Conselho da
União Europeia

Bruxelas, 28 de janeiro de 2016
(OR. en)

5455/16

Dossiê interinstitucional:
2012/0011 (COD)

DATAPROTECT 3
JAI 44
MI 27
DIGIT 2
DAPIX 13
FREMP 5
COMIX 39
CODEC 55

NOTA PONTO "I/A"

de:	Presidência
para:	Comité de Representantes Permanentes/Conselho
n.º doc. ant.:	15321/15
Assunto:	Proposta de regulamento do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (regulamento geral sobre a proteção de dados) [primeira leitura] – Acordo político

INTRODUÇÃO

1. Em 25 de janeiro de 2012, Comissão apresentou um pacote global para a proteção de dados, que compreendia:

   – a proposta de regulamento geral sobre a proteção de dados referida em epígrafe, que visa substituir a Diretiva relativa à proteção de dados de 1995 (antigo primeiro pilar);

   – uma proposta de diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou de execução de sanções penais, e à livre circulação desses dados, que visa substituir a Decisão-Quadro sobre a proteção de dados, de 2008 (antigo terceiro pilar).

2. O regulamento geral sobre a proteção de dados tem por objetivo reforçar os direitos das pessoas singulares em matéria de proteção de dados e facilitar a livre circulação de dados pessoais no mercado único digital, nomeadamente reduzindo a carga administrativa.

3. O Parlamento Europeu adotou em primeira leitura o regulamento geral sobre a proteção de dados proposto, em 12 de março de 2014 (7427/14).

4. Em 15 de junho de 2015, o Conselho chegou a acordo a respeito de uma abordagem geral (9565/15) referente ao regulamento geral sobre a proteção de dados, conferindo desse modo à Presidência um mandato de negociação para encetar trílogos com o Parlamento Europeu.

5. Desde junho de 2015, realizaram-se dez trílogos, após os quais a Presidência e os representantes do Parlamento Europeu, com a assistência da Comissão, chegaram a acordo quanto ao texto de compromisso global.

6. Na reunião de 16 de dezembro, o Comité de Representantes Permanentes subscreveu o texto que resultou do trílogo de 15 de dezembro de 2015.

7. A Comissão LIBE do Parlamento Europeu levou o texto acordado no trílogo a votação, numa reunião extraordinária realizada a 17 de dezembro. No mesmo dia, o Presidente do Comité de Representantes Permanentes recebeu do Presidente da Comissão LIBE uma carta (15323/15) em que este lhe comunicava que iria recomendar à Comissão LIBE e à Plenária que, sob reserva da revisão jurídico-linguística do texto, aprovassem sem alterações o acordo alcançado no trílogo.

8. Na reunião de 18 de dezembro de 2015, o COREPER confirmou o texto, na perspetiva de um acordo (15321/15).

9. Convida-se o Comité de Representantes Permanentes a recomendar ao Conselho que adote o acordo político a respeito do texto do regulamento geral sobre a proteção de dados na versão que consta do anexo à presente nota.

ANEXO

REGULAMENTO (UE) N.º XXX/2016
DO PARLAMENTO EUROPEU E DO CONSELHO

relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (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[1],

Tendo em conta o parecer do Comité das Regiões[2],

Tendo em conta o parecer da Autoridade Europeia para a Proteção de Dados[3],

Deliberando de acordo com o processo legislativo ordinário[4],

---

1 **[XXX]**
2 **[XXX]**
3 **[XXX]**
4 Posição do Parlamento Europeu de 14 de março de 2014 e Decisão do Conselho de **[XXX]**.

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 e o artigo 16.º, n.º 1, do Tratado 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. Tal deverá 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.

(3) A Diretiva 95/46/CE do Parlamento Europeu e do Conselho, 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.

(3-A) O tratamento dos dados pessoais deve ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto, mas 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 os princípios reconhecidos na Carta dos Direitos Fundamentais da União Europeia, consagrados nos Tratados, nomeadamente o direito ao respeito pela vida privada e familiar, o direito ao respeito pelo domicílio e pelas comunicações, o direito à proteção dos dados pessoais, o direito à liberdade de pensamento, de consciência e de religião, o direito à liberdade de expressão e de informação, o direito à liberdade de empresa, o direito à ação e a um tribunal imparcial, bem como o respeito pela diversidade cultural, religiosa e linguística.

(4) A integração económica e social resultante do funcionamento do mercado interno provocou um aumento significativo dos fluxos transfronteiriços. O intercâmbio de dados entre intervenientes públicos e privados, incluindo as pessoas, 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.

(5) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados registaram um espetacular aumento. 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 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 na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.

(6) 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 deverão poder controlar a utilização que é feita dos seus dados pessoais, e deverá ser reforçada a segurança jurídica e prática para as pessoas singulares, os operadores económicos e as autoridades públicas.

(6-A) Nos casos em que o presente regulamento preveja especificações ou restrições das suas regras pela legislação dos Estados-Membros, estes podem incorporar elementos do 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.

(7) Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação no modo como a proteção dos dados é aplicada a nível da UE, nem a insegurança jurídica nem o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas, particularmente nas atividades em linha. As diferenças entre os Estados-Membros quanto ao nível de proteção dos direitos e das liberdades individuais, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados, podem impedir a livre circulação de dados pessoais na União. Estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da UE, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Estas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.

(8) Para 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 individuais relativamente ao tratamento desses dados deverá ser equivalente em todos os Estados-Membros. É conveniente assegurar em toda a União a aplicação coerente e homogénea 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 dos dados, 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 dados sensíveis. Nessa medida, o regulamento não exclui legislação dos Estados-Membros que defina as circunstâncias de situações específicas de tratamento, incluindo a determinação mais precisa das condições em que é lícito o tratamento de dados pessoais.

(9) A proteção eficaz dos dados pessoais na União exige não só que sejam reforçados e especificados os direitos dos titulares dos dados e as obrigações dos responsáveis pelo tratamento e pela definição do tratamento dos dados pessoais, mas também que haja poderes equivalentes para controlar e assegurar a conformidade com as regras de proteção dos dados pessoais e sanções equivalentes para os infratores nos Estados-Membros.

(10) O artigo 16.º, n.º 2, do Tratado 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.

(11) 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 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 aos cidadãos de todos os Estados-Membros um mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento dos dados 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 não permite que a livre circulação de dados pessoais na União seja 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 um determinado número de derrogações. Além disso, as instituições e os órgãos da União, 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. Para definir a noção de micro, pequenas e médias empresas, é conveniente ter em conta a Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas.

(12) A proteção conferida pelo presente regulamento diz respeito às pessoas singulares, independentemente da sua nacionalidade ou local de residência, relativamente ao tratamento de dados pessoais. No que respeita ao tratamento de dados relativos a pessoas coletivas, em especial a empresas estabelecidas na qualidade de pessoas coletivas, incluindo a denominação, a forma jurídica e os contactos da pessoa coletiva, a proteção conferida pelo presente regulamento não pode ser invocada por qualquer pessoa.

(13) A proteção das pessoas singulares deverá ser neutra em termos tecnológicos e independente das técnicas utilizadas, sob pena de haver sério risco de ser contornada. Deverá aplicar-se ao tratamento de dados pessoais por meios automatizados, bem como ao tratamento manual, se os dados estiverem contidos em ficheiros ou a eles se destinam. 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 do presente regulamento.

(14) O presente regulamento não cobre questões de defesa dos direitos e das liberdades fundamentais ou da livre circulação de dados relacionados com atividades que se encontrem fora do âmbito de aplicação do direito da União, como as que se prendem com a segurança nacional, nem abrange o tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relacionadas com a política externa e de segurança comum da União.

(14-A) O Regulamento (CE) n.º 45/2001 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 instrumentos jurídicos da União aplicáveis ao tratamento de dados pessoais, deverão ser adaptados aos princípios e regras do 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, devem ser realizadas as necessárias adaptações do Regulamento (CE) n.º 45/2001, a fim de permitir a aplicação em simultâneo com o presente regulamento.

(15) O presente regulamento não deverá ser aplicável ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas, portanto sem qualquer ligação com uma atividade profissional ou comercial. As atividades pessoais ou domésticas poderão também incluir a troca de correspondência e a conservação de listas de endereços ou as atividades desenvolvidas no âmbito das redes sociais e do ambiente em linha, no contexto dessas mesmas atividades pessoais ou domésticas. Todavia, o presente Regulamento deverá ser aplicável aos responsáveis pelo tratamento dos dados e aos subcontratantes que forneçam os meios para o tratamento dos dados pessoais dessas atividades pessoais ou domésticas.

(16) 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 instrumento jurídico específico a nível da União. Por essa razão, o presente regulamento não deverá ser aplicável às atividades de tratamento para esses efeitos. Todavia, o tratamento de dados pessoais pelas autoridades competentes ao abrigo do presente regulamento para os referidos efeitos deverá ser regulado por esse instrumento jurídico mais específico a nível da União (Diretiva XX/YYY). Os Estados-Membros podem confiar às autoridades competentes na aceção da Diretiva XX/YYY outras 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 regulamento geral sobre a proteção de dados, os Estados-Membros podem manter ou aprovar disposições mais específicas para adaptar a aplicação das regras previstas no regulamento geral sobre a proteção de dados. 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.

(16-A) Na medida em que o presente regulamento é igualmente aplicável 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 quando os tribunais atuarem no âmbito das suas capacidades jurisdicionais, a fim de assegurar a independência do poder judicial no exercício das suas funções jurisdicionais, nomeadamente a tomada de decisões. O controlo de tais operações de tratamento de dados pode ser confiado a organismos específicos no âmbito do sistema judicial do Estado-Membro, que deverá controlar, em particular, o cumprimento das regras estabelecidas no presente regulamento, promover a sensibilização do poder judicial para as obrigações que lhe são impostas pelo presente regulamento e dar seguimento às reclamações relativas ao tratamento dos dados.

(17) O presente regulamento não deverá prejudicar a aplicação da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, 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.

(18) (...)

(19) Qualquer tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento dos dados ou de um subcontratante situado na União deverá ser feito em conformidade com o presente regulamento, independentemente de o tratamento em si ser realizado dentro ou fora da 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 neste contexto.

(20) 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 dos dados 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 ou não associadas a um pagamento. A fim de determinar se o responsável pelo tratamento dos dados 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 Internet do responsável pelo tratamento dos dados ou de um intermediário, ou 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, e/ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento dos dados tem a intenção de oferecer bens ou serviços a esses titulares de dados na União.

(21) 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, desde que o seu comportamento tenha lugar na União Europeia. A fim de determinar se uma atividade de tratamento pode ser considerada "controlo do comportamento" de titulares de dados, deverá apurar-se se essas pessoas são seguidas na Internet e a potencial utilização subsequente de técnicas de tratamento de dados 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.

(22) Sempre que a legislação nacional de um Estado-Membro seja aplicável por força do direito internacional público, o presente regulamento é aplicável igualmente aos responsáveis pelo tratamento de dados não estabelecidos na União, por exemplo numa missão diplomática ou num posto consular de um Estado-Membro.

(23) Os princípios da proteção de dados deverão aplicar-se a qualquer informação relativa a uma pessoa singular identificada ou identificável. Os dados que tenham sido pseudonimizados, mas possam ser atribuídos a uma pessoa singular mediante a utilização de informações suplementares, deverão ser considerados como informações sobre uma pessoa singular identificável. Para determinar se uma pessoa é identificável, importa considerar todos os meios suscetíveis de ser razoavelmente utilizados, tais como a seleção, quer pelo responsável pelo tratamento dos dados quer por qualquer outra pessoa, para identificar direta ou indiretamente a referida pessoa. Para determinar se há uma probabilidade razoável de os meios serem utilizados para identificar a pessoa, 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 tornados de tal forma 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.

(23-AA) O presente regulamento não deverá ser aplicado aos dados de pessoas falecidas. Os Estados-Membros podem prever regras para o tratamento dos dados de pessoas falecidas.

(23-A) A aplicação da pseudonimização aos dados pessoais pode reduzir os riscos para os titulares de dados em questão e ajudar os responsáveis pelo tratamento dos dados e os seus subcontratantes a cumprir as suas obrigações de proteção de dados. A introdução explícita da "pseudonimização" através dos artigos do presente regulamento não se destina, pois, a excluir eventuais outras medidas de proteção de dados.

(23-B) (...)

(23-C) A fim de criar incentivos para aplicar a pseudonimização durante o tratamento de dados pessoais, deverá ser possível tomar medidas de pseudonimização que permitam uma análise geral no âmbito do mesmo responsável pelo tratamento dos dados se este tiver tomado as medidas técnicas e organizativas necessárias para garantir, para o respetivo tratamento, a aplicação das disposições do presente regulamento, e assegurando que são conservadas em separado as informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico. São igualmente consideradas responsáveis pelo tratamento dos dados as pessoas autorizadas no âmbito do mesmo responsável pelo tratamento dos dados.

(24) As pessoas singulares podem ser associadas a identificadores em linha, 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.

(24-C novo) As autoridades públicas a quem os dados forem divulgados em cumprimento de 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 poderão ser consideradas destinatárias se receberem dados 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 nem implicar a interconexão de ficheiros. O tratamento destes dados por essas autoridades públicas deverá cumprir as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.

(25) O consentimento do titular dos dados deve ser dado mediante uma ação positiva clara 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 na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante qualquer 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 os fins a que se destine. 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.

(25-AA) Muitas vezes não é possível identificar na totalidade as finalidades do tratamento de dados para fins 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 em consonância 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.

(25-A) Os dados genéticos deverão ser definidos como todos os dados pessoais relacionados com as características genéticas de uma pessoa, hereditárias ou adquiridas, resultantes da análise de uma amostra biológica da pessoa em causa, designadamente da análise de cromossomas, do ácido desoxirribonucleico (ADN), do ácido ribonucleico (ARN), ou de qualquer outro elemento que permita obter informações equivalentes.

(26) 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, incluindo informações sobre a pessoa recolhidas durante a sua inscrição para a prestação de serviços de saúde e durante essa prestação, conforme referido na Diretiva 2011/24/UE; qualquer número, símbolo ou sinal particular atribuído a uma pessoa 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 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 real 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*.

(27) O estabelecimento principal de um responsável pelo tratamento dos dados 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 dos dados na União. Nesse caso, este último deverá ser considerado o estabelecimento principal. O estabelecimento principal de um responsável pelo tratamento dos dados 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 meios de tratamento mediante instalações estáveis. Este critério não deverá depender do facto de o tratamento ser efetivamente 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, o referido 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, e, 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 dos dados como o subcontratante, a autoridade de controlo principal deverá continuar a ser a autoridade de controlo do Estado-Membro onde o responsável pelo tratamento dos dados tem o estabelecimento principal, mas a autoridade de controlo do subcontratante deverá ser considerada uma autoridade de controlo interessada e 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 quando o projeto de decisão diga respeito apenas ao responsável pelo tratamento dos dados. 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 meios do tratamento sejam determinados por uma outra empresa.

(28) 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 central que controla o tratamento dos dados pessoais nas empresas a ela associadas constitui juntamente com estas empresas uma entidade que pode ser tratada como um "grupo empresarial".

(29) As crianças carecem de proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências, garantias e direitos relacionados com o tratamento dos seus dados pessoais. Trata-se, em especial, da utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como da recolha de dados de crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular da responsabilidade parental não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança.

(30) O tratamento de dados pessoais deverá ser efetuado de forma lícita e equitativa. Deverá ser transparente para as pessoas em causa a forma como os dados que lhes dizem respeito são recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento, bem como a medida em que esses dados são ou virão a ser tratados. O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento dos referidos dados sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples. Este princípio aplica-se, 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 em causa, bem como a salvaguardar o seu direito a obter a confirmação e a comunicação dos dados pessoais tratados que lhes dizem respeito. As pessoas 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 ao tratamento desses dados. Em especial, as finalidades específicas do tratamento deverão ser explícitas e legítimas e ser determinadas aquando da recolha dos dados. Os dados deverão ser adequados, pertinentes e limitados ao necessário para os efeitos para os quais são tratados; para tal, é especialmente necessário garantir que o período de conservação dos dados seja limitado ao mínimo. 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 dos dados deverá fixar os prazos para o seu 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, nomeadamente para evitar o acesso ou a utilização desses dados e do equipamento utilizado para o seu tratamento por parte de pessoas não autorizadas.

(31) Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da pessoa em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro ato legislativo da União ou de um Estado-Membro, nos termos do presente regulamento, sendo nomeadamente necessário que sejam cumpridas as obrigações legais a que o responsável pelo tratamento dos dados se encontre sujeito ou executados contratos em que o titular dos dados seja parte ou ainda que sejam efetuadas as diligências pré-contratuais que esse mesmo titular solicitar.

(31-A) Sempre que o presente regulamento se refira a uma base jurídica ou a uma medida legislativa, tal não significa necessariamente a obrigatoriedade de um ato legislativo adotado por um parlamento, sem prejuízo dos requisitos que decorram da ordem constitucional do Estado-Membro em questão. No entanto, tal base jurídica ou medida legislativa deverá ser clara e precisa e a sua aplicação deverá ser previsível para os particulares, como exigido pela jurisprudência do Tribunal de Justiça da União Europeia e pelo Tribunal Europeu dos Direitos do Homem.

(32) Sempre que o tratamento for realizado com base no consentimento do titular dos dados, o responsável pelo tratamento dos dados 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. Nos termos da Diretiva 93/13/CEE[1] do Conselho deverá ser fornecida uma declaração de consentimento previamente formulada pelo responsável pelo tratamento dos dados, 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 dos dados 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 tiver verdadeira liberdade de escolha e não puder recusar nem retirar o consentimento sem ser prejudicado.

(33) (...)

(34) Para que fique salvaguardado 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, em especial quando o responsável é uma autoridade pública e isso torne 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, 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 tal não ser necessário para a mesma execução.

(35) O tratamento deverá ser considerado lícito quando se revelar necessário no contexto de um contrato ou da intenção de celebrar um contrato.

(35-A) (...)

(36) Sempre que o tratamento dos dados for realizado em cumprimento de uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento dos dados, ou se o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública, o tratamento deverá ter uma base no direito da União ou na legislação nacional de um Estado-Membro. O presente regulamento não exige que haja 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 dos dados, 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 base poderá especificar as condições gerais do regulamento que rege a legalidade do tratamento dos dados, fixar regras específicas para determinar os responsáveis pelo tratamento dos dados, o tipo de dados a tratar, os titulares em questão, as entidades a que os dados podem ser comunicados, os limites a que as finalidades do tratamento devem obedecer, os prazos de conservação e outras medidas destinadas a garantir a legalidade e lealdade do tratamento. Deverá igualmente caber ao direito da União ou dos Estados-Membros determinar se o responsável pelo tratamento dos dados 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 de direito privado, por exemplo uma associação profissional, quando tal se justifique por motivos de interesse público, nomeadamente motivos de saúde pública e proteção social e de gestão dos serviços de saúde.

(37) O tratamento de dados pessoais deverá ser igualmente considerado lícito quando for necessário à proteção de um interesse essencial à vida do titular dos dados ou de qualquer outra pessoa. Em princípio, os dados pessoais só podem ser tratados com base no interesse vital de outra pessoa singular quando o tratamento não se puder basear manifestamente noutra base jurídica. Alguns tipos de tratamento de dados podem servir tanto importantes interesses públicos como interesses vitais do titular dos dados, por exemplo, se o tratamento for necessário para fins humanitários, nomeadamente 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.

(38) Os interesses legítimos dos responsáveis pelo tratamento dos dados, incluindo aqueles a quem os dados 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 dos dados, em situações como aquela em que o titular dos dados é cliente ou está ao serviço do responsável pelo tratamento dos dados. 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 são recolhidos, que estes 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 dos dados, 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 a base jurídica para autorizar as autoridades a procederem ao tratamento de dados, este fundamento jurídico não deverá ser aplicável aos tratamentos efetuados pelas autoridades públicas no exercício das suas funções. 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.

(38-A) Os responsáveis pelo tratamento dos dados 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.

(39) O tratamento de dados, 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 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 dos dados. 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.

(40) O tratamento de dados pessoais para outros fins que não aqueles para os quais os dados tenham sido inicialmente recolhidos apenas deverá ser autorizado se for compatível com as finalidades para as quais os dados tenham sido inicialmente recolhidos. Nesse caso não é necessário um fundamento jurídico distinto do que permitiu a recolha dos dados. 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 dos dados, o direito da União ou dos Estados-Membros pode determinar e definir as tarefas e finalidades para as quais o tratamento posterior será considerado compatível e lícito. As operações de tratamento posterior para fins de arquivo de interesse público, para fins estatísticos ou de investigação científica e histórica 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 estes 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 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 dos dados, a natureza dos dados, 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. Quando o titular dos dados tiver dado o seu consentimento ou o tratamento se basear 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 dos dados deverá ser autorizado a proceder ao tratamento posterior dos dados, 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 dados relativos a eventuais atos criminosos ou ameaças à segurança pública e a transmissão dos dados 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 dos dados. Todavia, deverá ser proibido proceder à transmissão no interesse legítimo do responsável pelo tratamento dos dados ou ao tratamento posterior de dados pessoais se a operação não for compatível com alguma obrigação legal, profissional ou outra obrigação vinculativa de confidencialidade.

(41) 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 pode implicar riscos importantes 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 será sistematicamente um tratamento sensível, uma vez que serão apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de um indivíduo. Tais dados não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que a legislação dos Estados-Membros pode estabelecer disposições específicas em matéria de proteção de dados, 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 dos dados. 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.

(42) As derrogações à proibição de tratamento de categorias de dados sensíveis deverão ser igualmente permitidas se forem previstas no direito da União ou dos Estados-Membros e, sob reserva de garantias adequadas, de forma a proteger os dados pessoais e outros direitos fundamentais, quando motivos de interesse público o justificarem, em especial, o tratamento de dados em matéria de legislação laboral, 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. Tal poderá ser feito 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, para fins de arquivo de interesse público ou para fins estatísticos ou de investigação histórica e científica. Deverá também ser prevista uma derrogação que permita o tratamento desses dados quando tal for necessário à declaração, ao exercício ou à defesa de um direito, independentemente de se tratar de um processo judicial, administrativo ou extrajudicial.

(42-A) As categorias especiais de dados pessoais que merecem uma proteção mais elevada só podem ser objeto de tratamento para fins relacionados com a saúde quando tal for necessário para atingir os objetivos no interesse das pessoas 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, para fins de arquivo de interesse público, para fins estatísticos ou de investigação histórica e científica 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. Os Estados-Membros deverão ser autorizados a manter ou introduzir outras condições, incluindo limitações, no que diz respeito ao tratamento de dados genéticos, biométricos ou dados relativos à saúde. Tal não deverá, no entanto, impedir a livre circulação de dados na União, quando essas condições se aplicam ao tratamento transfronteiras desses dados.

