica-se sem prejuízo das obrigações e dos compromissos já assumidos pelos Estados-Membros ou pela União por força de acordos bilaterais ou multilaterais com países terceiros.

#### *Artigo 22.º*

##### **Entrada em vigor**

A presente diretiva entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Os destinatários da presente diretiva são os Estados-Membros, em conformidade com os Tratados.

Feito em Bruxelas, em 27 de abril de 2016.

*Pelo Parlamento Europeu*  
O Presidente  
M. SCHULZ

*Pelo Conselho*  
A Presidente  
J.A. HENNIS-PLASSCHAERT

## ANEXO I

## Dados dos registos de identificação dos passageiros recolhidos pelas transportadoras aéreas

1. Código de identificação do registo PNR
  2. Data da reserva/emissão do bilhete
  3. Data(s) da viagem prevista
  4. Nome(s)
  5. Endereço e informações de contacto (número de telefone, endereço de correio eletrónico)
  6. Todas as informações sobre as modalidades de pagamento, incluindo o endereço de faturação
  7. Itinerário completo para o PNR em causa
  8. Informação de passageiro frequente
  9. Agência/agente de viagens
  10. Situação do passageiro, incluindo confirmações, situação do registo, não comparência ou passageiro de última hora sem reserva
  11. Informação do PNR separada/dividida
  12. Observações gerais (designadamente todas as informações disponíveis sobre menores não acompanhados com idade inferior a 18 anos, como nome e sexo do menor, idade, língua(s) falada(s), nome e contactos da pessoa que o acompanha no momento da partida e sua relação com o menor, nome e contactos da pessoa que o acompanha no momento da chegada e sua relação com o menor, agente presente na partida e na chegada)
  13. Informações sobre a emissão dos bilhetes, incluindo número do bilhete, data de emissão, bilhetes só de ida, dados ATFQ (Automatic Ticket Fare Quote)
  14. Número do lugar e outras informações relativas ao lugar
  15. Informações sobre a partilha de código
  16. Todas as informações relativas às bagagens
  17. Número e outros nomes de passageiros que figuram no PNR
  18. Todas as informações prévias sobre os passageiros (dados API) que tenham sido recolhidas (incluindo, tipo e número de documento(s), país de emissão e termo de validade do(s) documento(s), nacionalidade, nome(s) e apelido(s), sexo, data de nascimento, companhia aérea, número de voo, data de partida, data de chegada, aeroporto de partida, aeroporto de chegada, hora de partida e hora de chegada)
  19. Historial completo das modificações dos dados PNR enumerados nos pontos 1 a 18.
-

## ANEXO II

## Lista de infrações a que se refere o artigo 3.º, n.º 9

1. Participação em organização criminosa
  2. Tráfico de seres humanos
  3. Exploração sexual de crianças e pedopornografia
  4. Tráfico de estupefacientes e substâncias psicotrópicas
  5. Tráfico de armas, munições e explosivos
  6. Corrupção
  7. Fraude, incluindo a fraude lesiva dos interesses financeiros da União
  8. Branqueamento dos produtos do crime e contrafação de moeda, incluindo o euro
  9. Criminalidade informática/cibercrime
  10. Crimes contra o ambiente, incluindo o tráfico de espécies animais ameaçadas e de espécies e variedades vegetais ameaçadas
  11. Auxílio à entrada e à permanência irregulares
  12. Homicídio voluntário, ofensas corporais graves
  13. Tráfico de órgãos e tecidos humanos
  14. Rapto, sequestro e tomada de reféns
  15. Assalto organizado ou à mão armada
  16. Tráfico de bens culturais, incluindo antiguidades e obras de arte
  17. Contrafação e piratagem de produtos
  18. Falsificação de documentos administrativos e respetivo tráfico
  19. Tráfico de substâncias hormonais e de outros estimuladores de crescimento
  20. Tráfico de materiais nucleares e radioativos
  21. Violação
  22. Crimes abrangidos pela jurisdição do Tribunal Penal Internacional
  23. Desvio de avião ou navio
  24. Sabotagem
  25. Tráfico de veículos roubados
  26. Espionagem industrial
-











ISSN 1977-0774 (edição eletrónica)  
ISSN 1725-2601 (edição em papel)



**Serviço das Publicações da União Europeia**  
2985 Luxemburgo  
LUXEMBURGO

**PT**