(42-B) 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. Este tratamento é objeto de medidas adequadas e específicas, a fim de defender os direitos e liberdades das pessoas. 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, de 16 de dezembro de 2008, relativo às estatísticas da União sobre saúde pública e saúde e segurança no trabalho, designando todos os elementos relacionados com a saúde, nomeadamente, 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 pessoais sobre a saúde autorizadas por motivos de interesse público não deverão ter por resultado que os dados sejam tratados para outros fins por terceiros, nomeadamente empregadores, companhias de seguros e entidades bancárias.

(43) 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.

(44) Sempre que, no âmbito do exercício de atividades eleitorais, o funcionamento do sistema democrático exigir, num Estado-Membro, que os partidos políticos recolham dados sobre a opinião política dos cidadãos, o tratamento desses dados pode ser autorizado por motivos de interesse público, desde que sejam estabelecidas garantias adequadas.

(45) Se os dados tratados pelo responsável pelo tratamento dos dados 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 dos dados 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 mecanismo de autenticação com os mesmos dados de identificação usados pelo titular dos dados para aceder aos serviços em linha do responsável pelo tratamento dos dados.

(46) 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, adicionalmente, que se recorra à visualização sempre que for adequado. Tais informações poderão ser fornecidas por via eletrónica, por exemplo num sítio Web, quando se destinarem ao público. Isto é especialmente relevante em situações, como a publicidade em linha, a proliferação de operadores e a complexidade tecnológica das práticas, que tornem difícil que o titular dos dados saiba e compreenda se os seus dados pessoais estão a ser recolhidos, por quem e para que fins. Uma vez que as crianças carecem de proteção especial, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá estar redigida numa linguagem clara e simples que a criança compreenda facilmente.

(47) Deverão ser previstas modalidades para facilitar o exercício, pelo titular dos dados, dos direitos que lhe são conferidos nos termos do presente regulamento, incluindo mecanismos para solicitar e eventualmente obter a título gratuito, em especial, o acesso aos dados, a retificação, a supressão e o exercício do seu direito de oposição. O responsável pelo tratamento dos dados deverá pois 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 dos dados deverá ser obrigado a responder aos pedidos do titular sem demora injustificada e o mais tardar dentro de um mês e expor as suas razões quando tiver intenção de recusar o pedido.

(48) 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 dos dados deverá fornecer ao titular as informações adicionais necessárias para garantir 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 forem recolhidos junto do titular dos dados, este deve ser também informado da eventual obrigatoriedade de fornecer esses dados e das consequências de não os facultar. Estas informações podem ser fornecidas em combinação com ícones normalizados a fim de dar, de forma facilmente visível, inteligível e claramente legível uma útil perspetiva geral do tratamento previsto. Se forem apresentados por via eletrónica, os ícones deverão ser de leitura automática.

(49) As informações sobre o tratamento de dados pessoais deverão ser fornecidas ao titular dos dados no momento da sua recolha ou, se os dados não tiverem sido obtidos junto do seu titular, mas a partir de outra fonte, dentro de um prazo razoável, consoante as circunstâncias. Sempre que os dados forem suscetíveis de ser legitimamente comunicados a outro destinatário, o seu titular deverá ser informado aquando da primeira comunicação a esse destinatário. Sempre que o responsável pelo tratamento dos dados tiver a intenção de tratar os dados para outro fim que não aquele para o qual os dados tenham sido recolhidos, antes desse tratamento o responsável deverá fornecer ao titular dos dados informações sobre esse fim e outras informações necessárias. Quando não for possível informar o titular da origem dos dados por se ter recorrido a várias fontes, deverão ser-lhe fornecidas informações genéricas.

(50) Todavia, não é necessário impor tal obrigação quando o titular dos dados já dispuser dessa informação, ou se a lei previr expressamente o registo ou a comunicação dos dados, ou se a informação ao titular dos dados se revelar impossível de concretizar ou implicar um esforço desproporcionado. Tal seria o caso de um tratamento efetuado para fins de arquivo de interesse público, para fins estatísticos ou de investigação histórica e científica; para este efeito, pode ser considerado o número de titulares de dados, a antiguidade dos dados e as devidas garantias que tenham sido adotadas.

(51) 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. Aqui se inclui o seu direito de acederem aos dados pessoais 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, em especial, das finalidades a que se destina o tratamento dos seus dados, se possível, da duração da sua conservação, da identidade dos destinatários, da lógica subjacente ao eventual tratamento automático dos dados e das suas possíveis consequências, pelo menos quando tiver por base a definição de perfis. Quando possível, o responsável pelo tratamento dos dados poderá facultar o acesso a um sistema seguro em linha que possibilite ao titular aceder diretamente aos seus dados pessoais. Este direito não deverá prejudicar os direitos e as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, estas considerações não deverão resultar na recusa total de prestação de informações ao titular dos dados. Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, pode 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.

(52) O responsável pelo tratamento dos dados deverá adotar todas as medidas razoáveis para verificar a identidade do titular dos dados que solicite o acesso, em especial no contexto de serviços em linha e de identificadores em linha. Os responsáveis pelo tratamento dos dados não deverão conservar dados pessoais com a finalidade exclusiva de estar em condições de reagir a eventuais pedidos.

(53) As pessoas singulares deverão ter direito a que os dados que lhes digam respeito sejam retificados e o "direito a serem esquecidas" quando a conservação desses dados não cumprir o disposto no presente regulamento ou no direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento dos dados. 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, sempre que os titulares dos dados retirem o seu consentimento ao tratamento ou se oponham ao tratamento de dados pessoais que lhes digam respeito ou se o tratamento dos seus dados pessoais não respeitar o disposto no presente regulamento. Este direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança, não estando 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 este direito independentemente do facto de já ser adulto. No entanto, o prolongamento da conservação dos dados 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 dos dados, por motivos de interesse público no domínio da saúde pública, para fins de arquivo de interesse público, para fins estatísticos ou de investigação histórica e científica ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

(54) Para reforçar o "direito a ser esquecido" no ambiente em linha, o âmbito do direito ao apagamento deverá também ser alargado de forma a que o responsável pelo tratamento de dados que tenha tornado públicos os dados pessoais seja obrigado a informar os responsáveis que estejam a tratar esses dados, para que estes suprimam quaisquer ligações para esses dados pessoais, cópias ou reproduções dos mesmos. De forma a assegurar a informação supramencionada, o responsável pelo tratamento dos dados 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 os responsáveis que estejam a tratar os dados.

(54-A) Para restringir o tratamento de dados pessoais pode recorrer-se a métodos como a transferência temporária de determinados dados para outro sistema de tratamento ou impedir o acesso a determinados dados por parte dos utilizadores, ou ainda retirar temporariamente de um sítio Web dados aí publicados. Nos ficheiros automatizados, as restrições ao tratamento dos dados pessoais deverão, em princípio, ser impostas por meios técnicos de modo a que os dados não sejam sujeitos a outras operações de tratamento e não possam voltar a ser alterados; deverá indicar-se de forma bem clara no sistema que o tratamento dos dados pessoais se encontra sujeito a restrições.

(55) 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 de dados, num formato estruturado, de uso corrente, de leitura automática e interoperável, e a transmiti-los a outro responsável. Os responsáveis pelo tratamento de dados devem ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados. Este 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 noutro fundamento jurídico que não seja o consentimento ou um contrato. Por natureza própria, este direito não deverá ser exercido em relação aos responsáveis pelo tratamento de dados no exercício das suas funções públicas. Por conseguinte, não deverá ser aplicável especialmente quando o tratamento de dados pessoais for necessário para o cumprimento de uma obrigação jurídica à qual o responsável esteja sujeito, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que esteja investido o responsável pelo tratamento dos dados. O direito do titular dos dados a transmitir ou receber dados pessoais que lhe digam respeito não implica para os responsáveis pelo tratamento dos dados 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 não deverá prejudicar os direitos de outros titulares de dados nos termos do presente regulamento. Esse direito também não deverá prejudicar o direito dos titulares a obter o apagamento dos dados pessoais nem as restrições a esse direito estabelecidas no presente regulamento e, especialmente, 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 tais dados forem necessários para a execução do referido contrato. Sempre que seja tecnicamente possível, o titular dos dados deverá ter o direito de obter que os dados sejam transmitidos diretamente entre os responsáveis pelo tratamento de dados.

(56) 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 dos dados ou ainda por motivos de interesse legítimo do responsável pelo tratamento dos dados ou de terceiros, o titular não deverá deixar de ter o direito de se opor ao tratamento dos dados que digam respeito à sua situação específica. Deverá caber ao responsável pelo tratamento dos dados provar que os seus interesses legítimos imperiosos prevalecem sobre os interesses ou direitos e liberdades fundamentais do titular dos dados.

(57) 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. Este direito é explicitamente levado à atenção do titular e será apresentado de modo claro e distinto de quaisquer outras informações.

(58) O titular deverá ter o direito de não ficar sujeito a uma decisão, que poderá compreender uma medida, que avalie aspetos pessoais que lhe digam respeito e que se baseie exclusivamente no tratamento automatizado, com efeitos legais que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito em linha ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui também 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 seu desempenho profissional, a sua situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações, que tenha efeitos legais que lhe digam respeito ou a 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 dos dados, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da UE ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento dos dados, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento dos dados, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, incluindo a informação específica do titular dos dados, o direito de obter a intervenção humana e que essa medida não diga respeito a uma criança, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e o direito de contestar a decisão. Para 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 dos dados deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem incorreções nos dados são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de forma 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, opiniões políticas, religião ou convicções, filiação sindical, 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.

(58-A) A definição de perfis enquanto tal 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 deverá ter a possibilidade de emitir orientações neste âmbito.

(59) Podem ser impostas pelo direito da União ou dos Estados-Membros restrições a princípios específicos e aos direitos de informação, acesso, retificação, apagamento ou 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 impostas aos responsáveis pelo tratamento dos dados, desde que 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 efeitos de prevenção, investigação e repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública ou , ou de violação da deontologia de profissões regulamentadas para efeitos de outros interesses públicos, incluindo 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 os requisitos estabelecidos na Carta dos Direitos Fundamentais da União Europeia e na Convenção Europeia para a Proteção dos Direitos do Homem e das Liberdades Fundamentais.

(60) Deverá ser estabelecida a responsabilidade do responsável por qualquer tratamento de dados pessoais realizado por este ou por sua conta. Em especial, o responsável pelo tratamento dos dados 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. Tais 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 individuais.

(60-A) Estes riscos, 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 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 protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza económica ou social; ou quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou 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 e infrações penais 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 vulneráveis, em particular crianças; quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

(60-B) A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada em função da natureza, âmbito, contexto e finalidades do tratamento desses dados. Os riscos deverão ser avaliados de forma objetiva, de modo a determinar se é provável que as operações de tratamento de dados impliquem um risco ou mesmo um risco elevado.

(60-C) As orientações para a execução de medidas adequadas e a comprovação de conformidade pelos responsáveis pelo tratamento dos dados 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 concretamente recorrendo a códigos de conduta aprovados, a certificações aprovadas, às orientações do Comité Europeu para a Proteção de Dados ou às indicações fornecidas por um encarregado da proteção de dados. O Comité Europeu para a Proteção de Dados poderá emitir igualmente orientações sobre operações de tratamento de dados que não sejam suscetíveis de resultar num elevado risco para os direitos e liberdades individuais e indicar quais as medidas adequadas em tais casos para diminuir esse risco.

(61) A proteção dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige que sejam adotadas 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 dos dados 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 dos dados 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 dos dados 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.

(62) A proteção dos direitos e liberdades dos titulares dos dados, bem como a responsabilidade dos responsáveis pelo seu tratamento e dos subcontratantes, inclusive 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 dos dados 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 de dados.

(63) Sempre que um responsável pelo tratamento dos dados ou subcontratante não estabelecidos na União efetuem o tratamento de dados pessoais de titulares que se encontrem na União, e cujas atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a essas pessoas na União, independentemente de ser ou não exigido o pagamento do titular de dados, ou com o controlo do seu comportamento desde que o seu comportamento tenha lugar na União, o responsável pelo tratamento dos dados 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, conforme referido no artigo 9.º, n.º 1 nem o tratamento de dados relativos a condenações e infrações penais referidas no artigo 9.º-A, e não seja suscetível de implicar riscos para os direitos e liberdades individuais, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento, ou se o responsável pelo tratamento dos dados for uma autoridade ou organismo público. O representante deverá agir por conta do responsável pelo tratamento dos dados ou subcontratante e deverá poder ser contactado por qualquer autoridade de controlo. O representante deverá ser explicitamente designado por um mandato do responsável pelo tratamento dos dados 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, nos termos do presente regulamento, incumbem ao responsável pelo tratamento dos dados ou ao subcontratante. O representante deverá executar as suas tarefas em consonância com o mandato que recebeu do responsável pelo tratamento dos dados, nomeadamente no respeitante 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 ser sujeito a medidas de execução no caso de não cumprimento por parte do responsável pelo tratamento dos dados.

(63-A) Para assegurar o cumprimento do presente regulamento no que se refere ao tratamento a efetuar pelo subcontratante por conta do responsável pelo tratamento dos dados, 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 ou mecanismo de certificação aprovado poderá ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento dos dados. A realização de operações de tratamento de dados em subcontratação é regulada por um contrato ou por outro ato jurídico ao abrigo do direito da União, dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento dos dados 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 que podem correr os direitos e liberdades do titular dos dados. O responsável pelo tratamento dos dados 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 mecanismo de controlo da coerência e adotadas depois pela Comissão. Depois de concluído o tratamento por conta do responsável pelo tratamento dos dados, o subcontratante deverá, consoante a escolha do primeiro, devolver ou apagar os dados pessoais, a menos que seja exigida a conservação dos dados ao abrigo do direito da União ou do Estado-Membro a que o subcontratante está sujeito.

(64) (...)

(65) A fim de comprovar a observância do presente regulamento, o responsável pelo tratamento dos dados ou o subcontratante deverá conservar registos 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 seu pedido, para fiscalização dessas operações de tratamento.

(66) A fim de preservar a segurança e evitar o tratamento em violação do presente regulamento, o responsável pelo tratamento dos dados, ou o subcontratante, deverá avaliar os riscos que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Estas 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, 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 morais.

(66-A) Com o objetivo 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 dos titulares dos dados, 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 devem 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 dos dados 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.

(67) Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou morais aos interessados, como a perda de controlo sobre os 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 protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social. Por conseguinte, logo que o responsável pelo tratamento dos dados tenha conhecimento de uma violação de dados pessoais, deverá comunicá-la à autoridade de controlo competente sem demora injustificada e, se possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que o responsável pelo tratamento dos dados seja capaz de demonstrar, em conformidade com o princípio da responsabilidade, que a violação dos dados pessoais não é suscetível de implicar um risco para os direitos e liberdades individuais. Se não for possível efetuar a comunicação no prazo de 72 horas, a notificação deverá ser acompanhada de uma exposição dos motivos da demora, podendo as informações ser fornecidas por fases sem mais demora injustificada.

(67-A novo) Se a violação de dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades individuais, os interessados deverão ser notificados sem demora injustificada, a fim de permitir que tomem as precauções necessárias. A notificação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações ao titular dos dados para atenuar potenciais efeitos adversos. Os titulares dos dados deverão ser notificados o mais rapidamente possível, em estreita cooperação com a autoridade de controlo, e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes (por exemplo, autoridades de polícia). Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá que se envie uma notificação rápida aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra violações de dados recorrentes ou similares poderá justificar um prazo mais alargado.

(68) 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.

(68-A) (...)

(69) 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 da 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.

(70) 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. Por essa razão, tais obrigações gerais e indiscriminadas de notificação deverão ser suprimidas e substituídas por procedimentos e mecanismos eficazes mais centrados nos tipos de operações de tratamento suscetíveis de resultar num elevado risco para os direitos e liberdades individuais, devido à sua natureza, âmbito, contexto e finalidades. As referidas operações de tratamento poderão envolver a utilização de novas tecnologias, pertencer a um novo tipo, não ter sido antecedidas por uma avaliação de impacto sobre a proteção de dados por parte do responsável pelo tratamento dos dados ou ser consideradas necessárias à luz do período decorrido desde o tratamento inicial.

(70-A) Nesses casos, o responsável pelo tratamento dos dados deverá proceder, antes do tratamento, a uma avaliação do impacto sobre a proteção de dados, a fim de avaliar a probabilidade ou gravidade particular do elevado risco, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do risco, devendo ser apreciadas, nomeadamente, as medidas, garantias e mecanismos previstos para atenuar esse risco e para assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.

(71) 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 são tratados para tomar decisões relativas a determinadas pessoas 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 e infrações penais 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 direitos, 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. Nestes casos, a realização de uma avaliação de impacto sobre a proteção de dados não deverá ser obrigatória.

(72) 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 dos dados planearem criar uma aplicação ou um ambiente de tratamento comum em todo um setor ou segmento profissional, ou uma atividade horizontal amplamente utilizada.

(73) No contexto da adoção da legislação nacional que regula o desempenho das funções 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.

(74) Sempre que uma avaliação de impacto relativa à proteção de dados indicar que o tratamento, na falta das garantias e das medidas e mecanismos de segurança previstos para atenuar os riscos, implica um elevado risco para os direitos e liberdades individuais e o responsável pelo tratamento dos dados 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 de dados e da extensão e frequência do tratamento, que podem originar igualmente danos ou interferir com os direitos e liberdades do interessado. 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 deste processo de consulta, o resultado de uma avaliação do impacto sobre a proteção de dados efetuada relativamente ao tratamento em questão nos termos do artigo 33.º pode ser apresentado à autoridade de controlo, em especial as medidas previstas para atenuar o risco para os direitos e liberdades individuais.

(74-A) O subcontratante deverá prestar assistência ao responsável pelo tratamento dos dados, 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.

(74-B) 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.

(75) 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, ou se, no setor privado, for efetuado por um responsável pelo tratamento dos dados cujas atividades principais consistam em operações de tratamento que exijam o controlo regular e sistemático do titular dos dados, o responsável pelo tratamento destes ou o subcontratante pode ser assistido por um especialista em legislação e prática de proteção dados no controlo do cumprimento do presente regulamento a nível interno. No setor privado, as atividades principais do responsável pelo tratamento dos dados 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 dos dados, deverão estar em condições de desempenhar as suas funções e atribuições com independência.

(76) As associações ou outras entidades que representem categorias de responsáveis pelo tratamento de dados 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 dos dados e dos subcontratantes, tendo em conta o risco que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades individuais.

(76-A) 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 de dados 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.

(77) A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de mecanismos de certificação, 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.

(78) A circulação transfronteiras 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 destes fluxos transfronteiras 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 de dados, 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 de dados, 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. Sem prejuízo das demais disposições do presente regulamento, só é possível realizar transferências se as condições constantes do Capítulo V forem cumpridas pelo responsável pelo tratamento dos dados ou subcontratante.

(79) 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 da legislação da UE e prevejam um nível adequado de proteção dos direitos fundamentais dos titulares dos dados.

(80) A Comissão pode decidir, com efeitos no conjunto da União, que determinados países terceiros, um território ou um setor específico de um país terceiro, ou uma 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. Nestes casos, podem realizar-se transferências de dados pessoais para esses países sem que para tal seja necessária mais nenhuma autorização. A Comissão pode igualmente decidir revogar essa decisão, após notificação e apresentação de justificação exaustiva ao país terceiro.

(81) 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 de um 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 relativa a um território ou um setor específico de um 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 um nível adequado de proteção, essencialmente equivalente ao garantido 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 europeias de proteção de dados, e ainda conferir aos titulares dos dados direitos efetivos e oponíveis e vias efetivas de recurso administrativo e judicial.

(81-A) 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 quando avalia o nível de proteção nos países terceiros ou organizações internacionais.

(81-B) 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, incluindo 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 mecanismo de revisão periódica do funcionamento destas. A 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, tal como estabelecido no presente regulamento.

(82) A Comissão pode reconhecer que um país terceiro, território ou 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 constantes dos artigos 42.º a 44.º. 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 de tal proibição e iniciar consultas com o país ou organização em causa, a fim de corrigir a situação.

(83) Na falta de uma decisão sobre o nível de proteção adequado, o responsável pelo tratamento dos dados 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 UE, 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 forem oferecidas garantias em regimes administrativos juridicamente não vinculativos.

(84) A possibilidade de o responsável pelo tratamento dos dados 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 cláusulas num contrato mais abrangente, inclusive num 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 dos dados e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção.

(85) Os grupos empresariais ou os grupos de empresas envolvidas numa atividade económica conjunta deverão poder utilizar as regras vinculativas para empresas aprovadas para as suas transferências internacionais da União para entidades pertencentes ao mesmo grupo empresarial ou grupo de empresas 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.

(86) 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 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.

(87) Estas 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 o direito interno 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 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 e/ou para envidar esforços no sentido do cumprimento do direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por interesses vitais do titular dos dados.

(88) 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 dos dados, 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 dos dados deverá atender especialmente à natureza dos dados, 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 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 estatísticos ou de investigação histórica e científica, deverão ser tidas em consideração as expectativas legítimas da sociedade em matéria de avanço do conhecimento. O responsável pelo tratamento dos dados deverá informar da transferência a autoridade de controlo e o titular dos dados.

(89) 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 dos dados ou o subcontratante deverá adotar soluções que confiram aos titulares dos dados direitos efetivos e oponíveis quanto ao tratamento dos seus dados na União, após a transferência dos mesmos, e lhes garantam que continuarão a beneficiar dos direitos e garantias fundamentais.

(90) Alguns países terceiros aprovam leis, regulamentos e outros instrumentos legislativos destinados a regular diretamente as atividades de tratamento de dados 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 de dados 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 instrumentos legislativos 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 pelo direito do Estado-Membro ao qual o responsável pelo tratamento dos dados está sujeito.

(91) Sempre que os dados pessoais atravessam fronteiras fora do território da União, há um risco acrescido de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem 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 transfronteiro 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 mecanismos 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 no cumprimento das disposições do presente regulamento, incluindo as constantes do Capítulo V.

(92) 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 diz respeito ao tratamento dos seus dados pessoais. Os Estados-Membros podem criar várias autoridades de controlo de modo a refletir a sua estrutura constitucional, organizacional e administrativa.

(92-A) A independência das autoridades de controlo não deverá implicar que estas autoridades não possam ser sujeitas a mecanismos de controlo ou monitorização no que diz respeito às suas despesas. Não implica tão pouco que as autoridades de controlo não possam ser sujeitas a revisão judicial.

(93) Os Estados-Membros que criem várias autoridades de controlo deverão prever na sua legislação mecanismos que garantam a participação efetiva dessas mesmas autoridades no mecanismo 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 mecanismo, a fim de assegurar uma cooperação rápida e fácil com outras autoridades de controlo, com o Comité Europeu para a Proteção de Dados e com a Comissão.

(94) Deverão ser dados às autoridades de controlo os recursos financeiros e humanos, as instalações e as infraestruturas necessárias ao desempenho eficaz das suas funções, 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 estatal ou nacional.

(95) 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 por procedimento transparente pelo Parlamento, e/ou 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 autoridade de controlo deverá dispor do seu próprio pessoal, selecionado por si mesma ou por um organismo independente instituído nos termos da legislação dos Estados-Membros e exclusivamente sujeito à orientação do membro ou membros da autoridade de controlo.

(95-A) 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 dos dados 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 Europeia 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 regulamento e a promoção da sensibilização do público para os riscos, regras, garantias e direitos associados ao tratamento de dados pessoais.

(96) 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.

(97) Quando o tratamento de dados pessoais ocorra no contexto das atividades de um estabelecimento de um responsável pelo tratamento dos dados ou de um subcontratante na União e o responsável pelo tratamento dos dados 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 dos dados 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 dos dados 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 dos dados 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 Europeu para a Proteção de Dados pode 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.

(97-A) 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 disposto no 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.

(97-B) 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 dos dados ou do subcontratante e ser vinculativas para ambos. O responsável pelo tratamento dos dados 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 dos dados ou do subcontratante no que diz respeito às atividades de tratamento de dados na União.

(97-C) 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 dos dados 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 relativos a 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 se ocupa da matéria no âmbito do mecanismo de balcão único previsto no artigo 54.º-A ou se deverá ser a autoridade de controlo que a informou a ocupar-se da matéria a nível local. Ao decidir se se ocupa da matéria, a autoridade de controlo principal deverá ter em conta se há algum estabelecimento do responsável pelo tratamento dos dados 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 dos dados ou subcontratante. Quando a autoridade de controlo principal decide ocupar-se da matéria, 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 do mecanismo de balcão único previsto no artigo 54.º-A.

(98) As regras relativas à autoridade de controlo principal e ao mecanismo de balcão único previsto no artigo 54.º-A 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.

(99) (...)

(100) 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, particularmente em caso de reclamação apresentada por pessoas individuais, sem prejuízo dos poderes das autoridades competentes para o exercício da ação penal nos termos da legislação nacional, tendo em vista levar as violações ao presente regulamento ao conhecimento das autoridades judiciais e/ou intervir em processos judiciais. Essas competências deverão incluir o poder de impor uma limitação temporário ou definitiva ao tratamento dos dados, 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 no direito nacional, com imparcialidade e 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 nacional, 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 nacional. A adoção de tais decisões juridicamente vinculativas pode dar origem a revisões judiciais nos tribunais dos Estados-Membros das autoridades de controlo que tenham adotado as decisões.

(101) (...)

(101-A) 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 multas administrativas, 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.

(101-B) 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 dos dados 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 ao 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, ou ao tratamento realizado 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 que tenham de ser analisadas tomando em consideração as obrigações legais aplicáveis ao abrigo do direito nacional.

(102) As atividades de sensibilização das autoridades de controlo dirigidas ao público deverão incluir medidas específicas a favor dos responsáveis pelo tratamento dos dados e subcontratantes, incluindo as micro, pequenas e médias empresas, bem como os titulares individuais, em particular num contexto educacional.

(103) 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 da autoridade de controlo requerida no prazo de um mês a contar da receção do pedido.

(104) Nos casos em que se justifique, as autoridades de controlo deverão participar em operações conjuntas entre autoridades de controlo. A autoridade de controlo requerida deverá ser obrigada a responder ao pedido dentro de um determinado prazo.

(105) A fim de assegurar a aplicação coerente do presente regulamento em toda a União, deverá ser criado um mecanismo de controlo da coerência e para a cooperação entre as autoridades de controlo. Este mecanismo 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 mecanismo de controlo da coerência. Este mecanismo não deverá prejudicar medidas que a Comissão possa tomar no exercício das suas competências nos termos dos Tratados.

(106) Em aplicação do mecanismo de controlo da coerência, o Comité Europeu para a Proteção de Dados deverá emitir um parecer, dentro de um determinado prazo, 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 Europeu para a Proteção de Dados 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 juridicamente vinculativas em casos claramente definidos em que as autoridades de controlo tenham posições contraditórias, em especial no âmbito do mecanismo de cooperação entre a autoridade de controlo principal e as autoridades de controlo interessadas, a respeito da questão de fundo, designadamente se há ou não violação do presente regulamento.

(107) (...)

(108) 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 poderá adotar no seu território medidas provisórias devidamente justificadas, válidas por um período determinado que não deverá exceder os três meses.

(109) A aplicação deste mecanismo 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 mecanismo 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 mecanismo de controlo da coerência.

(110) A fim de promover a aplicação coerente do presente regulamento, o Comité Europeu para a Proteção de Dados deverá ser criado como um órgão independente da União. Para atingir os seus objetivos, o Comité Europeu para a Proteção de Dados deverá ser dotado de personalidade jurídica. O Comité Europeu para a Proteção de Dados 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 por um diretor da autoridade de controlo de cada Estado-Membro e da Autoridade Europeia para a Proteção de Dados ou pelos seus representantes. A Comissão e a Autoridade Europeia para a Proteção de Dados deverão participar nas suas atividades, a primeira sem direito de voto e a segunda sem direito de voto em casos particulares. O Comité Europeu para a Proteção de Dados deverá contribuir para a aplicação coerente do presente regulamento em toda a União, nomeadamente no aconselhamento da Comissão, em especial no que respeita ao nível de proteção em países terceiros ou em organizações internacionais, e na promoção da cooperação das autoridades de controlo em toda a União. O Comité Europeu para a Proteção de Dados deverá ser independente no exercício das suas funções.

(110-A) O Comité Europeu para a Proteção de Dados 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 Europeu para a Proteção de Dados pelo presente regulamento deverá atuar sob a direção exclusiva do presidente deste Comité, sendo responsável perante o mesmo.

(111) Os titulares dos dados deverão ter direito a apresentar reclamação a uma autoridade de controlo única, particularmente no Estado-Membro da sua residência habitual, e ter direito a intentar ação judicial, nos termos do artigo 47.º da Carta dos Direitos Fundamentais, se considerarem que os direitos que lhes são conferidos pelo presente regulamento foram violados ou se 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 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.

(112) Se o titular dos dados considerar que os direitos que lhe são conferidos pelo presente regulamento foram violados, deverá ter o direito de mandatar um organismo, organização ou associação sem fins lucrativos cujos objetivos estatutários sejam de interesse público, exerça a sua atividade no domínio da proteção dos dados pessoais e seja constituída ao abrigo do direito de um Estado-Membro, 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 exercer o direito à indemnização em nome dos titulares do dados, se tal possibilidade estiver prevista na legislação dos Estados-Membros. Os Estados-Membros podem prever que tal organismo, organização ou associação tenha, independentemente do mandato do titular dos dados, o direito de apresentar, no Estado-Membro em causa, uma reclamação e/ou 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 não cumprir o disposto no presente regulamento. O organismo, organização ou associação em causa pode não ser autorizada a pedir uma indemnização em nome do titular dos dados, independentemente do mandato que lhe é conferido por este.

(113) Todas as pessoas singulares ou coletivas têm o direito de interpor recurso de anulação das decisões do Comité Europeu para a Proteção de Dados para o Tribunal de Justiça da União Europeia ("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 podem 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 Europeu para a Proteção de Dados disserem direta e individualmente respeito a um responsável pelo tratamento dos dados, 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 Europeu para a Proteção de Dados, 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 intentar ação judicial perante os tribunais nacionais competentes contra as decisões das autoridades de controlo que produzam efeitos jurídicos que lhes digam respeito. Tais decisões pendem-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 intentadas nos tribunais do Estado-Membro em cujo território as referidas autoridades se encontrem estabelecidas e obedecer às disposições processuais nacionais desse mesmo 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 Europeu para a Proteção de Dados 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, sempre que considera a decisão inválida. No entanto, o tribunal nacional não pode reenviar a questão da validade da decisão do Comité Europeu para a Proteção de Dados 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.

(113-A) 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 interposta 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 interposta 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 para evitar soluções que poderiam ser inconciliáveis se as causas fossem julgadas separadamente.

(114) (...)

(115) (...)

(116) No que diz respeito a ações intentadas contra o responsável pelo tratamento dos dados 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 dos dados for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.

(117) (...)

(118) Qualquer dano de que alguém possa ser vítima em virtude de um tratamento que viole o disposto no presente regulamento deverá ser reparado pelo responsável pelo tratamento dos dados, ou pelo subcontratante, que no entanto pode ser exonerado da sua 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 da União Europeia, 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. Quando se faça referência a tratamentos que violem o disposto no presente regulamento, ficam igualmente abrangidos os que violem os atos delegados e de execução adotados nos termos do presente regulamento e da legislação nacional 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 de dados 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 a legislação nacional, a indemnização poderá ser repartida em função da responsabilidade que caiba a cada responsável pelo tratamento dos dados 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 dos dados ou subcontratante que tenha pago uma indemnização integral, pode posteriormente interpor uma ação de regresso contra outros responsáveis pelo tratamento de dados ou subcontratantes envolvidos no mesmo tratamento.

(118-A) 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 dos dados 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.

(118-B) Com o objetivo de reforçar a execução das normas constantes do presente regulamento, deverão ser impostas sanções e multas administrativas por infração a essas mesmas normas, 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 multa suscetível de ser imposta constituir um encargo desproporcionado para uma pessoa singular, pode ser feita uma repreensão em vez de ser aplicada uma multa. 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 dos dados ou subcontratante, a aceitação de um determinado código de conduta ou quaisquer outros fatores agravantes ou atenuantes. A imposição de sanções e multas administrativas deverá estar sujeita às garantias processuais adequadas em conformidade com os princípios gerais do direito da União e a Carta dos Direitos Fundamentais, incluindo a proteção jurídica eficaz e um processo equitativo.

(119) Os Estados-Membros podem 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 da União Europeia.

(120) A fim de reforçar e harmonizar as sanções administrativas aplicáveis em caso de infração ao presente regulamento, as autoridades de controlo deverão ter competência para impor multas administrativas. O presente regulamento deverá definir as infrações, o montante máximo e o critério de fixação do valor das multas administrativas 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 regulamento e para prevenir ou atenuar as consequências da infração. Sempre que forem impostas multas a empresas, estas deverão ser entendidas para esse efeito como empresas nos termos dos artigos 101.º e 102.º do TFUE. Sempre que forem impostas multas 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 multa. O mecanismo de controlo da coerência pode ser utilizado igualmente para a promoção de uma aplicação coerente das multas administrativas. Deverá caber aos Estados-Membros determinar se as autoridades públicas deverão estar sujeitas a multas administrativas, e em que medida. A imposição de uma multa administrativa 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 regulamento.

(120-A) (novo) Os sistemas jurídicos da Dinamarca e da Estónia não conhecem as multas administrativas tal como são previstas no presente regulamento. As regras relativas às multas administrativas podem ser aplicadas de modo que a multa 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 multas administrativas 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 multa. Em todo o caso, as multas impostas deverão ser efetivas, proporcionadas e dissuasivas.

(120-A) Sempre que o presente regulamento não harmonize sanções administrativas, ou se necessário noutros casos, por exemplo, em caso de infrações graves às disposições do 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 pela legislação nacional.

(121) 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 garantido pelo artigo 11.º da Carta dos Direitos Fundamentais da União Europeia. 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. Tais isenções e derrogações devem ser adotadas pelos Estados-Membros em relação aos princípios gerais, aos direitos do titular dos dados, ao responsável pelo tratamento destes e ao subcontratante, à transferência de dados 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 a legislação nacional do Estado-Membro a que esteja sujeito o responsável pelo tratamento dos dados. 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.

(121-A) O presente regulamento permite tomar em consideração o princípio do direito de acesso do público aos documentos oficiais aquando da aplicação das disposições nele estabelecidas. O acesso do público aos documentos oficiais pode ser considerado de interesse público. Os dados pessoais que constem de documentos na posse de 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, neste contexto, todas as autoridades ou outros organismos abrangidos pelo direito do Estado-Membro relativo ao acesso do público aos documentos. A Diretiva 2033/98/CE do Parlamento Europeu e do Conselho, de 17 de novembro de 2003, relativa à reutilização de informações do setor público não modifica nem de modo algum afeta o nível de proteção dos indivíduos relativamente ao tratamento de dados pessoais nos termos das disposições do direito da União ou do direito nacional, 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 definida por lei como incompatível com o direito relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

(122) (...)

(123) (...)

(124) A legislação nacional ou as convenções coletivas (incluindo "acordos setoriais") podem prever regras específicas para o tratamento de dados pessoais dos assalariados 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.

(125) O tratamento de dados pessoais para fins de arquivo de interesse público ou para fins estatísticos ou de investigação científica e histórica deverá ficar sujeito à salvaguarda adequada dos direitos e liberdades do titular dos dados nos termos do presente regulamento. Desse modo devem ficar asseguradas medidas técnicas e organizativas que garantam, em particular, o princípio da minimização dos dados. O tratamento posterior de dados pessoais para fins de arquivo de interesse público ou para fins estatísticos ou de investigação científica e histórica deverá ser efetuado depois de o responsável pelo tratamento dos dados ter avaliado a possibilidade de tais fins serem alcançados por um tipo de tratamento de dados 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). Os Estados-Membros deverão prever salvaguardas adequadas para o tratamento dos dados pessoais para fins de arquivo de interesse público ou para efeitos estatísticos ou de investigação científica e histórica. Os Estados-Membros deverão ser autorizados a estabelecer, em situações específicas e mediante garantias adequadas para o titular dos dados, especificações e derrogações dos requisitos de informação, retificação, apagamento, do direito a ser esquecido, à limitação do tratamento dos dados e à portabilidade dos dados e do direito de oposição aquando do tratamento de dados pessoais para fins de arquivo de interesse público ou para fins estatísticos ou de investigação científica e histórica. 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.

(125-A) (...)

(125-AA) Combinando informações provenientes dos registos, os investigadores podem obter novos conhecimentos de grande valor quando se trate por exemplo de doenças generalizadas como as doenças cardiovasculares, o cancro, a depressão, etc. 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 o impacto a longo prazo de uma série de condições sociais, tais como o desemprego e o ensino, e a combinação dessas informações com outras condições de vida. Os resultados da investigação com base em 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, etc. 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 dos Estados-Membros ou da União.

(125-B) 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 estipular que os dados pessoais possam ser objeto de posterior tratamento 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 ou Holocausto, ou crimes de guerra.

(126) 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 e deverá, além disso, ter em conta o objetivo da União mencionado no artigo 179.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia, 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.

(126-A) Quando os dados pessoais sejam tratados para fins históricos, 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.

(126-B) 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.

(126-C) 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 garantir o segredo estatístico. Por fins estatísticos deverão entender-se todas as operações de recolha e de tratamento de dados pessoais necessárias à realização de estudos estatísticos ou à produção de resultados estatísticos. Tais 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 não sejam utilizados para justificar medidas ou decisões tomadas a respeito de alguém.

(126-D) 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 Tratado sobre o Funcionamento da União Europeia, devendo as estatísticas nacionais cumprir também o disposto no direito nacional. O 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 fornece especificações suplementares em matéria de segredo estatístico aplicável às estatísticas europeias.

(127) No que se refere aos poderes das autoridades de controlo para obter, junto do responsável pelo tratamento dos dados 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.

(128) 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 Tratado sobre o Funcionamento da União Europeia.

(129) Por forma a cumprir os objetivos do presente regulamento, nomeadamente defender os direitos e liberdades fundamentais das pessoas singulares e, em especial, o seu direito à proteção dos dados pessoais, e assegurar a livre circulação desses dados na União, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia deverá ser delegado na Comissão. Em especial, deverão ser adotados atos delegados em relação aos critérios e requisitos aplicáveis aos mecanismos de certificação, às informações a fornecer por meio de ícones normalizados e aos procedimentos aplicáveis ao fornecimentos 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.

(130) Por forma a assegurar condições uniformes para a execução do presente regulamento, deverão ser conferidas 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 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 Comissão5. Neste contexto, a Comissão deverá prever medidas específicas para as micro, pequenas e médias empresas.

(131) Deverá ser utilizado o procedimento de exame para a adoção de atos de execução em matéria de cláusulas contratuais-tipo entre os responsáveis pelo tratamento dos dados e os subcontratantes e entre subcontratantes, normas técnicas e mecanismos de certificação, nível de proteção adequado conferido por um país terceiro, um território ou por um setor de tratamento de dados desse país terceiro ou por uma organização internacional, formatos e procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento dos dados, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas, assistência mútua, modalidades de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité Europeu para a Proteção de Dados, dado que o âmbito de aplicação destes atos é geral.

(132) A Comissão deverá adotar atos de execução imediatamente aplicáveis quando haja elementos que comprovem que determinado país terceiro, território ou setor de tratamento de dados desse país terceiro, ou uma organização internacional não assegura um nível de proteção adequado e imperativos urgentes assim o exigirem.

---

5 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).

(133) Atendendo a que os objetivos do presente regulamento, a saber, assegurar um nível equivalente de proteção das pessoas singulares e a livre circulação de dados na União, não podem ser suficientemente realizados pelos Estados-Membros e podem, pois, devido à dimensão e aos efeitos da ação, ser mais bem realizados a nível da União, esta última pode adotar 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, o presente regulamento não excede o necessário para atingir esse objetivo.

(134) 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 estiverem cumpridas as condições previstas no presente regulamento, para que o responsável pelo tratamento dos dados 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.

(135) 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, incluindo as obrigações que incumbem ao responsável pelo tratamento dos dados 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 entre estes dois atos jurídicos.

(136) (...)

(137) (...)

(138) (...)

(139) (...)

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 e, em especial, o seu direito à proteção dos dados pessoais.

2-A. (...)

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) (...)

   c) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do Título V, Capítulo 2, do Tratado da União Europeia;

   d) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;

e) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais, execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública.

2-A. 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 instrumentos jurídicos da União aplicáveis ao tratamento de dados pessoais, são adaptados aos princípios e regras do presente regulamento nos termos previstos no artigo 90.º-A.

3. 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 dos dados 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 dos dados 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 Europeia.

3. O presente regulamento aplica-se ao tratamento de dados pessoais por um responsável pelo tratamento de dados estabelecido não na União, mas num lugar em que se aplique o direito nacional 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", toda a informação relativa a uma pessoa singular identificada ou identificável ('titular dos dados'); é considerada identificável a pessoa 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 a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa.

2) (...)

3) "Tratamento", qualquer operação ou conjunto de operações efetuadas sobre dados pessoais ou conjuntos de dados pessoais, 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 divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

3-A) "Limitação do tratamento", a inserção de uma marca nos dados pessoais conservados com o objetivo de limitar o seu tratamento no futuro;

3-AA) "Definição de perfis", qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados para avaliar certos aspetos pessoais de uma pessoa singular, em especial para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;

3-B) "Pseudonimização", o tratamento de dados pessoais de forma a que já não possam ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, enquanto essas informações suplementares forem mantidas separadamente e sujeitas a medidas técnicas e organizativas para garantir essa não atribuição a uma pessoa identificada ou identificável;

4) "Ficheiro", qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico;

5) "Responsável pelo tratamento", a pessoa singular ou coletiva, a autoridade pública, a agência ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios de tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento dos dados ou os critérios específicos aplicáveis à sua nomeação podem ser indicados pelo direito da União ou de um Estado-Membro;

6) "Subcontratante", a pessoa singular ou coletiva, a autoridade pública, agência ou qualquer outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

7) "Destinatário", a pessoa singular ou coletiva, a autoridade pública, agência ou qualquer outro organismo que receba comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Todavia, não são consideradas destinatários as autoridades públicas suscetíveis de receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros; o tratamento destes dados pelas referidas autoridades públicas deve estar em conformidade com as regras de proteção de dados aplicáveis de acordo com as finalidades do tratamento.

7-A) "Terceiro", a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não seja o titular dos dados, o responsável pelo tratamento dos dados, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento dos dados ou do subcontratante, estão autorizadas a tratar os dados;

8) "Consentimento do titular dos dados", qualquer manifestação de vontade, livre, específica, informada e explícita, pela qual a pessoa em causa aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento;

9) "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;

10) "Dados genéticos", todos os dados pessoais relacionados com as características genéticas de uma pessoa, hereditárias ou adquiridas, que deem informações únicas sobre a fisiologia ou a saúde do indivíduo, resultantes designadamente da análise de uma amostra biológica proveniente da pessoa em causa;

11) "Dados biométricos", quaisquer dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa que permitam ou confirmem a identificação única dessa pessoa, nomeadamente imagens faciais ou dados dactiloscópicos;

12) "Dados relativos à saúde", dados pessoais relacionados com a saúde física ou mental de uma pessoa, inclusive com a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;

12-A) (...)

13) "Estabelecimento principal",

a) no que se refere a um responsável pelo tratamento dos dados 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 e, 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;

14) "Representante", a pessoa singular ou coletiva estabelecida na União que, designada por escrito pelo responsável pelo tratamento dos dados ou subcontratante, nos termos do artigo 25.º, representa o responsável pelo tratamento dos dados ou o subcontratante no que se refere às suas obrigações respetivas nos termos do presente regulamento;

15) "Empresa", qualquer 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;

16) "Grupo empresarial", um grupo composto pela empresa que exerce o controlo e pelas empresas controladas;

17) "Regras vinculativas para as empresas", as regras internas de proteção de dados pessoais aplicadas por um responsável pelo tratamento dos dados ou um subcontratante estabelecido no território de um Estado-Membro da União 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;

18) (...)

19) "Autoridade de controlo", uma autoridade pública independente instituída por um Estado-Membro nos termos do artigo 46.º;

19-A) "Autoridade de controlo interessada", uma autoridade de controlo afetada pelo tratamento pelo facto de:

a) o responsável pelo tratamento dos dados ou o subcontratante estar estabelecido no território do Estado-Membro dessa mesma autoridade de controlo;

b) os titulares de dados que residem nesse Estado-Membro serem substancialmente afetados, ou suscetíveis de o ser, pelo tratamento dos dados;

c) ter sido apresentada uma reclamação junto dessa autoridade de controlo.

19-B) "Tratamento transfronteiras de dados pessoais",

a) o tratamento que ocorre no contexto das atividades dos estabelecimentos de um responsável pelo tratamento dos dados ou de um subcontratante em vários Estados-Membros da União, estando o responsável pelo tratamento ou o subcontratante estabelecido em vários Estados-Membros; ou

b) o tratamento que ocorre no contexto das atividades de um único estabelecimento de um responsável pelo tratamento dos dados ou de um subcontratante na União, mas que afeta, ou é suscetível de afetar substancialmente, titulares de dados em vários Estados-Membros.

19-C) "Objeção pertinente e fundamentada",

uma objeção que visa determinar se há ou não violação do presente regulamento ou, consoante o caso, se a ação prevista relativamente ao responsável pelo tratamento dos dados ou ao subcontratante respeita o regulamento. A objeção deve demonstrar 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;

20) "Serviços da sociedade da informação", qualquer serviço definido no artigo 1.º, n.º 2, da Diretiva 98/34/CE do Parlamento Europeu e do Conselho, de 22 de junho de 1998, relativa a um procedimento de informação no domínio das normas e regulamentações técnicas e das regras relativas aos serviços da sociedade da informação;

21) "Organização internacional", uma organização e os organismos por ela tutelados regidos pelo direito internacional público ou outro organismo que seja instituído 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 devem ser:

   a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados ("licitude, lealdade e transparência");

   b) Recolhidos com finalidades determinadas, explícitas e legítimas e não posteriormente tratados de forma incompatível com essas finalidades; o tratamento posterior de dados pessoais para fins de arquivo de interesse público, ou para fins estatísticos ou de investigação científica e histórica, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 83.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 razoáveis para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora ("exatidão");

   e) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; 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 estatísticos ou de investigação científica e histórica, em conformidade com o artigo 83.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");

e-B) 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 acidental, adotando as medidas técnicas ou organizativas adequadas ("integridade e confidencialidade");

e-E) (...)

f) (...)

2. O responsável pelo tratamento dos dados 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 de dados pessoais 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 dos dados 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 dos dados;

f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento dos dados 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. Tal não se aplica ao tratamento de dados efetuado por autoridades públicas no exercício das suas funções.

2. (...)

2-A. (novo) 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 artigo 6.º, 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 previstas no Capítulo IX.

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

a) Pelo direito da União; ou

b) Pela legislação do Estado-Membro à qual o responsável pelo tratamento dos dados 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 dos dados. Este fundamento jurídico pode prever disposições específicas para adaptar a aplicação das regras do presente regulamento, nomeadamente as condições gerais de licitude do tratamento dos dados pelo responsável pelo seu tratamento, o tipo de dados objeto de tratamento, os titulares em questão, as entidades a que os dados 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, inclusive para outras situações específicas de tratamento previstas no Capítulo IX. A legislação da União ou do Estado-Membro deve responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

3-A. Quando o tratamento para fins que não sejam aqueles para os quais os dados 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 nas alíneas a-A) a g) do artigo 21.º, n.º 1, o responsável pelo tratamento dos dados, a fim de verificar se o tratamento para outros fins é compatível com a finalidade para a qual os dados foram inicialmente recolhidos, tem nomeadamente em conta:

a) Qualquer ligação entre a finalidade para a qual os dados 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 relacionados com condenações e infrações penais forem tratados nos termos do artigo 9.º-A;

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.

4. (...)

5. (...)

Artigo 7.º

Condições aplicáveis ao consentimento

1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento dos dados deve poder demonstrar que foi dado o consentimento do titular dos dados para o tratamento dos seus dados pessoais.

1-A. (...)

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 tem de ser apresentado de uma forma que o distinga claramente desses outros assuntos de forma inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa nenhuma parte da declaração relativamente à qual o titular dos dados tenha dado o seu consentimento e 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. Deve ser tão fácil retirar o consentimento como dá-lo.

4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados 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, o tratamento dos dados pessoais de crianças de menos de 16 anos ou, se a legislação de um Estado-Membro o previr, de idade inferior, mas não abaixo dos 13 anos, só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares da responsabilidade parental das crianças.

1-A. Nesses casos, o responsável pelo tratamento dos dados envida todos os esforços razoáveis para verificar que o consentimento foi dado ou autorizado pelo titular da responsabilidade parental da criança, tendo em conta a tecnologia disponível.

2. O disposto no n.º 1 não prejudica 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.

3. (...)

4. (...).

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, a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos destinados a identificar uma pessoa de forma inequívoca ou de dados relativos à saúde ou à vida sexual e orientação sexual.

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; ou

   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 da legislação dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados; ou

   c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento; ou

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 não sejam divulgados a terceiros sem o consentimento dos seus titulares; ou

e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular; ou

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 das suas funções jurisdicionais; ou

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; ou

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 4; ou

h-B) 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; ou

i) Se o tratamento for necessário para fins de arquivo de interesse público, para fins estatísticos ou de investigação científica e histórica, em conformidade com o artigo 83.º, n.º 1, com base no direito da União ou na legislação 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.

j) (...)

3. (...)

4. 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.

5. 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 9.º-A

Tratamento de dados relacionados com condenações e infrações penais

O tratamento de dados pessoais relacionados com condenações e infrações penais ou outras medidas de segurança conexas com base no artigo 6.º, n.º 1, só pode ser 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 podem ser conservados sob o controlo das autoridades públicas.

Artigo 10.º

Tratamento que não permite a 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, em tais casos, o responsável pelo tratamento dos dados 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 18.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 MODALIDADES

Artigo 11.º

Transparência das informações e das comunicações

1. (...)

2. (...)

Artigo 12.º

Transparência das informações, das comunicações e das modalidades para o exercício dos direitos dos titulares dos dados

1. O responsável pelo tratamento dos dados toma as medidas adequadas para fornecer ao titular as informações a que se referem o artigo 14.º e o artigo 14.º-A e qualquer comunicação prevista nos artigos 15.º a 20.º e 32.º a respeito do tratamento de dados pessoais, 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, por via eletrónica sempre que for adequado. Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios.

1-A. O responsável pelo tratamento dos dados facilita o exercício dos direitos do titular dos dados nos termos dos artigos 15.º a 20.º. Nos casos a que se refere o artigo 10.º, n.º 2, o responsável pelo tratamento dos dados 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 20.º, exceto se demonstrar que não está em condições de identificar o titular dos dados.

2. O responsável pelo tratamento dos dados 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, o mais tardar, no prazo de um mês a contar da data de receção do pedido. Este prazo pode ser prorrogado por um máximo de mais dois meses, quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos. Caso haja lugar a prorrogação, o titular dos dados é informado 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 via eletrónica, a informação é, sempre que possível, fornecida por meios eletrónicos, salvo pedido em contrário do titular.

3. Se o responsável pelo tratamento dos dados 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.

4. As informações fornecidas nos termos dos artigos 14.º e 14.º-A e as comunicações e medidas previstas nos artigos 15.º a 20.º e 32.º são fornecidas a título gratuito. Se os pedidos apresentados por um titular de dados forem manifestamente infundados ou excessivos, e particularmente devido ao seu caráter repetitivo, o responsável pelo tratamento dos dados pode exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos pelo fornecimento das informações ou pela comunicação ou adoção da medida solicitada, ou pode recusar-se a dar seguimento ao pedido. Nesses casos, cabe ao responsável pelo tratamento demonstrar o caráter manifestamente infundado ou excessivo do pedido.

4-A. Sem prejuízo do disposto no artigo 10.º, se tiver dúvidas razoáveis quanto à identidade da pessoa que apresenta o pedido a que se referem os artigos 15.º a 19.º, o responsável pelo tratamento dos dados pode solicitar que lhe sejam fornecidas as informações adicionais que forem necessárias para confirmar a identidade do titular dos dados.

4-B. As informações a fornecer pelos titulares dos dados nos termos do artigo 14.º e do artigo 14.º-A podem ser dadas em combinação com ícones normalizados a fim de dar, de 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.

4-C. São atribuídas à Comissão competências para adotar atos delegados em conformidade com o artigo 86.º, a fim de determinar quais as informações a fornecer por meio dos ícones e os procedimentos aplicáveis ao fornecimento de ícones normalizados.

5. (...)

6. (...).

Artigo 13.º

Direitos relativos aos destinatários

(...)

SECÇÃO 2

INFORMAÇÃO E ACESSO AOS DADOS

Artigo 14.º

Informações a facultar quando os dados são recolhidos junto do titular

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

   a) A identidade e os contactos do responsável pelo tratamento dos dados, do seu eventual representante e do encarregado da proteção de dados;

   b) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico do tratamento;

   c) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento dos dados ou de um terceiro;

d) Se os houver, os destinatários ou categorias de destinatários dos dados pessoais;

e) Se for esse o caso, o facto de o responsável pelo tratamento dos dados 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 42.º ou 43.º, ou no artigo 44.º, n.º 1, alínea h), a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;

1-A. Para além das informações referidas no n.º 1, aquando da recolha dos dados pessoais, o responsável pelo tratamento dos dados fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:

a) Período de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse período;

b) ...

c) ...

d) ...

e) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a sua retificação ou apagamento, ou a limitação do tratamento dos dados pessoais referentes ao titular, ou o direito de se opor ao tratamento desses dados e do direito à portabilidade dos dados;

e-A) 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;

f) O direito de apresentar reclamação a uma autoridade de controlo;

g) 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 e as eventuais consequências de não fornecer esses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 20.º, n.ºs 1 e 3, 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.

1-B. Quando o responsável pelo tratamento dos dados tiver a intenção de proceder ao tratamento posterior dos dados 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 1-A.

2. (...)

3. (...)

4. (...)

5. Os n.ºs 1, 1-A e 1-B não se aplicam quando e na medida em que o titular dos dados já tiver conhecimento das informações.

6. (...)

7. (...)

8. (...).

Artigo 14.º-A

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

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

   a) A identidade e os contactos do responsável pelo tratamento dos dados, do seu eventual representante e do encarregado da proteção de dados;

   b) As finalidades do tratamento a que os dados pessoais se destinam, bem como o fundamento jurídico do tratamento;

   b-A) As categorias dos dados pessoais em questão;

   c) (...)

   d) Se os houver, os destinatários ou categorias de destinatários dos dados pessoais;

   d-A) Se for esse o caso, o facto de o responsável pelo tratamento dos dados tencionar transferir dados pessoais para um país terceiro ou uma organização internacional, e a existência ou não de uma decisão de adequação adotada pela Comissão ou, no caso das transferências mencionadas no artigo 42.º ou artigo 43.º, a referência às garantias apropriadas ou adequadas e aos meios de obter cópia das mesmas, ou onde foram disponibilizadas;

2. Para além das informações referidas no n.º 1, o responsável pelo tratamento dos dados fornece ao titular as seguintes informações, necessárias para lhe garantir um tratamento equitativo e transparente:

   b) Período de conservação dos dados pessoais ou, se não for possível, os critérios usados para definir esse período;

   b-A) Se o tratamento dos dados se basear no artigo 6.º, n.º 1, alínea f), os interesses legítimos do responsável pelo tratamento dos dados ou de um terceiro;

c) (...)

e) A existência do direito de solicitar ao responsável pelo tratamento o acesso aos dados pessoais que lhe digam respeito, e a sua retificação ou apagamento, ou a limitação do tratamento dos dados pessoais referentes ao titular, bem como do direito de se opor ao tratamento desses dados e do direito à portabilidade dos dados;

e-A) 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;

f) O direito de apresentar reclamação a uma autoridade de controlo;

g) A origem dos dados pessoais e, eventualmente, se provêm de fontes acessíveis ao público;

h) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 20.º, n.ºs 1 e 3, 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 dos dados comunica as informações referidas nos n.ºs 1 e 2:

a) Num prazo razoável após a obtenção dos dados, mas o mais tardar no prazo de um mês, tendo em conta as circunstâncias específicas em que estes forem tratados;

b) Se os dados 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;

c) Se estiver prevista a divulgação dos dados a outro destinatário, o mais tardar aquando da primeira divulgação desses dados.

3-A. Quando o responsável pelo tratamento dos dados tiver a intenção de proceder ao tratamento posterior dos dados para um fim que não seja aquele para o qual os dados tenham sido obtidos, 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 a 3-A 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, em particular para o tratamento para fins de arquivo de interesse público, para fins estatísticos ou de investigação científica e histórica, sob reserva das condições e garantias previstas no artigo 83.º, n.º 1, e na medida em que o direito referido no n.º 1 seja suscetível de tornar impossível ou prejudicar gravemente a obtenção dos objetivos inerentes aos fins de arquivo de interesse público, aos fins estatísticos ou de investigação científica e histórica; em tais casos, o responsável pelo tratamento dos dados 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 à qual o responsável pelo tratamento dos dados estiver sujeito, prevendo medidas adequadas para proteger os legítimos interesses do titular;

d) Os dados devam permanecer confidenciais em virtude de uma obrigação de sigilo profissional regulamentada pelo direito da União ou a legislação de um Estado-Membro, inclusive uma obrigação estatutária de confidencialidade.

Artigo 15.º

Direito de acesso do titular dos dados

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

a) As finalidades do tratamento dos dados;

b) As categorias dos dados pessoais em causa;

c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, especialmente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;

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

e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais que lhe digam respeito, ou do direito de se opor ao tratamento desses mesmos dados;

f) O direito de apresentar reclamação a uma autoridade de controlo;

g) Se os dados não tiverem sido recolhidos junto do titular, quaisquer informações disponíveis sobre a origem desses dados;

h) A existência de decisões automatizadas, incluindo a definição de perfis referida no artigo 20.º, n.ºs 1 e 3, 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.

1-A. 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 42.º relativo à transferência de dados.

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

2. (...)

2-A. O direito de obter uma cópia a que se refere o n.º 1-B não deve prejudicar os direitos e as liberdades de terceiros.

3. (...)

4. (...).

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 dos dados a retificação dos dados pessoais inexatos que lhe digam respeito. Tendo em conta as finalidades do tratamento dos dados, o titular tem direito a que sejam completados os dados pessoais incompletos que lhe digam respeito, inclusive 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 dos dados 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 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 de dados pessoais nos termos do artigo 19.º, n.º 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento de dados pessoais nos termos do artigo 19.º, n.º 2;

   d) Os dados foram tratados ilicitamente;

   e) Os dados 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 dos dados esteja sujeito;

   f) Os dados foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8.º, n.º 1.

1-A. (...)

2. (...)

2-A. Quando o responsável pelo tratamento dos dados 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 de que o titular 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 dos dados pessoais se revele necessário:

a) Ao exercício da liberdade de expressão e de informação;

b) Ao cumprimento de uma obrigação jurídica que exija o tratamento de dados pessoais 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 dos dados;

c) Por motivos de interesse público no domínio da saúde pública, nos termos do artigo 9.º, n.º 2, alíneas h) e h-B), bem como do artigo 9.º, n.º 4;

d) Para fins de arquivo de interesse público, para fins estatísticos ou de investigação científica e histórica, nos termos do artigo 83.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 inerentes aos fins de arquivo de interesse público, aos fins estatísticos ou de investigação científica e histórica;

e) Para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

4. (...)
5. (...)
6. (...)
7. (...)
8. (...)
9. (...)

Artigo 17.º-A

Direito à limitação do tratamento dos dados

1. O titular dos dados tem o direito de obter do responsável a limitação do tratamento dos dados pessoais, se:

   a) Contestar a exatidão dos dados, durante um período que permita ao responsável pelo tratamento dos dados verificar a sua exatidão;

   a-B) O tratamento for ilícito e o titular dos dados se opuser ao seu apagamento e solicitar, em contrapartida, a limitação da sua utilização;

   b) O responsável pelo tratamento dos dados 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;

   c) Se tiver oposto ao tratamento dos dados nos termos do artigo 19.º, n.º 1, até se verificar que os motivos legítimos do responsável pelo tratamento prevalecem sobre os do titular.

2. Quando o tratamento dos dados pessoais tiver sido limitado nos termos do n.º 1, estes 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 dos dados nos termos do n.º 1 é informado pelo responsável pelo tratamento dos dados antes de ser anulada a limitação ao referido tratamento.

Artigo 17.º-B

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

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

Artigo 18.º

Direito de portabilidade dos dados

1. (...)

2. 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 dos dados, 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 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-A. (novo) Ao exercer o seu direito de portabilidade dos dados nos termos do n.º 1, o titular dos dados tem o direito de obter que os dados sejam transmitidos diretamente entre os responsáveis pelo tratamento dos dados, sempre que tal seja tecnicamente possível.

2-A. O exercício deste direito aplica-se sem prejuízo do artigo 17.º. O direito a que se refere o n.º 2 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 dos dados.

2-AA. O direito a que se refere o n.º 2 não deve prejudicar os direitos e as liberdades de terceiros.

3. (...)

SECÇÃO 4

DIREITO DE OPOSIÇÃO E DECISÕES INDIVIDUAIS AUTOMATIZADAS

Artigo 19.º

Direito de oposição

1. O titular tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos seus dados pessoais com base no artigo 6.º, n.º 1, alíneas e) ou f), ou no artigo 6.º, n.º 4, incluindo a definição de perfis com base nestas disposições. O responsável pelo tratamento dos dados 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, 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 seu titular 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.

2-A. Sempre que o titular se opuser ao tratamento de dados pessoais para efeitos de comercialização direta, estes deixam de ser tratados para esse fim.

2-B. (novo) 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 e é apresentado de modo claro e distinto de quaisquer outras informações.

2-B. 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.

2-AA. Quando os dados pessoais forem tratados para fins estatísticos ou de investigação científica e histórica, nos termos do artigo 83.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 seus dados pessoais, salvo se o tratamento for necessário para o exercício de funções de interesse público.

3. (...).

Artigo 20.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.

1-A. 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 e um responsável pelo tratamento dos dados; ou

b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento dos dados estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular; ou

c) For baseada no consentimento explícito do titular dos dados.

1-B. Nos casos a que se referem o n.º 1-A, alíneas a) e c), o responsável pelo tratamento dos dados 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.

2. (...)

3. As decisões a que se refere o n.º 1-A 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, alíneas 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.

4. (...)

5. (...)

SECÇÃO 5

Limitações

Artigo 21.º

Limitações

1. A legislação da União ou dos Estados-Membros a que estejam sujeitos o responsável pelo tratamento dos dados ou o seu subcontratante pode limitar por medida legislativa o alcance das obrigações e dos direitos previstos nos artigos 12.º a 20.º, e no artigo 32.º, bem como no artigo 5.º, na medida em que tais disposições correspondam aos direitos e obrigações previstos nos artigos 12.º a 20.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) A segurança do Estado;

a-B) A defesa;

a) A segurança pública;

b) 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;

c) Outros objetivos importantes dos interesses públicos gerais 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;

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

d) A prevenção, investigação, deteção e repressão de violações da deontologia de profissões regulamentadas;

e) 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), a-B), a), b), c) e d);

f) A defesa do titular dos dados ou dos direitos e liberdades de outrem;

g) A execução de ações cíveis.

2. Em especial, qualquer medida legislativa referida no n.º 1 incluirá, 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 dos dados ou às categorias de responsáveis pelo tratamento dos dados;

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; 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 DE DADOS E SUBCONTRATANTE

SECÇÃO 1
OBRIGAÇÕES GERAIS

Artigo 22.º

Responsabilidade do responsável pelo tratamento dos dados

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 individuais, 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 de dados pessoais é realizado em conformidade com o presente regulamento. Essas medidas são revistas e atualizadas consoante as necessidades.

2. (...)

2-A. Quando forem proporcionadas em relação às atividades de tratamento de dados, as medidas referidas no n.º 1 incluem a aplicação de orientações adequadas em matéria de proteção de dados pelo responsável pelo tratamento dos dados.

2-B. O cumprimento de códigos de conduta aprovados nos termos do artigo 38.º ou de um mecanismo de certificação aprovado nos termos do artigo 39.º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações do responsável pelo tratamento.

3. (...)

4. (...)

Artigo 23.º

Proteção de dados desde a conceção e por defeito

1. Tendo em conta as técnicas mais avançadas e os custos da sua aplicação, e atendendo à natureza, âmbito, contexto e finalidades do tratamento dos dados, bem como aos riscos decorrentes do tratamento para os direitos e liberdades individuais, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento dos dados 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 forma a que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.

2. O responsável pelo tratamento dos dados 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; este princípio aplica-se à quantidade de dados recolhidos, à extensão do tratamento, ao seu período de conservação e à sua acessibilidade. Em especial, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.

2-A. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.ºs 1 e 2 um mecanismo de certificação aprovado nos termos do artigo 39.º.

3. (...)

4. (...)

Artigo 24.º

Responsáveis conjuntos pelo tratamento

1. Quando dois ou mais responsáveis pelo tratamento de dados determinem conjuntamente as finalidades e os meios desse tratamento, ambos são considerados responsáveis conjuntos pelo tratamento dos dados. Ambos determinam as respetivas responsabilidades por acordo entre si e de modo transparente, a fim de garantir o cumprimento das obrigações previstas no 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 14.º e 14.º-A, 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. O acordo pode designar um ponto de contacto para os titulares dos dados.

2. Independentemente dos termos do acordo referido no 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 dos dados.

3. O acordo reflete devidamente as funções efetivamente exercidas por cada um dos responsáveis conjuntos pelo tratamento e as relações destes com os titulares dos dados, e a essência do acordo é disponibilizada ao titular dos dados.

Artigo 25.º

Representantes dos responsáveis pelo tratamento dos dados não estabelecidos na União

1. Se for aplicável o artigo 3.º, n.º 2, o responsável pelo tratamento dos dados ou o subcontratante designa por escrito um representante seu na União.

2. Esta obrigação não se aplica:
   a) (...);
   b) As 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 relativos a condenações e infrações penais referido no artigo 9.º-A, e não seja suscetível de implicar riscos para os direitos e liberdades individuais, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento;

c) Às autoridades ou organismos públicos;

d) (...)

3. O representante deve estar estabelecido num dos Estados-Membros onde se encontram os titulares dos dados pessoais que são objeto do tratamento no contexto da oferta que lhes é feita de bens ou serviços, ou cujo comportamento é controlado.

3-A. Para efeitos do cumprimento do presente regulamento, o representante é mandatado pelo responsável pelo tratamento dos dados ou pelo subcontratante para ser contactado em complemento ou em substituição do responsável pelo tratamento dos dados ou do subcontratante, em especial por autoridades de controlo e por titulares, relativamente a todas as questões relacionadas com o tratamento de dados pessoais.

4. A designação de um representante pelo responsável pelo tratamento dos dados ou pelo subcontratante não prejudica as ações judiciais que possam vir a ser intentadas contra o próprio responsável pelo tratamento dos dados ou o subcontratante.

Artigo 26.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 modo a que o tratamento satisfaça os requisitos estabelecidos no presente regulamento e garanta a defesa dos direitos do titular dos dados.

1-A. O subcontratante não recorre a outro subcontratante sem que o responsável pelo tratamento dos dados tenha dado, previamente e por escrito, o seu consentimento específico ou geral. Neste último caso, o subcontratante informa sempre o responsável pelo tratamento dos dados 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.

2. A realização de operações de tratamento de dados em subcontratação é regulada por contrato ou outro ato jurídico previsto no direito da União ou dos Estados-Membros, que vincule o subcontratante ao responsável pelo tratamento, estabeleça o objeto e a duração do tratamento, a sua natureza e finalidade do tratamento, o tipo de dados pessoais e as categorias dos titulares dos dados, as obrigações e os direitos do responsável pelo tratamento, e em que se preveja, designadamente, que o subcontratante:

a) Trata os dados pessoais apenas mediante instruções documentadas do responsável pelo tratamento dos dados, 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 dos dados desse requisito jurídico antes de tratar os dados, salvo se a lei proibir tal informação por motivos importantes de interesse público;

b) Garante que as pessoas autorizadas a tratar os dados pessoais assumiram um compromisso de confidencialidade ou se encontram sujeitas às obrigações estatutárias de confidencialidade.

c) Adota todas as medidas exigidas nos termos do artigo 30.º;

d) Respeita as condições a que se referem os n.ºs 1-A e 2-A para recorrer a outro subcontratante;

e) Tendo em conta a natureza do tratamento, e na medida do possível, presta assistência ao responsável pelo tratamento dos dados 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 dos dados no sentido de garantir o cumprimento das obrigações previstas nos artigos 30.º a 34.º, tendo em conta a natureza do tratamento e a informação ao dispor do subcontratante;

g) Consoante a escolha do responsável pelo tratamento dos dados, apaga ou devolve-lhe todos os dados pessoais depois, de concluir os serviços de tratamento, apagando as cópias existentes, a menos que seja exigida a sua conservação pelo direito da União ou do Estado-Membro;

h) Disponibiliza ao responsável pelo tratamento dos dados 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 dos dados ou por outro auditor por este mandatado. O subcontratante informa imediatamente o responsável pelo tratamento dos dados se, no seu entender, alguma instrução violar o presente regulamento ou as disposições da União ou dos Estados-Membros em matéria de proteção de dados.

2-A. Se o subcontratante recorrer a 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 jurídico 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 jurídico entre o responsável pelo tratamento dos dados e o subcontratante, referidas no n.º 2, em particular a obrigação de apresentar garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma a 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 dos dados, pelo cumprimento das obrigações desse outro subcontratante.

2-AA. O facto de o subcontratante cumprir um código de conduta aprovado nos termos do artigo 38.º ou um mecanismo de certificação aprovado nos termos do artigo 39.º pode ser utilizado como elemento para demonstrar as garantias suficientes a que se referem os n.ºs 1 e 2-A.

2-AB. Sem prejuízo de um eventual contrato individual entre o responsável pelo tratamento dos dados e o subcontratante, o contrato ou outro ato jurídico referidos nos n.ºs 2 e 2-A podem ser baseados, totalmente ou em parte, nas cláusulas contratuais-tipo referidas nos n.ºs 2-B e 2-C, inclusivamente quando fazem parte de uma certificação concedida ao responsável pelo tratamento dos dados ou ao subcontratante por força dos artigos 39.º e 39.º-A.

2-B. A Comissão pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos n.ºs 2 e 2-A de acordo com o procedimento de exame referido no artigo 87.º, n.º 2.

2-C. A autoridade de controlo pode estabelecer cláusulas contratuais-tipo para as matérias referidas nos n.ºs 2 e 2-A e de acordo com o mecanismo de controlo da coerência referido no artigo 57.º.

3. O contrato ou outro ato jurídico a que se referem os n.ºs 2 e 2-A devem ser feitos por escrito, incluindo em formato eletrónico.

4. Sem prejuízo do disposto nos artigos 77.º, 79.º e 79.º-B, o subcontratante que, em violação do presente regulamento, determinar as finalidades e os meios de tratamento de dados, é considerado responsável pelo tratamento no que respeita ao tratamento em questão.

5. (...).

Artigo 27.º

Tratamento sob a autoridade do responsável pelo tratamento dos dados e do subcontratante

O subcontratante, bem como qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento dos dados ou do subcontratante, tenha acesso a dados pessoais, só pode efetuar o seu tratamento por instrução do responsável pelo tratamento, a não ser que tal lhe seja exigido pelo direito da União ou dos Estados-Membros.

Artigo 28.º

Registos das atividades de tratamento

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

   a) O nome e os contactos do responsável pelo tratamento dos dados e de qualquer responsável conjunto pelo tratamento dos dados, do representante do responsável pelo tratamento dos dados e do encarregado da proteção de dados, caso exista;

   b) (...)

   c) As finalidades do tratamento dos dados;

d) A descrição das categorias de titulares de dados e das categorias de dados pessoais;

e) As categorias de destinatários a quem os dados pessoais foram ou serão divulgados, incluindo os destinatários estabelecidos em países terceiros;

f) Se for aplicável, as transferências de dados para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 44.º, n.º 1, alínea h), a documentação que comprove a existência das garantias adequadas;

g) Se possível, os prazos previstos para o apagamento das diferentes categorias de dados;

h) Se possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 30.º, n.º 1.

2-A. Cada subcontratante e, caso exista, o representante deste, conserva um registo de todas as categorias de atividades de tratamento de dados pessoais realizadas em nome de um responsável pelo tratamento dos dados, do qual constará:

a) O nome e os contactos do subcontratante ou subcontratantes e de cada responsável pelo tratamento dos dados em nome do qual o subcontratante atua, bem como do representante do responsável pelo tratamento dos dados ou do subcontratante e do encarregado da proteção de dados, caso exista;

b) (...)

c) As categorias de tratamentos de dados efetuados em nome de cada responsável pelo tratamento;

d) Se for aplicável, as transferências de dados para países terceiros ou organizações internacionais, incluindo a identificação desses países terceiros ou organizações internacionais e, no caso das transferências referidas no artigo 44.º, n.º 1, alínea h), a documentação que comprove a existência das garantias adequadas;

e) Se for possível, uma descrição geral das medidas técnicas e organizativas no domínio da segurança referidas no artigo 30.º, n.º 1.

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

3. Quando lhes for solicitado, o responsável pelo tratamento dos dados e o subcontratante, e, caso exista, o representante do responsável pelo tratamento dos dados ou do subcontratante, facultam o registo à autoridade de controlo.

4. As obrigações a que se referem os n.ºs 1 e 2-A não se aplicam às empresas ou organizações com menos de 250 assalariados, 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 o tratamento de dados relativos a condenações e infrações penais referido no artigo 9.º-A.

5. (...)

6. (...).

Artigo 29.º

Cooperação com a autoridade de controlo

1. O responsável pelo tratamento dos dados e o subcontratante e, caso exista, o representante do responsável pelo tratamento dos dados ou do subcontratante, cooperam com a autoridade de controlo no exercício das suas funções, a pedido desta.

2. (...).

SECÇÃO 2
SEGURANÇA DOS DADOS

Artigo 30.º

Segurança do tratamento

1. Tendo em conta as técnicas mais avançadas e os custos da sua aplicação, e atendendo à natureza, âmbito, contexto e finalidades do tratamento dos dados, bem como aos riscos, de probabilidade e gravidade variáveis, que o tratamento representa para os direitos e liberdades individuais, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para garantir um nível de segurança adequado ao risco, nomeadamente, 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 de dados pessoais;

   c) A capacidade de restabelecer a disponibilidade e o acesso aos dados 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.

1-A. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento dos dados, 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.

2. (...)

2-A. O cumprimento de códigos de conduta aprovados nos termos do artigo 38.º ou de um mecanismo de certificação aprovado nos termos do artigo 39.º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no n.º 1.

2-B. O responsável pelo tratamento dos dados e o subcontratante tomam medidas para assegurar que qualquer pessoa que, agindo sob a autoridade do responsável pelo tratamento dos dados ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento dos dados, exceto se tal lhe for exigido pela legislação da União ou de um Estado-Membro.

3. (...)

4. (...).

Artigo 31.º

Notificação da violação de dados pessoais à autoridade de controlo

1. Em caso de violação de dados pessoais, o responsável pelo tratamento dos dados notifica desse facto a autoridade de controlo competente nos termos do artigo 51.º, sem demora injustificada e, sempre que possível, o mais tardar 72 horas após ter tido conhecimento do ocorrido, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades individuais. A notificação à autoridade de controlo é acompanhada de uma justificação fundamentada caso não seja feita no prazo de 72 horas.

1-A. (...)

2. O subcontratante notifica o responsável pelo tratamento dos dados 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 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) (...)

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

e) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento dos dados para reparar a violação de dados pessoais, inclusive, se for caso disso, para atenuar os seus eventuais efeitos negativos;

f) (...)

3-A. Caso, e na medida em que não seja possível fornecer as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.

4. O responsável pelo tratamento dos dados documenta quaisquer violações de dados pessoais, incluindo os factos com elas relacionados, 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.

5. (...)

6. (...)

Artigo 32.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 individuais, o responsável pelo tratamento dos dados comunica a violação de dados pessoais ao titular dos mesmos, sem demora injustificada.

2. A comunicação ao titular dos dados referida no n.º 1descreve numa linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e recomendações previstas no artigo 31.º, n.º 3, alíneas b), d) e e).

3. A comunicação ao titular dos dados a que se refere o n.º 1 não é exigida se:

a) O responsável pelo tratamento dos dados tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados afetados pela violação de dados pessoais, especialmente medidas que tornem os dados incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, como, por exemplo, a cifragem; ou

b) O responsável pelo tratamento dos dados tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares referido no 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 dos dados não tiver já comunicado a violação de dados pessoais ao titular, a autoridade de controlo, tendo considerado a probabilidade de a violação resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontra preenchida qualquer das condições referidas no n.º 3.

5. (...)

6. (...).

SECÇÃO 3

AVALIAÇÃO DE IMPACTO SOBRE A PROTEÇÃO DE DADOS E CONSULTA PRÉVIA

Artigo 33.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 individuais, o responsável pelo tratamento dos dados 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.

1-A. Ao efetuar uma avaliação de impacto sobre a proteção de dados, o responsável pelo tratamento dos dados solicita o parecer do encarregado da proteção de dados, nos casos em que este tenha sido designado.

2. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o n.º 1 é em particular exigida nos seguintes casos:

a) A avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, que é baseada no tratamento automatizado, incluindo a definição de perfis, e com base na qual são adotadas decisões que produzem efeitos jurídicos relativamente à pessoa em causa 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 relacionados com condenações e infrações penais a que se refere o artigo 9.º-A;

c) Um controlo sistemático de zonas acessíveis ao público em grande escala;

d) (...)

e) (...)

2-A. 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 ao abrigo do n.º 1. A autoridade de controlo comunica essas listas ao Comité Europeu para a Proteção de Dados.

2-B. A autoridade de controlo pode também elaborar e tornar pública uma lista dos tipos de operações de tratamento em relação aos quais não é exigida uma análise de impacto sobre a proteção de dados. A autoridade de controlo comunica essas listas ao Comité Europeu para a Proteção de Dados.

2-C. Antes de adotar as listas a que se referem os n.ºs 2-A e 2-B, a autoridade de controlo competente aplica o mecanismo de controlo da coerência referido no artigo 57.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.

3. A avaliação compreende, pelo menos:

a) Uma descrição sistemática das operações de tratamento de dados previstas e a finalidade do tratamento inclusive, se for caso disso, os interesses legítimos do responsável pelo tratamento dos dados;

b) Uma avaliação da necessidade e proporcionalidade das operações de tratamento de dados em relação aos objetivos;

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

d) As medidas previstas para fazer face aos riscos, incluindo as garantias, medidas de segurança e mecanismos 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.

3-A. 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 38.º por parte desses responsáveis ou subcontratantes.

4. Se for adequado, o responsável pelo tratamento dos dados 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.

5. Se o tratamento efetuado ao abrigo do artigo 6.º, n.º 1, alíneas c) ou e), tiver como base jurídica o direito da União ou do Estado-Membro a que o responsável pelo tratamento dos dados está sujeito, e esse direito regular a operação ou 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 dessa base jurídica, não são aplicáveis os n.ºs 1 a 3, salvo se os Estados-Membros considerarem necessário proceder a essa avaliação antes das atividades de tratamento.

6. (...)

7. (...)

8. Se necessário, o responsável pelo tratamento dos dados procede a um controlo para avaliar se o tratamento de dados pessoais 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 de dados representam.

Artigo 34.º

Consulta prévia

1. (...)

2. O responsável pelo tratamento dos dados consulta a autoridade de controlo antes de proceder ao tratamento de dados pessoais quando a avaliação de impacto sobre a proteção de dados prevista no artigo 33.º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco.

3. Sempre que considerar que o tratamento previsto referido no n.º 2 violaria o disposto no presente regulamento, especialmente se o responsável pelo tratamento dos dados não tiver identificado ou atenuado suficientemente os riscos, a autoridade de controlo, num período máximo de oito semanas após o pedido de consulta, dá orientações, por escrito, ao responsável pelo tratamento dos dados e ao subcontratante, se o houver, e pode recorrer a todos os seus poderes referidos no artigo 53.º. Este período pode ser prorrogado por mais seis semanas, tendo em conta a complexidade do tratamento previsto. Caso haja lugar a prorrogação, o responsável pelo tratamento dos dados ou o subcontratante, se o houver, é informado no prazo de um mês a contar da data de receção do pedido, nomeadamente dos motivos do atraso. Estes prazos podem ser suspensos até que a autoridade de controlo tenha obtido as informações que tenha solicitado para efeitos da consulta.

4. (...)

5. (...)

6. Quando consultar a autoridade de controlo nos termos do n.º 2, o responsável pelo tratamento dos dados comunica-lhe os seguintes elementos:

   a) Se for aplicável, a repartição de responsabilidades entre o responsável pelo tratamento dos dados, os responsáveis conjuntos e os subcontratantes envolvidos no tratamento, em particular 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 33.º, e

   f) Quaisquer outras informações solicitadas pela autoridade de controlo.

7. 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 pessoais.

7-A. Não obstante o n.º 2, a legislação dos Estados-Membros pode exigir que os responsáveis pelo tratamento dos dados consultem a autoridade de controlo e dela obtenham uma autorização prévia em relação ao tratamento de dados pessoais por um responsável no exercício de uma missão de interesse público, nomeadamente o tratamento desses dados por motivos de proteção social e de saúde pública.

8. (...)

9. (...).

SECÇÃO 4
ENCARREGADO DA PROTEÇÃO DE DADOS

Artigo 35.º

Designação do encarregado da proteção de dados

1. O responsável pelo tratamento dos dados 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 que atuem no exercício das sua funções jurisdicionais; ou

   b) As atividades principais do responsável pelo tratamento dos dados 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 dos dados 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 relacionados com condenações e infrações penais a que se refere o artigo 9.º-A.

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 dos dados 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 dos dados ou o subcontratante ou as associações e outros organismos que representem categorias de responsáveis pelo tratamento dos dados ou de subcontratantes podem, ou, se tal lhes for exigido pelo direito da União ou dos Estados-Membros, designam um encarregado da proteção de dados. O encarregado da proteção de dados pode atuar em nome das associações e de outros organismos que representem os responsáveis pelo tratamento dos dados 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 da legislação e das práticas de proteção de dados, bem como na sua capacidade para desempenhar as funções referidas no artigo 37.º.

6. (...)

7. (...)

8. O encarregado da proteção de dados pode ser um elemento do pessoal da entidade responsável pelo tratamento dos dados ou do subcontratante, ou exercer as suas funções com base num contrato de prestação de serviços.

9. O responsável pelo tratamento dos dados ou o subcontratante publica os contactos do encarregado da proteção de dados e comunica-os à autoridade de controlo.

10. (...)

11. (...).

Artigo 36.º

Cargo de encarregado da proteção de dados

1. O responsável pelo tratamento dos dados ou o subcontratante assegura 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 ou o subcontratante apoia o encarregado da proteção de dados no exercício das funções a que se refere o artigo 37.º, fornecendo-lhe os recursos necessários ao desempenho dessas funções e à manutenção dos seus conhecimentos, e dando-lhe acesso aos dados pessoais e às operações de tratamento.

2-A. (novo) Os titulares dos dados podem contactar o encarregado da proteção de dados sobre todos os assuntos relacionados com o tratamento dos seus dados pessoais e o exercício dos direitos que lhe são conferidos pelo presente regulamento.

3. O responsável pelo tratamento dos dados ou o subcontratante assegura-se de que o encarregado da proteção de dados não recebe instruções relativamente ao exercício das suas funções. Pelo simples facto de desempenhar as suas funções, o delegado não é destituído nem penalizado pelo responsável pelo tratamento ou pelo subcontratante. O encarregado da proteção de dados informa diretamente a direção do responsável pelo tratamento dos dados ou do subcontratante ao mais alto nível.

4. O encarregado da proteção de dados está vinculado ao dever de sigilo ou de confidencialidade no exercício das suas funções, em conformidade com o direito da União ou dos Estados--Membros.

4-A. O encarregado da proteção de dados pode exercer outras funções e atribuições. O responsável pelo tratamento dos dados ou o subcontratante assegura-se de que essas funções e atribuições não resultam num conflito de interesses.

Artigo 37.º

Funções do encarregado da proteção de dados

1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:
   a) Informar e aconselhar o responsável pelo tratamento dos dados ou o subcontratante, bem como os empregados que efetuam o tratamento de dados pessoais, quanto às suas obrigações nos termos do presente regulamento e de outras disposições da União ou dos Estados-Membros relativas à proteção de dados.

   b) Controlar a conformidade com o presente regulamento, com outras disposições da União ou dos Estados-Membros relativas à proteção de dados e com as orientações do responsável pelo tratamento dos dados ou do subcontratante 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) (...)

   d) (...)

   e) (...)

   f) 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 33.º;

g) Cooperar com a autoridade de controlo;

h) Atuar como ponto de contacto para a autoridade de controlo em assuntos relacionados com o tratamento de dados pessoais, incluindo a consulta prévia referida no artigo 34.º, e consultar esta autoridade sobre qualquer outro assunto, consoante as necessidades.

2. (...)

2-A. 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 38.º

Códigos de conduta

1. Os Estados-Membros, as autoridades de controlo, o Comité Europeu para a Proteção de Dados 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 de dados e as necessidades específicas das micro, pequenas e médias empresas.

1-A. As associações e outros organismos representantes de categorias de responsáveis pelo tratamento dos dados ou de subcontratantes podem elaborar códigos de conduta, alterar ou aumentar esses códigos, a fim de especificar a aplicação de certas disposições do presente regulamento, tais como:

a) O tratamento de dados equitativo e transparente;

a-A) Os legítimos interesses dos responsáveis pelo tratamento dos dados em contextos específicos;

b) A recolha de dados;

b-B) A pseudonimização dos dados pessoais;

c) A informação do público e dos titulares dos dados;

d) O exercício dos direitos dos titulares dos dados;

e) As informações e a proteção das crianças e o modo de obter o consentimento do titular da responsabilidade parental da criança;

e-E) As medidas e procedimentos a que se referem os artigos 22.º e 23.º e as medidas destinadas a garantir a segurança do tratamento referidas no artigo 30.º;

e-F) A notificação de violações de dados pessoais às autoridades de controlo e a comunicação dessas violações aos titulares dos dados;

f) A transferência de dados pessoais para países terceiros ou organizações internacionais;

g) (...)

h) As ações extrajudiciais e outros procedimentos de resolução de litígios entre os responsáveis pelo tratamento dos dados e os titulares dos dados em relação ao tratamento de dados pessoais, sem prejuízo dos direitos dos titulares dos dados nos termos dos artigos 73.º e 75.º.

1-A-B. Além do cumprimento por parte dos responsáveis pelo tratamento dos dados ou dos subcontratantes sujeitos ao regulamento, os responsáveis pelo tratamento dos dados ou subcontratantes que não estão sujeitos ao presente regulamento de acordo com o artigo 3.º também podem cumprir códigos de conduta aprovados em conformidade com o n.º 2 e de aplicabilidade geral em conformidade com o n.º 4, de modo a fornecer garantias apropriadas no quadro das transferências dos dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 42.º, n.º 2, alínea d). Os responsáveis pelo tratamento dos dados 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.

1-B. Os códigos de conduta referidos no n.º 1-A devem prever certos mecanismos que permitam ao organismo referido no artigo 38.º-A, n.º 1, efetuar a supervisão obrigatória do cumprimento das suas disposições por parte dos responsáveis pelo tratamento dos dados ou subcontratantes que se comprometam a aplicá-lo, sem prejuízo das funções e competências da autoridade de controlo competente nos termos do artigo 51.º ou 51.º-A.

2. As associações e outros organismos a que se refere o n.º 1-A que tencionem elaborar um código de conduta, ou alterar ou aumentar um código existente, apresentam o projeto de código à autoridade de controlo competente nos termos do artigo 51.º. A autoridade de controlo emite um parecer sobre a conformidade do projeto de código de conduta ou da alteração ou aditamento com o presente regulamento e aprova este projeto, alteração ou aditamento se determinar que são previstas garantias apropriadas suficientes.

2-A. Se o parecer a que se refere o n.º 2 confirmar que o código de conduta, ou a alteração ou aditamento, está conforme com o presente regulamento e o código for aprovado, e se o código de conduta não estiver relacionado com atividades de tratamento realizadas em vários Estados-Membros, a autoridade de controlo regista e publica o código.

2-B. 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 51.º, apresenta-o pelo procedimento previsto no artigo 57.º, antes da aprovação, ao Comité Europeu para a Proteção de Dados, que emite um parecer sobre a conformidade do projeto de código de conduta, ou da alteração ou aditamento, com o presente regulamento, ou, na situação referida no n.º 1-A-B, prevê as garantias adequadas.

3. Se o parecer a que se refere o n.º 2-B confirmar que os códigos de conduta, ou a alteração ou aditamento, estão conformes com o presente regulamento, ou previr garantias adequadas na situação referida no n.º 1-A-B, o Comité Europeu para a Proteção de Dados apresenta o seu parecer à Comissão.

4. São atribuídas à Comissão competências para adotar atos de execução a fim de declarar, mediante decisão, que os códigos de conduta aprovados, bem como as alterações ou aditamentos aos códigos de conduta aprovados existentes que lhe sejam apresentados nos termos do n.º 3, são de aplicabilidade geral na União. Esses atos de execução são adotados em conformidade com o procedimento de exame previsto no artigo 87.º, n.º 2.

5. A Comissão assegura a publicidade adequada dos códigos aprovados que declarou, mediante decisão, serem de aplicabilidade geral em conformidade com o n.º 4.

5-A. O Comité Europeu para a Proteção de Dados recolhe todos os códigos de conduta aprovados e respetivas alterações num registo e disponibiliza-os ao público pelos meios adequados.

Artigo 38.º-A

Supervisão dos códigos de conduta aprovados

1. Sem prejuízo das funções e competências da autoridade de controlo competente ao abrigo dos artigos 52.º e 53.º, a supervisão de um código de conduta nos termos do artigo 38.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 o efeito 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 dos dados 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 dar seguimento a reclamações relativas a violações do código ou à forma como o código tenha sido ou esteja a ser aplicado pelo responsável pelo tratamento dos dados ou subcontratante, e para tornar estes procedimentos e estruturas transparentes para os titulares dos dados e o público;

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 ao Comité Europeu para a Proteção de Dados, de acordo com o mecanismo de controlo da coerência referido no artigo 57.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 adota, sob reserva das garantias adequadas, as medidas que forem adequadas em caso de infração ao código por um responsável pelo tratamento dos dados 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 adoção.

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 não estiverem em conformidade com o presente regulamento.

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

Artigo 39.º

Certificação

1. Os Estados-Membros, as autoridades de controlo, o Comité Europeu para a Proteção de Dados e a Comissão promovem, em especial a nível da União, a criação de mecanismos 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 executadas pelos responsáveis pelo tratamento dos dados e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas.

1-A. Além do cumprimento dos responsáveis pelo tratamento dos dados ou dos subcontratantes sujeitos ao presente regulamento, os mecanismos de certificação em matéria de proteção de dados, bem como selos ou marcas aprovados de acordo com o n.º 2-A 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 nos termos do artigo 3.º no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais nos termos referidos no artigo 42.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 adequadas, inclusivamente em relação aos direitos dos titulares dos dados.

1-B. A certificação é voluntária e está disponível através de um processo transparente.

2. A certificação prevista no presente artigo não diminui a responsabilidade dos responsáveis pelo tratamento dos dados e subcontratantes pelo cumprimento do presente regulamento nem prejudica as funções e competências da autoridade de controlo competente nos termos do artigo 51.º ou 51.º-A.

2-A. A certificação prevista no presente artigo é emitida pelos organismos de certificação referidos no artigo 39.º-A, ou pela autoridade de controlo competente com base nos critérios aprovados pela autoridade de controlo competente ou, de acordo com o artigo 57.º, pelo Comité Europeu para a Proteção de Dados. Neste último caso, os critérios aprovados pelo Comité Europeu para a Proteção de Dados podem ter como resultado uma certificação comum, o Selo Europeu de Proteção de Dados.

3. (novo) Os responsáveis pelo tratamento dos dados e subcontratantes que submetem o seu tratamento ao mecanismo de certificação fornecem ao organismo de certificação a que se refere o artigo 39.º-A, 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.

4. A certificação é emitida aos responsáveis pelo tratamento dos dados 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 39.º-A ou pela autoridade de controlo competente, se os requisitos para a certificação não estiverem ou tiverem deixados de estar reunidos.

5. O Comité Europeu para a Proteção de Dados recolhe todos os mecanismos de certificação e todos os selos e marcas de proteção de dados aprovados num registo e disponibiliza-os ao público pelos meios adequados.

Artigo 39.º-A

Organismo e procedimento de certificação

1. Sem prejuízo das funções e poderes da autoridade de controlo competente nos termos dos artigos 52.º e 53.º, a certificação é emitida e renovada por um organismo de certificação que tenha um nível adequado de competência em matéria de proteção de dados, depois de informada a autoridade de controlo para que esta exerça as suas competências nos termos do artigo 53.º, n.º 1-B, alínea f-A), sempre que necessário. Os Estados-Membros indicam se estes organismos de certificação são acreditados:

   a) pela autoridade de controlo competente nos termos do artigo 51.º ou 51.º-A; e/ou

   b) pelo organismo nacional de acreditação nomeado em conformidade com o 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, em conformidade com a norma EN-ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo competente de acordo com o artigo 51.º ou 51.º-A.

2. O organismo de certificação referido no n.º 1 pode ser acreditado para este efeito se:

   a) Tiver demonstrado que goza de independência e dispõe dos conhecimentos necessários em relação ao objeto da certificação, de forma satisfatória para a autoridade de controlo competente;

a-A) Se tiver comprometido a respeitar os critérios referidos no artigo 39.º, n.º 2-A, e aprovados pela autoridade de controlo competente nos termos do artigo 51.º ou 51.º-A ou, nos termos do artigo 57.º, pelo Comité Europeu para a Proteção de Dados;

b) Tiver estabelecido procedimentos para a emissão, revisão periódica e retirada de mecanismos de certificação, selos e marcas de proteção de dados;

c) Tiver estabelecido procedimentos e estruturas para dar seguimento a reclamações relativas a violações da certificação ou à forma como a certificação tenha sido ou esteja a ser implementada pelo responsável pelo tratamento dos dados ou subcontratante, e para tornar estes procedimentos e estruturas transparentes para os titulares dos dados e o público;

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 acreditação dos organismos de certificação referida no n.º 1 é efetuada com base nos critérios aprovados pela autoridade de controlo competente nos termos do artigo 51.º ou 51.º-A ou, nos termos do artigo 57.º, pelo Comité Europeu para a Proteção de Dados. No caso de acreditações nos termos do n.º 1, alínea b), estes requisitos complementam os requisitos previstos no Regulamento n.º 765/2008 e as regras técnicas que descrevem os métodos e procedimentos dos organismos de certificação.

4. O organismo de certificação a que se refere o n.º 1 é responsável pela correta avaliação necessária à certificação, ou pela revogação dessa certificação, sem prejuízo da responsabilidade que cabe ao responsável pelo tratamento dos dados 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 reúna os requisitos.

5. O organismo de certificação a que se refere o n.º 1 fornece à autoridade de controlo competente os motivos que levaram à concessão ou revogação da certificação solicitada.

6. Os requisitos referidos no n.º 3, e os critérios referidos no artigo 39.º, n.º 2-A, são publicados pela autoridade de controlo sob uma forma facilmente acessível. As autoridades de controlo também comunicam estas informações ao Comité Europeu para a Proteção de Dados. O Comité Europeu para a Proteção de Dados recolhe todos os mecanismos de certificação e selos de proteção de dados aprovados num registo e disponibiliza-os ao público pelos meios adequados.

6-A. Sem prejuízo das disposições do Capítulo VIII, a autoridade de controlo competente ou o organismo nacional de acreditação 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 não estiverem em conformidade com o presente regulamento.

7. São atribuídas à Comissão competências para adotar atos delegados em conformidade com o artigo 86.º, a fim de especificar os requisitos a ter em conta relativamente aos mecanismos de certificação em matéria de proteção de dados referidos no artigo 39.º, n.º 1.

7-A. (...)

8. A Comissão pode estabelecer normas técnicas para os mecanismos de certificação e os selos e marcas em matéria de proteção de dados, e mecanismos para promover e reconhecer os mecanismos de certificação e selos e marcas de proteção de dados. Os atos de execução correspondentes são adotados em conformidade com o procedimento de exame previsto no artigo 87.º, n.º 2.

CAPÍTULO V
TRANSFERÊNCIA DE DADOS PESSOAIS PARA PAÍSES TERCEIROS OU ORGANIZAÇÕES INTERNACIONAIS

Artigo 40.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 pode ser realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas pelo responsável pelo tratamento dos dados 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 fique comprometido o nível de proteção das pessoas singulares garantido pelo presente regulamento.

Artigo 41.º

Transferências acompanhadas de uma decisão de adequação

1. Pode ser realizada uma transferência de dados pessoais para um país terceiro ou uma organização internacional 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, 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 os precedentes jurisprudenciais, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares 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 impor o cumprimento das 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. Após avaliar a adequação do nível de proteção, a Comissão pode determinar que um país terceiro, um território, um ou mais setores específicos desse país terceiro, ou uma organização internacional, garante um nível de proteção adequado na aceção do n.º 2. O ato de execução prevê um mecanismo de revisão 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). O ato de execução é adotado em conformidade com o procedimento de exame previsto no artigo 87.º, n.º 2.

3-A. (...)

4. (...)

4-A. 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 e das decisões adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE.

5. A Comissão determina, sempre que a informação disponível o revelar, em especial na sequência da revisão a que se refere o n.º 3, que um país terceiro, território ou setor específico desse país terceiro, ou uma organização internacional deixou de garantir um nível de proteção adequado na aceção do n.º 2 e, na medida do necessário, revoga, altera ou suspende a decisão referida no n.º 3, sem efeitos retroativos. O ato de execução correspondente é adotado em conformidade com o procedimento de exame referido no artigo 87.º, n.º 2, ou, em casos de extrema urgência, em conformidade com o procedimento referido no artigo 87.º, n.º 3.

5-A. 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.

6. As decisões tomadas por força do n.º 5 não prejudicam as transferências de dados pessoais para o país terceiro, território ou setor específico desse país terceiro, ou para a organização internacional em causa, nos termos dos artigos 42.º a 44.º.

7. 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.

8. 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.

Artigo 42.º

Transferências mediante garantias adequadas

1. Não tendo sido tomada nenhuma decisão nos termos do artigo 41.º, n.º 3, os responsáveis pelo tratamento dos dados 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:

   o-A) Um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos; ou

   a) Regras vinculativas para empresas em conformidade com o artigo 43.º; ou

   b) Cláusulas-tipo de proteção de dados adotadas pela Comissão em conformidade com o procedimento de exame referido no artigo 87.º, n.º 2; ou

   c) Cláusulas-tipo de proteção de dados adotadas por uma autoridade de controlo e aprovadas pela Comissão nos termos do procedimento de exame referido no artigo 87.º, n.º 2; ou

d) Um código de conduta, aprovado nos termos do artigo 38.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento dos dados ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados; ou

e) Um mecanismo de certificação, aprovado nos termos do artigo 39.º, acompanhado de compromissos vinculativos e com força executiva assumidos pelos responsáveis pelo tratamento dos dados ou pelos subcontratantes no país terceiro no sentido de aplicarem as garantias adequadas, nomeadamente no que respeita aos direitos dos titulares dos dados.

2-A. 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 dos dados ou subcontratantes e os responsáveis pelo tratamento dos dados, subcontratantes ou destinatários dos dados no país terceiro ou organização internacional; ou

b) Disposições a inserir no regime administrativo instituído entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

3. (...)

4. (...)

5. (...)

5-A. A autoridade de controlo aplica o mecanismo de controlo da coerência a que se refere o artigo 57.º nos casos enunciados no n.º 2-A.

5-B. 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.

Artigo 43.º

Transferências mediante aplicação de regras vinculativas para empresas

1. Em conformidade com o mecanismo de controlo da coerência previsto no artigo 57.º, a autoridade de controlo competente aprova regras vinculativas para empresas, que devem:

   a) Ser juridicamente vinculativas e aplicáveis a todas as entidades em causa do grupo empresarial ou dos grupos 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;

   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 em causa 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 caráter 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 períodos de conservação, a qualidade dos dados, a proteção dos dados desde a conceção e por defeito, a base jurídica 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 para empresas;

e) Os direitos dos titulares dos dados relativamente ao tratamento dos seus dados pessoais e os mecanismos 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 20.º, o direito de apresentar reclamação à autoridade de controlo competente e aos tribunais competentes dos Estados-Membros nos termos do artigo 75.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 dos dados 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) supra, são comunicadas aos titulares dos dados para além das informações referidas nos artigos 14.º e 14.º-A;

h) As funções de qualquer encarregado da proteção de dados designado nos termos do artigo 35.º ou de qualquer outra pessoa ou entidade responsável, a nível do grupo de empresas, pelo controlo do cumprimento das regras vinculativas aplicáveis às empresas e pela supervisão das ações de formação e do tratamento de reclamações;

h-H) Os procedimentos de reclamação;

i) Os mecanismos existentes no grupo para assegurar a verificação do cumprimento das regras vinculativas aplicáveis às empresas. Esses mecanismos passam pela realização de auditorias sobre a proteção de dados e pelo 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 de empresas que exerce o controlo, devendo também ser facultados à autoridade de controlo competente, a pedido desta;

j) Os mecanismos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controlo;

k) O mecanismo de cooperação com a autoridade de controlo para assegurar o cumprimento, por qualquer entidade do grupo, em especial facultando à autoridade de controlo os resultados de verificações das medidas referidas na alínea i) supra;

l) Os mecanismos de comunicação, à autoridade de controlo competente, de todos os requisitos legais a que uma entidade do grupo esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas; e

m) Ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal.

2-A. (...)

3. (...)

4. A Comissão pode especificar o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento dos dados, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas a aplicar às empresas na aceção do presente artigo. Esses atos de execução são adotados em conformidade com o procedimento de exame previsto no artigo 87.º, n.º 2.

Artigo 43.º-A (novo)

Transferências ou divulgações não autorizadas pelo direito da União

1. As decisões judiciais e as decisões de autoridades administrativas de um país terceiro que exijam que o responsável pelo tratamento dos dados 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 44.º

Derrogações aplicáveis a situações específicas

1. Na falta de uma decisão de adequação nos termos do artigo 41.º, n.º 3, ou de garantias adequadas nos termos do artigo 42.º, designadamente de regras vinculativas aplicáveis às empresas, as transferências ou conjunto de transferências de dados pessoais para países terceiros ou organizações internacionais só podem ser efetuadas se:

   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; ou

   b) A transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo seu tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular; ou

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

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

   e) A transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial; ou

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

g) A transferência for realizada a partir de um registo que, nos termos do direito da União 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; ou

h) Quando uma transferência não poder basear-se no disposto nos artigos 41.º ou 42.º, incluindo as regras vinculativas aplicáveis às empresas, e não for aplicável nenhuma das derrogações previstas para as situações específicas referidas nas alíneas a) a g), 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 dos dados 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 dos dados informa da transferência a autoridade de controlo. Para além da informação referida nos artigos 14.º e 14.º-A, o responsável pelo tratamento dos dados presta informações ao titular dos dados sobre a transferência e os interesses legítimos visados pelo responsável pelo tratamento dos dados.

2. As transferências efetuadas nos termos do n.º 1, 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. (...)

4. O n.º 1, alíneas a), b), c) e h), não é aplicável a atividades levadas a cabo por autoridades públicas no exercício dos seus poderes.

5. O interesse público referido no n.º 1, alínea d), deve ser reconhecido pelo direito da União ou pelo direito do Estado-Membro a que o responsável pelo tratamento dos dados se encontre sujeito.

5-A. Na falta de uma decisão de adequação, o direito da União ou o direito interno 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 dos dados ou o subcontratante documenta a avaliação, bem como as garantias adequadas referidas no n.º 1, alínea h), nos registos a que se refere o artigo 28.º.

7. (...).

Artigo 45.º

Cooperação internacional no domínio da proteção de dados pessoais

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

   a) Estabelecer mecanismos 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 relativa à proteção de dados pessoais, nomeadamente através da notificação, transmissão de reclamações, assistência na investigação e intercâmbio de informações, sob reserva das garantias adequadas de proteção dos dados pessoais e de outros direitos e liberdades fundamentais;

c) Associar as partes interessadas aos debates e atividades que visem 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.

2. (...)

CAPÍTULO VI
AUTORIDADES DE CONTROLO INDEPENDENTES

SECÇÃO 1
ESTATUTO INDEPENDENTE

Artigo 46.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 proteger os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento dos seus dados pessoais e facilitar a livre circulação desses dados na União.

1-A. As autoridades de controlo contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, cooperam entre si e com a Comissão, nos termos do Capítulo VII.

2. Quando estiverem estabelecidas mais do que uma autoridade de controlo num Estado-Membro, este determina qual a autoridade de controlo que as representa no Comité Europeu para a Proteção de Dados e estabelece o mecanismo para assegurar que as regras relativas ao mecanismo de controlo da coerência referido no artigo 57.º, são cumpridas pelas autoridades.

3. Os Estados-Membros notificam a Comissão das disposições do direito nacional que adotarem nos termos do n.º 1, o mais tardar na data fixada no artigo 91.º, n.º 2 e, sem demora, de qualquer alteração posterior a essas mesmas disposições.

Artigo 47.º

Independência

1. Cada autoridade de controlo age com total independência no desempenho das funções 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. (...)

5. Os Estados-Membros asseguram que cada autoridade de controlo disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários ao desempenho eficaz das suas funções e ao exercício dos seus poderes, inclusive no contexto da assistência mútua, da cooperação e da participação no Comité Europeu para a Proteção de Dados.

6. 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.

7. Os Estados-Membros asseguram que cada autoridade de controlo fique sujeita a um controlo financeiro que não afete a sua independência. Os Estados-Membros asseguram que cada autoridade de controlo disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral estatal ou nacional.

Artigo 48.º

Condições gerais aplicáveis aos membros da autoridade de controlo

1. Os Estados-Membros preveem que cada membro da autoridade de controlo seja nomeado por procedimento transparente:
   – pelo Parlamento; ou
   – pelo Governo; ou
   – pelo Chefe de Estado do Estado-Membro em causa; ou
   – por um organismo independente incumbido da nomeação nos termos do direito dos Estados-Membros.

2. Os membros da autoridade de controlo devem possuir as qualificações, a experiência e os conhecimentos necessários ao desempenho das suas funções e ao exercício dos seus poderes, em especial no domínio da proteção de dados pessoais.

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

4. Os membros da autoridade de controlo só podem ser exonerados se tiverem cometido uma falta grave ou se tiverem deixado de cumprir as condições exigidas para o exercício das suas funções.

Artigo 49.º

Regras aplicáveis à constituição da autoridade de controlo

1. Os Estados-Membros preveem, por via legislativa:

   a) A constituição de cada autoridade de controlo;

   b) As qualificações e condições de elegibilidade necessárias para a nomeação dos membros de cada autoridade de controlo;

   c) As regras e procedimentos aplicáveis à 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 a entrada em vigor do presente regulamento, e pode 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 normas que regem a cessação da relação de trabalho.

g) (...)

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 termo deste, 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, o dever de sigilo profissional aplica-se, em especial, à comunicação, por particulares, de violações ao presente regulamento.

Artigo 50.º

Sigilo profissional

(...)

SECÇÃO 2
COMPETÊNCIA, FUNÇÕES E PODERES

Artigo 51.º

Competência

1. As autoridades de controlo são competentes para desempenhar as funções 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, alíneas c) ou e), é competente a autoridade de controlo do Estado-Membro em causa. Nesses casos, não é aplicável o artigo 51.º-A.

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 51.º-A

Competência da autoridade de controlo principal

1. Sem prejuízo do disposto no artigo 51.º, a autoridade de controlo do estabelecimento principal ou do estabelecimento único do responsável pelo tratamento dos dados ou do subcontratante é competente para atuar como autoridade de controlo principal para o tratamento transfronteiras efetuado pelo referido responsável pelo tratamento ou subcontratante nos termos previstos no artigo 54.º-A.

2-A. Em derrogação do n.º 1, cada autoridade de controlo é competente para dar seguimento a 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.

2-B. Nos casos previstos no n.º 2-A, a autoridade de controlo informa imediatamente 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 se ocupa da matéria, nos termos previstos no artigo 54.º-A, tendo em conta se há ou não algum estabelecimento do responsável pelo tratamento dos dados ou subcontratante no Estado-Membro sobre o qual a autoridade de controlo a tenha informado.

2-C. Quando a autoridade de controlo principal decide ocupar-se da matéria, aplica-se o procedimento previsto no artigo 54.º-A. 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 54.º-A, n.º 2.

2-D. Caso a autoridade de controlo principal decida não se ocupar da matéria, é a autoridade de controlo que a informou que dela se ocupa, nos termos dos artigos 55.º e 56.º.

3. A autoridade de controlo principal é o único interlocutor do responsável pelo tratamento dos dados ou do subcontratante no tratamento transfronteiras efetuado pelo referido responsável pelo tratamento ou subcontratante.

Artigo 52.º

Funções

1. Sem prejuízo de outras funções previstas nos termos do presente regulamento, cada autoridade de controlo é responsável, no seu território, por:

a) Controlar e impor o cumprimento do presente regulamento;

a-A) Promover a sensibilização e a compreensão do público relativamente aos riscos, regras, garantias e direitos associados ao tratamento de dados pessoais. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial;

a-B) Aconselhar, nos termos do direito nacional, o Parlamento nacional, o Governo e outras instituições e organismos quanto às medidas legislativas e administrativas relacionadas com a proteção dos direitos e liberdades individuais no que diz respeito ao tratamento de dados pessoais;

a-C) Promover a sensibilização dos responsáveis pelo tratamento de dados e dos subcontratantes para as suas obrigações nos termos do presente regulamento;

a-D) Se lhe for solicitado, prestar informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, cooperar com as autoridades de controlo de outros Estados-Membros para esse efeito;

b) Atender às reclamações apresentadas pelos titulares de dados, ou por organismos, organizações ou associações nos termos do artigo 76.º, e investigar, na medida do necessário, o conteúdo da reclamação, informando 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;

c) Cooperar, nomeadamente partilhando informações e prestar assistência mútua a outras autoridades de controlo, tendo em vista assegurar a coerência da aplicação e da execução do presente regulamento;

d) Conduzir investigações sobre a aplicação do presente regulamento, nomeadamente com base em informações recebidas de outra autoridade de controlo ou outra autoridade pública;

e) Acompanhar factos novos relevantes, na medida em que tenham incidência na proteção de dados pessoais, particularmente a evolução a nível das tecnologias da informação, comunicação e das práticas comerciais;

f) Adotar as cláusulas contratuais-tipo previstas no artigo 26.º, n.º 2-C, e no artigo 42.º, n.º 2, alínea c);

f-A) Elaborar e conservar uma lista associada à exigência de realizar uma avaliação do impacto sobre a proteção de dados, nos termos do artigo 33.º, n.º 2-A;

g) Dar orientações sobre as operações de tratamento previstas no artigo 34.º, n.º 3;

g-A) Incentivar a elaboração de códigos de conduta nos termos do artigo 38.º, dar parecer sobre eles e aprovar os que preveem garantias suficientes, nos termos do artigo 38.º, n.º 2;

g-B) Incentivar o estabelecimento de mecanismos de certificação de proteção de dados, e de selos e marcas de proteção de dados, nos termos do artigo 39.º, n.º 1, e aprovar os critérios de certificação nos termos do artigo 39.º, n.º 2-A;

g-C) Se necessário, proceder a uma revisão periódica das certificações emitidas, nos termos do artigo 39.º, n.º 4;

h) Redigir e publicar os critérios de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 38.º-A e de um organismo de certificação nos termos do artigo 39.º-A;

h-A) Conduzir o processo de acreditação de um organismo para monitorizar códigos de conduta nos termos do artigo 38.º-A e de um organismo de certificação nos termos do artigo 39.º-A;

h-B) Autorizar as cláusulas contratuais e disposições previstas no artigo 42.º, n.º 2-A;

i) Aprovar as regras vinculativas para as empresas nos termos do artigo 43.º;

j) Contribuir para as atividades do Comité Europeu para a Proteção de Dados;

j-B) Conservar registos internos de violações ao presente regulamento e das medidas adotadas, em especial as advertências emitidas e as sanções impostas;

k) Desempenhar quaisquer outras tarefas relacionadas com a proteção de dados pessoais.

2. (...)

3. (...)

4. As autoridades de controlo facilitam a apresentação das reclamações previstas no n.º 1, alínea b), tomando certas medidas, como fornecer formulários de reclamação que possam também ser preenchidos eletronicamente, sem excluir outros meios de comunicação.

5. O desempenho das funções de cada autoridade de controlo é gratuito para o titular dos dados e para o encarregado da proteção de dados, se existir.

6. Quando os pedidos forem manifestamente infundados ou excessivos, particularmente devido ao seu caráter recorrente, a autoridade de controlo pode exigir o pagamento de uma taxa razoável, tendo em conta os custos administrativos, ou pode indeferi-los. Cabe à autoridade de controlo demonstrar o caráter manifestamente infundado ou excessivo dos pedidos.

Artigo 53.º

Poderes

1. Cada autoridade de controlo tem os seguintes poderes de investigação:

a) Ordenar que o responsável pelo tratamento dos dados e o subcontratante e, se existir, o seu representante, lhe forneçam as informações de que necessite para o desempenho das suas funções;

a-A) Realizar investigações sob a forma de auditorias sobre a proteção de dados;

a-B) Rever as certificações emitidas nos termos do artigo 39.º, n.º 4;

b) (...)

c) (...)

d) Notificar o responsável pelo tratamento dos dados ou o subcontratante de alegadas violações do presente regulamento;

d-A) Obter, do responsável pelo tratamento de dados e do subcontratante, acesso a todos os dados pessoais e a todas as informações necessárias ao exercício das suas funções;

d-B) Obter acesso a todas as instalações do responsável pelo tratamento dos dados e do subcontratante, incluindo os equipamentos e meios de tratamento de dados, em conformidade com o direito da União ou com o direito processual dos Estados-Membros.

1-B. Cada autoridade de controlo tem os seguintes poderes de correção:

a) Fazer advertências ao responsável pelo tratamento de dados ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições do presente regulamento;

b) Fazer repreensões a um responsável pelo tratamento de dados ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições do presente regulamento;

c-A) Ordenar ao responsável pelo tratamento de dados 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 de dados 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;

d-A) Ordenar ao responsável pelo tratamento dos dados que comunique ao titular dos dados uma violação de dados pessoais;

e) Impor uma limitação temporária ou definitiva ao tratamento de dados, ou mesmo a sua proibição;

f) Ordenar a retificação, a limitação ou o apagamento de dados nos termos dos artigos 16.º, 17.º e 17.º-A, bem como a notificação dessas medidas aos destinatários a quem tenham sido divulgados os dados nos termos dos artigos 17.º, n.º 2-A e 17.º-B;

f-A) (novo) Retirar a certificação ou ordenar ao organismo de certificação que retire uma certificação emitida nos termos dos artigos 39.º e 39.º-A, ou ordenar ao organismo de certificação que não emita uma certificação se os requisitos de certificação não estiverem ou deixarem de estar cumpridos;

g) Impor uma multa administrativa nos termos do artigo 79.º, para além, ou em vez das medidas referidas na presente disposição, consoante as circunstâncias de cada caso;

h) Ordenar a suspensão do envio de dados para destinatários em países terceiros ou para organizações internacionais.

i) (...)

j) (...)

1-C. Cada autoridade de controlo tem os seguintes poderes consultivos e de autorização:

a) Aconselhar o responsável pelo tratamento dos dados em conformidade com o procedimento de consulta prévia previsto no artigo 34.º;

a-A) Emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao Parlamento nacional, ao Governo do Estado-Membro ou, em conformidade com o direito nacional, a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais;

a-B) Autorizar o tratamento previsto no artigo 34.º, n.º 7-A, se a lei do Estado-Membro exigir tal autorização prévia;

a-C) Emitir pareceres e aprovar projetos de códigos de conduta nos termos do artigo 38.º, n.º 2;

a-D) Acreditar organismos de certificação nos termos do artigo 39.º-A;

a-E) Emitir certificações e aprovar os critérios de certificação nos termos do artigo 39.º, n.º 2-A;

b) Adotar as cláusulas-tipo de proteção de dados previstas no artigo 26.º, n.º 2-C, e no artigo 42.º, n.º 2, alínea c);

c) Autorizar as cláusulas contratuais previstas no artigo 42.º, n.º 2-A, alínea a);

c-A) Autorizar os acordos administrativos previstos no artigo 42.º, n.º 2-A, alínea d);

d) Aprovar as regras vinculativas para as empresas nos termos do artigo 43.º.

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

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

4. Os Estados-Membros podem estabelecer por lei que as suas autoridades de controlo terão outros poderes para além dos previstos nos n.ºs 1, 1-B e 1-C. O exercício desses poderes não deve prejudicar o efetivo funcionamento das disposições do Capítulo VII.

Artigo 54.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 impostas. O relatório é apresentado ao Parlamento nacional, ao Governo e às outras autoridades designadas pelo direito nacional. O relatório é facultado ao público, à Comissão e ao Comité Europeu para a Proteção de Dados.

CAPÍTULO VII
COOPERAÇÃO E COERÊNCIA

SECÇÃO 1
COOPERAÇÃO

Artigo 54.º-A

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.

1-A. A autoridade de controlo principal pode a qualquer momento solicitar que as outras autoridades de controlo interessadas prestem assistência mútua nos termos do artigo 55.º e pode realizar operações conjuntas nos termos do artigo 56.º, nomeadamente para proceder a investigações ou monitorizar a execução de medidas relativas a responsáveis pelo tratamento dos dados ou subcontratantes estabelecidos noutros Estados-Membros.

2. 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 tomem as suas posições em devida consideração.

3. Quando uma das outras autoridades de controlo interessadas expressa uma objeção pertinente e fundamentada ao projeto de decisão num prazo de quatro semanas após ter sido consultada nos termos do n.º 2, a autoridade de controlo principal, caso não dê seguimento à objeção ou o parecer não seja pertinente e fundamentado, remete o assunto para o mecanismo de controlo da coerência previsto no artigo 57.º.

3-A. Se a autoridade de controlo principal pretender dar seguimento à objeção apresentada, envia às outras autoridades de controlo interessadas um projeto de decisão revisto para que emitam parecer. Este projeto de decisão revisto é sujeito ao procedimento mencionado no n.º 3 num prazo de duas semanas.

4. Se nenhuma das outras autoridades de controlo interessadas se tiver oposto ao projeto de decisão apresentado pela autoridade de controlo principal no prazo previsto nos n.ºs 3 e 3-A, considera-se que a autoridade de controlo principal e as autoridades de controlo interessadas estão de acordo com o projeto de decisão e ficam por ela vinculadas.

4-A. A autoridade de controlo principal adota a decisão e dela notifica o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento dos dados ou do subcontratante, consoante o caso, e informa as outras autoridades de controlo interessadas e o Comité Europeu para a Proteção de Dados 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.

4-B. Em derrogação do disposto no n.º 4-A, 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 dos dados.

4-B-B. 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 dos dados e informa desse facto o estabelecimento principal ou o estabelecimento único do responsável pelo tratamento dos dados 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.

4-C. Após ter sido notificado da decisão da autoridade de controlo principal nos termos dos n.ºs 4--A e 4-B-B, o responsável pelo tratamento dos dados 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 dos dados 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.

4-D. 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 previsto no artigo 61.º.

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

Artigo 55.º

Assistência mútua

1. As autoridades de controlo prestam entre si qualquer informação útil e assistência mútua, a fim de executar e aplicar o presente regulamento de forma coerente, e tomam 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 consulta, inspeção e investigação.

2. As autoridades de controlo tomam 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. O pedido 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 à qual tenha sido dirigido um pedido de assistência não pode recusar dar-lhe seguimento, a menos que:

   a) não seja competente no que respeita à matéria do pedido ou às medidas cuja execução lhe é solicitada; ou

   b) dar seguimento ao pedido seja incompatível com o disposto no presente regulamento ou com 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 adotadas para lhe dar resposta. Nos casos de recusa previstos no n.º 4, expõe os motivos que a levaram a indeferir o pedido.

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

7. Não é cobrada nenhuma taxa pelas medidas tomadas na sequência de pedidos de assistência mútua. As autoridades de controlo podem estabelecer com outras autoridades de controlo regras para a indemnização, por outras autoridades de controlo, 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 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 51.º, n.º 1. Neste caso, considera-se que é urgente intervir, nos termos do artigo 61.º, n.º 1, e solicitar uma decisão vinculativa urgente ao Comité Europeu para a Proteção de Dados, nos termos do artigo 61.º, n.º 2.

9. (...)

10. A Comissão pode especificar o formato e os procedimentos para a assistência mútua referidos no presente artigo, bem como as modalidades de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité Europeu para a Proteção de Dados, nomeadamente o formato normalizado referido no n.º 6. Esses atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 87.º, n.º 2.

Artigo 56.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 dos dados ou o subcontratante tenha estabelecimentos em vários Estados-Membros ou 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, têm direito a participar nas operações conjuntas, consoante o caso, uma autoridade de controlo de cada um desses Estados-Membros. A autoridade de controlo competente em conformidade com o artigo 51.º-A, n.º 1, ou o artigo 51.º-A, n.º 2-C, convida a autoridade de controlo de cada um desses Estados-Membros a participar nas operações conjuntas em causa e responde sem demora ao pedido das autoridades de controlo para participar.

3. As autoridades de controlo podem, em conformidade com o direito do seu próprio Estado-Membro, e com a autorização da autoridade de controlo do Estado-Membro de origem, conferir poderes, nomeadamente poderes de investigação, aos membros ou ao pessoal da autoridade de controlo do Estado-Membro de origem implicados nas operações conjuntas ou, na medida em que a legislação nacional do Estado-Membro da autoridade de controlo de acolhimento o permita, autorizar os membros ou o pessoal da autoridade de controlo do Estado-Membro de origem a exercer os seus poderes de investigação, em conformidade com a legislação nacional 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 do Estado-Membro de acolhimento. Os membros ou pessoal da autoridade de controlo do Estado-Membro de origem estão sujeitos ao direito nacional da autoridade de controlo do Estado-Membro de acolhimento.

3-A. Se, em conformidade com o n.º 1, o pessoal da autoridade de controlo do Estado-Membro de origem exercer atividades noutro Estado-Membro, o Estado-Membro da autoridade de controlo de acolhimento assume a responsabilidade pelos seus atos, nomeadamente 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.

3-B. O Estado-Membro em cujo território forem causados os danos assegura a reparação destes 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 este último das somas que tenha pago aos seus representantes legais.

3-C. Sem prejuízo do exercício dos seus direitos perante terceiros e sem prejuízo do disposto no n.º 3-B, cada Estado-Membro renuncia, no caso previsto no n.º 1, a solicitar a outro Estado--Membro o reembolso do montante dos danos que tenha sofrido.

4. (...)

5. Sempre que se tencione efetuar uma operação conjunta e uma autoridade de controlo não cumprir, no prazo de um mês, a obrigação estabelecida na segunda frase do n.º 2, as outras autoridades de controlo podem adotar uma medida provisória no território do respetivo Estado-Membro em conformidade com o artigo 51.º. Neste caso, considera-se que é urgente intervir, nos termos do artigo 61.º, n.º 1, e solicitar um parecer ou uma decisão vinculativa urgente ao Comité Europeu para a Proteção de Dados, nos termos do artigo 61.º, n.º 2.

6. (...)

SECÇÃO 2
COERÊNCIA

Artigo 57.º

Mecanismo de controlo da coerência

1. 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 mecanismo de controlo da coerência previsto na presente secção.

Artigo 58.º

Parecer do Comité Europeu para a Proteção de Dados

1. O Comité Europeu para a Proteção de Dados 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 Europeu para a Proteção de Dados, quando esta:

   c) 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 33.º, n.º 2--A; ou

   c-A) Incida sobre uma questão, prevista no artigo 38.º, n.º 2-B, de saber se um projeto de código de conduta ou uma alteração ou aditamento a um código de conduta cumpre o presente regulamento; ou

   c-B) Vise aprovar os critérios de acreditação de um organismo nos termos do artigo 38.º-A, n.º 3, ou um organismo de certificação nos termos do artigo 39.º-A, n.º 3; ou

   d) Vise determinar as cláusulas-tipo de proteção de dados referidas no artigo 42.º, n.º 2, alínea c) e no artigo 26.º, n.º 2-C; ou

e) Vise autorizar as cláusulas contratuais previstas no artigo 42.º, n.º 2-A, alínea a); ou

f) Vise aprovar regras vinculativas para empresas na aceção do artigo 43.º.

2. As autoridades de controlo, o presidente do Comité Europeu para a Proteção de Dados ou a Comissão podem solicitar que o Comité Europeu para a Proteção de Dados analise qualquer matéria 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 55.º ou de operações conjuntas previstas no artigo 56.º.

3. Nos casos referidos nos n.ºs 1 e 2, o Comité Europeu para a Proteção de Dados emite parecer sobre a matéria que lhe é apresentada, a não ser que tenha já antes emitido parecer sobre a mesma matéria. O referido parecer é adotado no prazo de oito semanas por maioria simples dos membros que compõem o Comité Europeu para a Proteção de Dados. Este prazo pode ser prorrogado por mais seis semanas, em virtude da complexidade da matéria em apreço. Para efeitos do projeto de decisão referido no n.º 1 e enviado aos membros do Comité nos termos do n.º 6, 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. (...)

5. As autoridades de controlo e a Comissão comunicam por via eletrónica, sem demora injustificada, ao Comité Europeu para a Proteção de Dados, 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.

6. O Presidente do Comité Europeu para a Proteção de Dados informa sem demora injustificada por via eletrónica:

a) Os membros do Comité Europeu para a Proteção de Dados e a Comissão de quaisquer informações pertinentes que lhe tenham sido comunicadas, utilizando um formato normalizado. Se necessário, o Secretariado do Comité Europeu para a Proteção de Dados fornece traduções das informações pertinentes.

b) A autoridade de controlo referida, consoante o caso, nos n.ºs 1 e 2 e a Comissão do parecer e torna-o público.

7. (...)

7-A. As autoridades de controlo competentes não adotam os projetos de decisão referidos no n.º 1 enquanto estiver a decorrer o prazo referido no n.º 3.

7-B. (...)

8. A autoridade de controlo referida no n.º 1 tem na melhor conta o parecer do Comité Europeu para a Proteção de Dados e, no prazo de duas semanas a contar da receção do parecer, comunica por via eletrónica ao presidente do Comité Europeu para a Proteção de Dados se mantém ou tenciona alterar o projeto de decisão e, se existir, o projeto de decisão alterado, utilizando para tal um formato normalizado.

9. Quando as autoridades de controlo interessadas informarem o presidente do Comité Europeu para a Proteção de Dados, no prazo referido no n.º 8, 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 58.º-A, n.º 1.

Artigo 58.º-A

Resolução de litígios pelo Comité Europeu para a Proteção de Dados

1. A fim de assegurar a aplicação correta e coerente do presente regulamento em cada caso, o Comité Europeu para a Proteção de Dados adota uma decisão vinculativa nos seguintes casos:

a) Quando, num dos casos referidos no artigo 54.º-A, n.º 3, a autoridade de controlo interessada tiver expressado uma objeção pertinente e fundamentada a um projeto de decisão da autoridade principal ou esta tiver rejeitado a objeção por carecer de pertinência e/ou de fundamento. A decisão vinculativa diz respeito a todas as matérias sobre que incida a referida objeção pertinente e fundamentada, sobretudo à questão de saber se há violação do 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 Europeu para a Proteção de Dados nos casos referidos no artigo 58.º, n.º 1, ou não seguir o parecer do Comité Europeu para a Proteção de Dados emitido nos termos do artigo 58.º. Nesse caso, qualquer autoridade de controlo interessada, ou a Comissão, pode remeter o assunto para o Comité Europeu para a Proteção de Dados.

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 a matéria lhe é remetida. Este prazo pode ser prorrogado por mais um mês em virtude da complexidade da matéria 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 não houver maioria, 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. (...)

6. O presidente do Comité Europeu para a Proteção de Dados 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 Europeu para a Proteção de Dados, depois de a autoridade de controlo ter notificado a decisão final a que se refere o n.º 7.

7. Sem demora injustificada e o mais tardar um mês depois de o Comité Europeu para a Proteção de Dados 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. A autoridade de controlo principal ou, consoante o caso, a autoridade de controlo à qual tiver sido apresentada a reclamação, informa o Comité Europeu para a Proteção de Dados da data em que a decisão final é notificada, respetivamente, ao responsável pelo tratamento dos dados ou ao subcontratante e ao titular. A decisão final das autoridades de controlo interessadas é adotada nos termos do artigo 54.º-A, n.ºs 4-A, 4-B e 4-B-B. A decisão final remete para a decisão a que se refere o n.º 1 e especifica que a decisão referida no n.º 1 é publicada no sítio Web do Comité Europeu para a Proteção de Dados nos termos do n.º 6. A decisão final é acompanhada da decisão a que se refere o n.º 1.

Artigo 59.º

Parecer da Comissão

(...)

Artigo 60.º

Suspensão de um projeto de medida

(...)

Artigo 61.º

Procedimento de urgência

1. Em circunstâncias excecionais, quando a autoridade de controlo interessada considere que é urgente intervir a fim de defender os direitos e liberdades dos titulares dos dados, pode, em derrogação do mecanismo de controlo da coerência referido nos artigos 57.º, 58.º e 58.º-A ou do procedimento a que se refere o artigo 54.º-A, 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 Europeu para a Proteção de Dados 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 Europeu para a Proteção de Dados, 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 Europeu para a Proteção de Dados, 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 58.º, n.º 3, e do artigo 58.º-A, n.º 2, os pareceres urgentes ou decisões vinculativas urgentes a que se referem os n.ºs 2 e 3 são adotados no prazo de duas semanas por maioria simples dos membros do Comité Europeu para a Proteção de Dados.

Artigo 62.º

Troca de informações

1. A Comissão pode adotar atos de execução de aplicação geral para:

   a) (...)

   b) (...)

   c) (...)

   d) Especificar as modalidades de intercâmbio eletrónico de informações entre as autoridades de controlo e entre estas e o Comité Europeu para a Proteção de Dados, nomeadamente o formato normalizado referido no artigo 58.º.

Esses atos de execução são adotados em conformidade com o procedimento de exame referido no artigo 87.º, n.º 2.

2. (...)

3. (...)

Artigo 63.º

Execução

(...)

SECÇÃO 3
COMITÉ EUROPEU PARA A PROTEÇÃO DE DADOS

Artigo 64.º

Comité Europeu para a Proteção de Dados

1-A. O Comité Europeu para a Proteção de Dados é instituído como um organismo da União e está dotado de personalidade jurídica.

1-B. O Comité Europeu para a Proteção de Dados é representado pelo seu presidente.

2. O Comité Europeu para a Proteção de Dados 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.

3. Quando, num determinado Estado-Membro, haja mais do que uma autoridade de controlo com responsabilidade pelo controlo da aplicação do disposto no presente regulamento, é nomeado um representante comum nos termos da legislação nacional desse mesmo Estado-Membro.

4. A Comissão tem o direito de participar nas atividades e reuniões do Comité Europeu para a Proteção de Dados, sem direito de voto. A Comissão designa um representante. O presidente do Comité Europeu para a Proteção de Dados informa a Comissão das atividades do Comité a que preside.

5. Nos casos relacionados com o artigo 58.º-A, 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 65.º

Independência

1. O Comité Europeu para a Proteção de Dados é independente no exercício das suas funções ou poderes, nos termos dos artigos 66.º e 67.º.

2. Sem prejuízo dos pedidos da Comissão referidos no artigo 66.º, n.º 1, alínea b), e n.º 2, o Comité Europeu para a Proteção de Dados não solicita nem recebe instruções de outrem no exercício das suas funções ou poderes.

Artigo 66.º

Funções do Comité Europeu para a Proteção de Dados

1. O Comité Europeu para a Proteção de Dados assegura a aplicação coerente do presente regulamento. Para o efeito, o Comité Europeu para a Proteção de Dados exerce, por sua iniciativa ou, nos casos pertinentes, a pedido da Comissão, as seguintes atividades:

a-A) Controlar e assegurar a correta aplicação do presente regulamento nos casos previstos no artigo 57.º, n.º 3, sem prejuízo das funções das autoridades nacionais de controlo;

a) Aconselhar a Comissão em todas as questões relacionadas com a proteção de dados pessoais na União, nomeadamente em qualquer projeto de alteração ao presente regulamento;

a-A) Aconselhar a Comissão sobre o formato e os procedimentos de intercâmbio de informações entre os responsáveis pelo tratamento dos dados, os subcontratantes e as autoridades de controlo no que respeita às regras vinculativas aplicáveis às empresas;

a-B) (novo) Emitir diretrizes, recomendações e boas 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;

b) Analisar, por iniciativa própria ou a pedido de um dos seus membros ou da Comissão, qualquer questão relativa à aplicação do presente regulamento e emitir diretrizes, recomendações e boas práticas, a fim de incentivar a aplicação coerente do presente regulamento;

b-A) (novo) Emitir diretrizes, recomendações e boas práticas nos termos do artigo 66.º, n.º 1, alínea b), para definir mais concretamente os critérios e condições aplicáveis às decisões baseadas na definição de perfis, nos termos do artigo 20.º, n.º 2;

b-B) (novo) Emitir diretrizes, recomendações e boas práticas nos termos do artigo 66.º, n.º 1, alínea b), para determinar as violações e a demora injustificada referidas no artigo 31.º, n.ºs 1 e 2, bem como as circunstâncias particulares em que o responsável pelo tratamento dos dados ou o subcontratante é obrigado a notificar a violação de dados pessoais;

b-C) (novo) Emitir diretrizes, recomendações e boas práticas nos termos do artigo 66.º, n.º 1, alínea b), a respeito das circunstâncias em que as violações de dados pessoais são suscetíveis de resultar num risco elevado para os direitos e liberdades individuais a que se refere o artigo 32.º, n.º 1.

b-D) (novo) Emitir diretrizes, recomendações e boas práticas nos termos do artigo 66.º, n.º 1, alínea b), 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 dos dados 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 43.º;

b-E) (novo) Emitir diretrizes, recomendações e boas práticas nos termos do artigo 66.º, n.º 1, alínea b), para definir mais concretamente os critérios e requisitos aplicáveis à transferência de dados efetuadas com base no artigo 44.º, n.º 1;

b-A) Elaborar diretrizes dirigidas às autoridades de controlo em matéria de aplicação das medidas a que se refere o artigo 53.º, n.ºs 1, 1-B e 1-C, e à fixação de multas administrativas nos termos do artigo 79.º;

c) Examinar a aplicação prática das diretrizes, recomendações e boas práticas referidas nas alíneas b) e b-A);

c-A-0) Emitir diretrizes, recomendações e boas práticas nos termos da alínea b) do n.º 1 para definir procedimentos comuns para a comunicação, por particulares, de infrações ao presente regulamento, nos termos do artigo 49.º, n.º 2.

c-A) Incentivar a elaboração de códigos de conduta e a criação de mecanismos de certificação, bem como de selos e marcas de proteção dos dados nos termos dos artigos 38.º e 39.º;

c-B) Proceder à acreditação dos organismos de certificação e à respetiva revisão periódica nos termos do artigo 39.º-A e conservar um registo público de organismos acreditados, nos termos do artigo 39.º-A, n.º 6, e de responsáveis pelo tratamento de dados ou subcontratantes acreditados, estabelecidos em países terceiros, nos termos do artigo 39.º, n.º 4;

c-D) Especificar as exigências mencionadas no artigo 39.º-A, n.º 3, para acreditação dos organismos de certificação nos termos do artigo 39.º;

c-D-A) Dar parecer à Comissão a respeito dos requisitos de certificação a que se refere o artigo 39.º-A, n.º 7;

c-D-B) Dar parecer à Comissão sobre o os símbolos a que se refere o artigo 12.º, n.º 4-B;

c-E) Dar parecer à Comissão para avaliar a adequação do nível de proteção num país terceiro ou organização internacional, e também para avaliar se um país terceiro, o território ou a organização internacional ou o setor específico deixou de garantir um nível de proteção adequado. Para esse efeito, a Comissão fornece ao Comité Europeu para a Proteção de Dados toda a documentação necessária, inclusive a correspondência com o Governo do país terceiro, o território ou o setor de tratamento de dados nesse país terceiro ou com a organização internacional.

d) Emitir pareceres relativos aos projetos de decisão das autoridades de controlo nos termos do mecanismo de controlo da coerência referido no n.º 2 e sobre as matérias apresentadas nos termos do artigo 57.º, n.º 4;

e) Promover a cooperação e o intercâmbio bilateral e multilateral efetivo de informações e práticas entre as autoridades de controlo;

f) Promover programas de formação comuns e facilitar o intercâmbio de pessoal entre as autoridades de controlo, bem como, se necessário, com as autoridades de controlo de países terceiros ou organizações internacionais;

g) 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.

g-B) Emitir pareceres sobre os códigos de conduta elaborados a nível da União nos termos do artigo 38.º, n.º 4;

i) Conservar um registo eletrónico, acessível ao público, das decisões tomadas pelas autoridades de controlo e pelos tribunais sobre questões tratadas no âmbito do mecanismo de controlo da coerência.

2. Se consultar o Comité Europeu para a Proteção de Dados, a Comissão pode indicar um prazo para a formulação do parecer, tendo em conta a urgência da matéria.

3. O Comité Europeu para a Proteção de Dados transmite os seus pareceres, diretrizes e boas práticas à Comissão e ao comité referido no artigo 87.º, e procede à sua publicação.

4. (...)

4-A. Quando se justificar, o Comité Europeu para a Proteção de Dados consulta as partes interessadas e dá-lhes a oportunidade de formular observações, num prazo razoável. Sem prejuízo do artigo 72.º, o Comité Europeu para a Proteção de Dados torna públicos os resultados do processo de consulta.

Artigo 67.º

Relatórios

1. (...)

2. O Comité Europeu para a Proteção de Dados elabora um relatório anual sobre a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais na União e, quando for relevante, em países terceiros e organizações internacionais. O relatório é publicado e enviado ao Parlamento Europeu, ao Conselho e à Comissão.

3. O relatório anual compreende uma análise da aplicação prática das diretrizes, recomendações e boas práticas a que se refere o artigo 66.º, n.º 1, alínea c), bem como das decisões vinculativas a que se refere o artigo 57.º, n.º 3.

Artigo 68.º

Procedimento

1. Salvo disposição em contrário do presente regulamento, o Comité Europeu para a Proteção de Dados decide por maioria simples dos seus membros.

2. O Comité Europeu para a Proteção de Dados adota o seu regulamento interno por maioria de dois terços dos membros que o compõem e determina as suas modalidades de funcionamento.

Artigo 69.º

Presidente

1. O Comité Europeu para a Proteção de Dados 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 70.º

Funções do presidente

1. O presidente tem as seguintes funções:

   a) Convocar as reuniões do Comité Europeu para a Proteção de Dados e preparar a respetiva ordem de trabalhos;

   a-A) Comunicar as decisões adotadas pelo Comité Europeu para a Proteção de Dados nos termos do artigo 58.º-A à autoridade de controlo principal e às autoridades de controlo interessadas;

   b) Assegurar o exercício das funções do Comité Europeu para a Proteção de Dados dentro dos prazos previstos, em especial no que respeita ao mecanismo de controlo da coerência referido no artigo 57.º.

2. O Comité Europeu para a Proteção de Dados estabelece no seu regulamento interno a repartição de funções entre o presidente e os vice-presidentes.

Artigo 71.º

Secretariado

1. O Comité Europeu para a Proteção de Dados dispõe de um secretariado disponibilizado pela Autoridade Europeia para a Proteção de Dados.

1-A. O secretariado desempenha as suas funções sob a direção exclusiva do presidente do comité.

1-B. O pessoal da Autoridade Europeia para a Proteção de Dados encarregado de exercer as funções conferidas ao Comité Europeu para a Proteção de Dados pelo presente regulamento está sujeito a uma hierarquia distinta do restante pessoal da autoridade.

1-C. Quando se justificar, o Comité Europeu para a Proteção de Dados 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 encarregado de exercer as funções conferidas ao Comité Europeu para a Proteção de Dados pelo presente regulamento.

2. O secretariado fornece ao Comité Europeu para a Proteção de Dados apoio de caráter analítico, administrativo e logístico.

3. O secretariado é responsável, em especial:

a) Pela gestão corrente do Comité Europeu para a Proteção de Dados;

b) Pela comunicação entre os membros do Comité Europeu para a Proteção de Dados, o seu presidente e a Comissão, e pela comunicação com outras instituições e o público;

c) Pelo recurso a meios eletrónicos para a comunicação interna e externa;

d) Pela tradução de informações pertinentes;

e) Pela preparação e acompanhamento das reuniões do Comité Europeu para a Proteção de Dados;

f) 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 Europeu para a Proteção de Dados.

Artigo 72.º

Confidencialidade

1. Os debates do Comité Europeu para a Proteção de Dados são confidenciais quando o referido comité o considerar necessário, nos termos do seu regulamento interno.

2. O acesso aos documentos apresentados aos membros do Comité Europeu para a Proteção de Dados, aos peritos e aos representantes de países terceiros é regido pelo Regulamento (CE) n.º 1049/2001.

3. (...)

CAPÍTULO VIII

VIAS DE RECURSO, RESPONSABILIDADE E SANÇÕES

Artigo 73.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 seus dados pessoais não cumpre o presente regulamento.

2. (...)

3. (...)

4. (...)

5. 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 74.º.

Artigo 74.º

Direito de intentar 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 o direito de intentar ação judicial contra quaisquer 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 o direito de intentar ação judicial se a autoridade de controlo competente nos termos dos artigos 51.º e 51.º-A não atender à reclamação ou não informar o titular dos dados, no prazo de três meses, do andamento ou do resultado da reclamação que tenha apresentado nos termos do artigo 73.º.

3. As ações contra as autoridades de controlo são intentadas nos tribunais do Estado-Membro em cujo território essas autoridades se encontrem estabelecidas.

3-A. Quando for intentada ação contra uma decisão de uma autoridade de controlo que tenha sido precedida de um parecer ou uma decisão do Comité Europeu para a Proteção de Dados no âmbito do mecanismo de controlo da coerência, a autoridade de controlo transmite esse parecer ou decisão ao tribunal.

4. (...)

5. (...)

Artigo 75.º

Direito de intentar ação judicial contra um responsável pelo tratamento dos dados 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, previsto no artigo 73.º, os titulares dos dados têm o direito de intentar 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 mesmo regulamento.

2. As ações judiciais contra os responsáveis pelo tratamento dos dados ou os subcontratantes são intentadas nos tribunais do Estado-Membro em que tenham estabelecimento. Em alternativa, a ações podem ser intentadas nos tribunais do Estado-Membro em que o titular dos dados tenha a sua residência habitual, salvo se o responsável pelo tratamento dos dados ou o subcontratante for uma autoridade de um Estado-Membro no exercício dos seus poderes públicos.

3. (...)

4. (...)

Artigo 76.º

Representação dos titulares dos dados

1. O titular dos dados tem o direito de mandatar um organismo, organização ou associação, devidamente constituída sem fins lucrativos ao abrigo do direito de um Estado-Membro, cujos objetivos estatutários sejam do interesse público e cuja atividade abranja a proteção dos direitos e liberdades do titular dos dados no que respeita à proteção dos seus dados pessoais, para, em seu nome, apresentar reclamação e exercer os direitos previstos nos artigos 73.º, 74.º e 75.º, bem como exercer o direito de receber uma indemnização referido no artigo 77.º, se tal estiver previsto no direito do Estado-Membro.

2. Os Estados-Membros podem prever que o organismo, organização ou associação referido no n.º 1, independentemente de um mandato conferido pelo titular dos dados, tenha nesse Estado-Membro direito a apresentar uma reclamação à autoridade de controlo competente nos termos do artigo 73.º, e a exercer os direitos a que se referem os artigos 74.º e 75.º, caso considere que ocorreu uma violação dos direitos do titular dos dados em virtude do tratamento de dados pessoais em violação do disposto no presente regulamento.

3. (...)

4. (...)

5. (...)

Artigo 76.º-A

Suspensão do processo

1. Quando um tribunal de um Estado-Membro tiver 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 dos dados ou subcontratante, deve contactar o referido tribunal desse outro Estado-Membro a fim de confirmar a existência de tal processo.

2. Caso estejam pendentes num tribunal de outro Estado-Membro processos relativos ao mesmo assunto no que se refere às atividades de tratamento do mesmo responsável pelo tratamento dos dados ou subcontratante, o tribunal onde a ação foi intentada em segundo lugar pode suspender o seu processo.

2-A. Se esse processo estiver 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 77.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 dos dados ou do subcontratante pelo dano sofrido.

2. Qualquer responsável pelo tratamento dos dados 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 legítimas do responsável pelo tratamento dos dados.

3. O responsável pelo tratamento dos dados 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 dos dados ou subcontratante, ou um responsável pelo tratamento dos dados 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 dos dados 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 dos dados ou um subcontratante tem o direito de reclamar a outros responsáveis pelo tratamento de dados 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 nacional do Estado-Membro a que se refere o artigo 75.º, n.º 2.

Artigo 78.º

Sanções

(...)

Artigo 79.º

Condições gerais para a aplicação de multas administrativas

1-A. Cada autoridade de controlo assegura que a aplicação de multas administrativas nos termos do presente artigo relativamente a violações do presente regulamento a que se referem os n.ºs 3 (novo), 3-A (novo) e 3-AA (novo) é, em cada caso individual, efetiva, proporcionada e dissuasiva.

2. (...)

2-A. Consoante as circunstâncias de cada caso, as multas administrativas são aplicadas para além ou em vez das medidas referidas no artigo 53.º, n.º 1-B, alíneas a) a f-A) e alínea h). Ao decidir sobre a aplicação de uma multa administrativa e sobre o montante da multa administrativa 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) (...)

d) A iniciativa tomada pelo responsável pelo tratamento dos dados ou pelo subcontratante para atenuar os danos sofridos pelos titulares;

e) O grau de responsabilidade do responsável pelo tratamento dos dados ou do subcontratante tendo em conta as medidas técnicas ou organizativas por eles implementadas nos termos dos artigos 23.º e 30.º;

f) Quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento dos dados ou pelo subcontratante;

g) (novo) O grau de cooperação com a autoridade de controlo, a fim de sanar a infração e atenuar os seus eventuais efeitos negativos;

g-A) (novo) 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 dos dados ou o subcontratante a notificaram, e em caso afirmativo, em que medida o fizeram;

i) No caso de as medidas a que se refere o artigo 53.º, n.º 1-B, terem sido previamente impostas ao responsável pelo tratamento dos dados ou ao subcontratante em causa relativamente à mesma matéria, o cumprimento dessas medidas;

j) O cumprimento de códigos de conduta aprovados nos termos do artigo 38.º ou de mecanismos de certificação aprovados nos termos do artigo 39.º;

k) (...)

m) 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.

2-B. Se o responsável pelo tratamento dos dados 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 multa não pode exceder o montante especificado para a violação mais grave.

3. (...)

3. (novo) A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 2-A, a multas administrativas 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 dos dados e do subcontratante nos termos dos artigos 8.º, 10.º, 23.º, 24.º, 25.º, 26.º, 27.º, 28.º, 29.º, 30.º, 31.º, 32.º, 33.º, 34.º, 35.º, 36.º, 37.º, 39.º e 39.º-A;

a-A) As obrigações do organismo de certificação nos termos dos artigos 39.º e 39.º-A;

a-B) As obrigações do organismo de supervisão nos termos do artigo 38.º-A, n.º 4;

3-A. (novo) A violação das disposições a seguir enumeradas está sujeita, em conformidade com o n.º 4-A, a multas administrativas até 20 000 000 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) 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 20.º;

b-A) As transferências de dados pessoais para um destinatário num país terceiro ou uma organização internacional nos termos dos artigos 40.º a 44.º;

b-B) As obrigações nos termos da legislação dos Estados-Membros adotada ao abrigo do capítulo IX;

c) 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 53.º, n.º 1-B, ou o facto de não facultar acesso, em violação do artigo 53.º, n.º 1.

3-AA. (novo) O incumprimento de uma ordem emitida pela autoridade de controlo a que se refere o artigo 53.º, n.º 1, alínea b), está sujeito, em conformidade com o n.º 2-A, a multas administrativas 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:

3-B. Sem prejuízo dos poderes de correção das autoridades de controlo nos termos do artigo 53.º, n.º 1-B, os Estados-Membros podem prever normas que permitam determinar se e em que medida as multas administrativas podem ser aplicadas às autoridades e organismos públicos estabelecidos no seu território.

4. O exercício das competências que lhe são atribuídas pelo presente artigo por parte da autoridade de controlo fica sujeito às garantias processuais adequadas previstas no direito da União e dos Estados-Membros, incluindo o direito à ação judicial e a um processo equitativo.

5. Quando o sistema jurídico dos Estados-Membros não preveja multas administrativas, pode aplicar-se o artigo 79.º de modo a que a multa 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 multas administrativas impostas pelas autoridades de controlo. Em todo o caso, as multas impostas devem ser efetivas, proporcionadas e dissuasivas. Os referidos Estados-Membros notificam a Comissão dessas disposições de direito interno o mais tardar na data fixada no artigo 91.º, n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

6. (...)

7. (...)

Artigo 79.º-B

Sanções

1. Os Estados-Membros estabelecem o regime de sanções aplicável às violações ao presente regulamento, em particular às violações que não são sujeitas a multas administrativas nos termos do artigo 79.º, e tomam todas as medidas necessárias para assegurar a sua aplicação. As sanções devem ser efetivas, proporcionadas e dissuasivas.

2. (...)

3. Os Estados-Membros notificam a Comissão das disposições do direito interno que adotem nos termos do n.º 1, o mais tardar na data prevista no artigo 91.º, n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

CAPÍTULO IX
DISPOSIÇÕES RELATIVAS A SITUAÇÕES ESPECÍFICAS DE TRATAMENTO DE DADOS

Artigo 80.º

Tratamento de dados pessoais 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 de dados pessoais para fins jornalísticos e para fins de expressão académica, artística ou literária.

2. Para o tratamento de dados pessoais efetuado para fins jornalísticos ou para fins de expressão académica, artística ou literária, os Estados-Membros estabelecem isenções ou derrogações das disposições do Capítulo II (princípios), do Capítulo III (direitos do titular dos dados), do Capítulo IV (responsável pelo tratamento dos dados 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 adotem nos termos do n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

Artigo 80.º-A

Tratamento dos dados pessoais 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 o exercício de funções de interesse público podem ser divulgados pela autoridade ou organismo nos termos do direito da União ou do direito 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 80.º-A-A

Tratamento de dados pessoais e reutilização das informações do setor público

(...)

Artigo 80.º-B

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 81.º

Tratamento de dados pessoais para fins relacionados com a saúde

(...)

Artigo 81.º-A

Tratamento de dados genéticos

(...)

Artigo 82.º

Tratamento de dados 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 assalariados 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. Essas normas 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 num grupo empresarial ou num grupo de empresas e os sistemas de controlo no local de trabalho.

2-A. Os Estados-Membros notificam a Comissão das disposições de direito interno que adotem nos termos do n.º 1, o mais tardar na data prevista no artigo 91.º, n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

3. (...)

Artigo 83.º

Garantias e derrogações ao tratamento dos dados pessoais para fins de arquivo de interesse público ou para fins estatísticos ou de investigação científica e histórica

1. O tratamento dos dados pessoais para fins de arquivo de interesse público, ou para fins estatísticos ou de investigação científica e histórica, está sujeito, nos termos do presente regulamento, a garantias adequadas para os direitos e liberdades do titular dos dados. Desse modo fica assegurada a adoção de medidas técnicas e organizativas que garantam, em particular, o respeito do princípio da minimização dos dados. Essas medidas podem incluir a pseudonimização, desde que os fins visados possam ser atingidos deste modo. Sempre que possam ser atingidos por novos tratamentos de dados que não permitam, ou já não permitam, a identificação dos titulares dos dados, os referidos fins serão atingidos desse modo.

2. Quando os dados pessoais sejam tratados para fins de investigação científica e 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, 17.º-A e 19.º, sob reserva das condições e garantias previstas no n.º 1, 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, 17.º-A, 17.º-B, 18.º e 19.º, sob reserva das condições e garantias previstas no n.º 1, 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 84.º

Obrigações de sigilo

1. Os Estados-Membros podem adotar normas específicas para estabelecer os poderes das autoridades de controlo previstos no artigo 53.º, n.º 1, alíneas d-A) e d-B), relativamente a responsáveis pelo tratamento de dados 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.

2. Os Estados-Membros notificam a Comissão das normas que adotarem nos termos do n.º 1, o mais tardar na data prevista no artigo 91.º, n.º 2 e, sem demora, de qualquer alteração subsequente das mesmas.

Artigo 85.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 de dados pessoais, tais normas podem continuar a ser aplicadas, desde que cumpram o disposto no presente regulamento.

2. As igrejas e associações religiosas que apliquem um conjunto completo de normas nos termos do n.º 1 ficam sujeitas ao controlo 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 86.º

Exercício da delegação

1. É conferido à Comissão o poder de adotar atos delegados, sob reserva das condições estabelecidas no presente artigo.

2. A delegação de poderes a que se referem o artigo 12.º, n.º 4-C, e o artigo 39.º-A, n.º 7, é conferida à Comissão por um período indeterminado a contar da data de entrada em vigor do presente regulamento.

3. A delegação de poderes a que se referem o artigo 12.º, n.º 4-C, e o artigo 39.º-A, n.º 7, 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 revogação produz efeitos no dia seguinte ao da sua publicação no Jornal Oficial da União Europeia ou numa data posterior nela especificada. A decisão de revogação não prejudica a validade dos atos delegados já em vigor.

4. Logo que adote 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 4-C, e do artigo 39.º-A, n.º 7, 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 desse ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não têm objeções a formular. Esse prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 87.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. Sempre que se faça referência ao presente número, é aplicável o artigo 5.º do Regulamento (UE) n.º 182/2011.

3. Sempre que se faça referência ao presente número, é aplicável o artigo 8.º do Regulamento (UE) n.º 182/2011 em conjugação com o seu artigo 5.º.

CAPÍTULO XI

DISPOSIÇÕES FINAIS

Artigo 88.º

Revogação da Diretiva 95/46/CE

1. A Diretiva 95/46/CE é revogada a partir da data indicada no artigo 91.º, n.º 2.

2. As referências à diretiva revogada são consideradas como referências ao 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 como referências ao Comité Europeu para a Proteção de Dados criado pelo presente regulamento.

Artigo 89.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 de dados pessoais 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 89.º-B

Relação com acordos celebrados anteriormente

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

Artigo 90.º

Avaliação

1. A Comissão apresenta periodicamente ao Parlamento Europeu e ao Conselho relatórios sobre a avaliação e a revisão do presente regulamento.

2. No contexto dessas avaliações, a Comissão examina, em particular, a aplicação e o funcionamento das disposições dos seguintes capítulos:

   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 41.º, n.º 3, 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.

2-A. Para o efeito referido o n.º 1, a Comissão pode solicitar informações aos Estados-Membros e às autoridades de controlo.

2-B. 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 e o Conselho, bem como outros organismos ou fontes pertinentes.

3. O primeiro relatório é apresentado o mais tardar quatro anos após a entrada em vigor do presente regulamento. Os relatórios subsequentes são apresentados com uma periodicidade de quatro anos. Os relatórios são publicados.

4. 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 90.º-A (novo)

Revisão de outros instrumentos da UE em matéria de proteção de dados

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

Artigo 91.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 [*dois anos a contar da data referida no n.º 1*].*****

**** JO: inserir a data***

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

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*